Uudet teknologiat ja digitaalisesti resilientti Suomi

Juhana Harju

Tammikuu 2026

1. Tiivistelmä

1.1 Mitä digitaalinen resilienssi tarkoittaa?

Digitaalinen resilienssi tarkoittaa yhteiskunnan, talouden ja organisaatioiden kykyä sietää, sopeutua ja palautua digitaalisista häiriöistä ja uhkista. Käsite kattaa sekä teknisen infrastruktuurin kestävyyden että yhteiskunnallisen valmiuden reagoida ja mukautua. Tämä selvitys tarkastelee neljää keskeistä teknologia-aluetta, jotka vaikuttavat merkittävästi Suomen digitaaliseen resilienssiin: lohkoketjuteknologioita, kryptovaluuttoja ja digitaalisia valuuttaratkaisuja, reunalaskentaa ja IoT-ekosysteemejä sekä biometristä tunnistamista ja yksityisyyssuojausteknologioita.

Suomi on merkittävän teknologisen murroksen keskellä. Digitalisaation nopea eteneminen, tekoälyn räjähdysmäinen kehitys ja uusien teknologioiden kypsyminen muuttavat yhteiskunnan, talouden ja julkisen hallinnon toimintaympäristöä perustavanlaatuisesti. Vaikka julkisuudessa tekoäly on vienyt suurimman huomion, neljä tarkasteltua teknologia-aluetta kehittyvät nopeasti taustalla ja vaikuttavat laajasti yhteiskunnan eri osa-alueisiin.

Digitaalinen resilienssi voidaan nähdä myös laajemmin yksilön, yhteisön ja yhteiskunnan – suomalaisen, työhön, harrastuksiin tai koulutukseen liittyvien yhteisöjemme ja Suomen – voimavarana, mitä meidän kannattaa jatkuvasti kehittää. Se tulisi nähdä luontaisena lisäyksenä kokonaisturvallisuuden malliimme, mikä on herättänyt kansainvälistä kiinnostusta erityisesti Venäjän aloitettua täysimittaisen hyökkäyksen Ukrainaan 24.2.2022. Suomen kokonaisturvallisuus-ajattelu on näyttäytynyt poikkeuksellisena, sillä siinä on pyritty yhdistämään sekä julkisen sektorin kyvykkyydet, yksityisen sektorin voimavarat niin normaalitilassa kuin kriisioloissa ja kansalaisten aktivointi valmistautumaan, varautumaan ja toimimaan tarvittaessa.

Häilyvyys ja säilyvyys

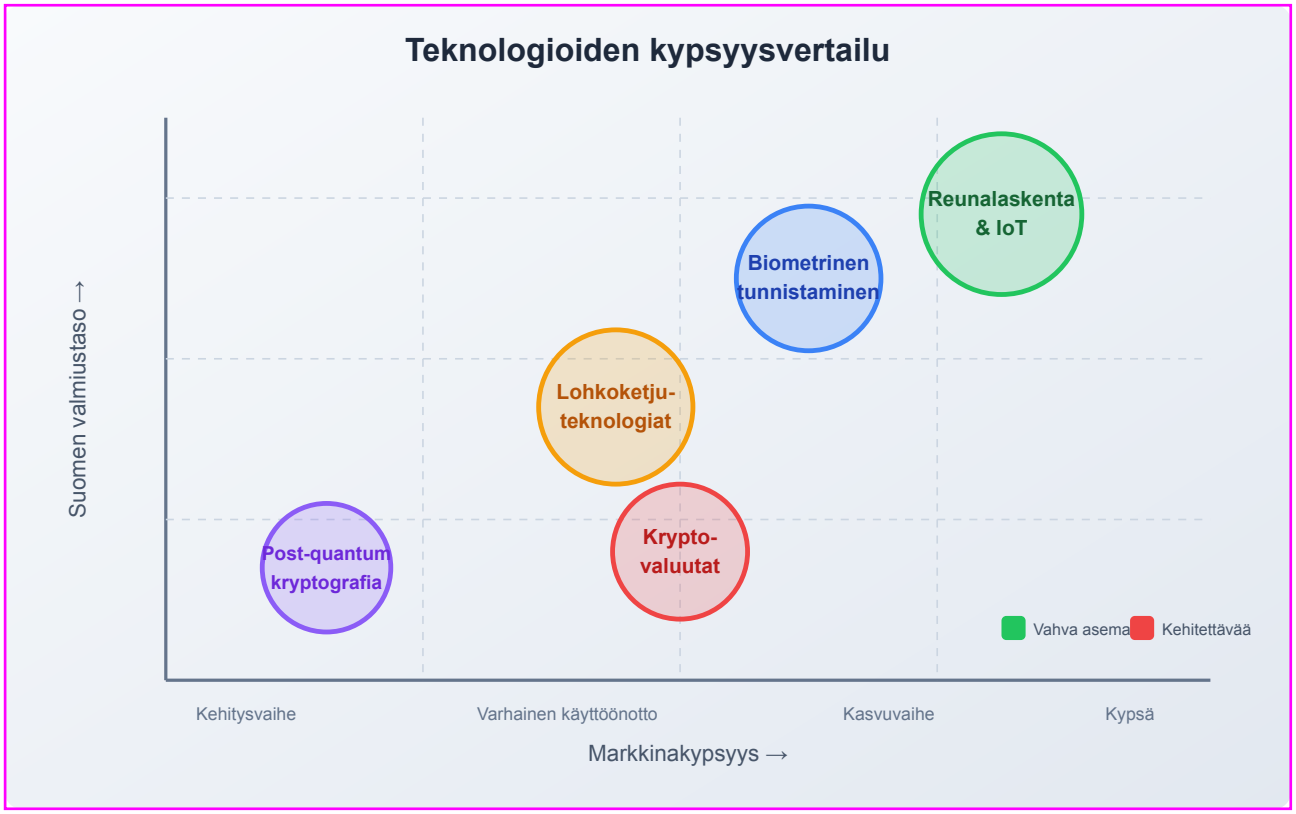
Digitaalinen resilienssi on osa kokonaisturvallisuutta, mutta sitä määrittää kaksi erityistä piirrettä, jotka on syytä käydä tässä läpi, häilyvyys ja säilyvyys.

Häilyvyys kuvaa digitaalisten uhkien vaikeasti hahmotettavaa luonnetta. Siirtymä normaalista poikkeusoloihin tai turvallisesta tilanteesta hybridihyökkäyksen kohteena olemiseen ei ole suuri, eikä digitaalista vaikuttamista ole aina helppo havaita. Se voi jäädä myös kokonaan havaitsematta, jos ulkopuolinen toimija noudattaa onnistuneesti 'kerää nyt, murra myöhemmin' strategiaa. Riski on siis häilyvä: mahdollistaa uskottavan kiistettävyyden, tuottaa aineistoa propagandalle ja pelottelulle ja vaikeuttaa oikein suhteutettujen voimavarojen kohdistamista sen torjuntaan.

Säilyvyys tasapainottaa tätä epävarmuutta. Panostukset digitaalista resilienssiä vahvistavaan koulutukseen, innovointiin, yritystoimintaan ja yhteiskunnan toimintatapoihin ja rakenteisiin eivät mene herkästi hukkaan, vaan kasaantuvat. Kotivaraa täytyy jatkuvasti kierrättää, mikäli sen haluaa pitää ajantasaisena. Kierrättämättä jäänyt voi pilaantua ja resursseja hukataan. Digitaalinen osaaminen vaatii sekin päivitystä, jotta se on ajantasaista, mutta toiminnan ja arvioinnin viitekehyksenä se ei digitalisoituneessa yhteiskunnassamme herkästi vanhene.

Säilyvyys viittaa myös niihin etuihin, mitä vahva digitaalinen resilienssi arjessa tuottaa:

- Yksilötasolla: Arjen sujuvuus työssä, harrastuksissa ja koulutuksessa, vahvistunutta henkilökohtaista varautumista tietoturvan kautta
- Yhteisötasolla: Työyhteisöjen ja harrastusryhmien tuki osaamisen ja työkalujen jakamisessa – kuten Business Finlandin Defense and Digital Resilience -ohjelma korostaa
- Yhteiskuntatasolla: Suomi hyötyy kokonaisturvallisuutensa osana, houkutellen kansainvälistä kiinnostusta mallinsa ansiosta



Kuva 1. Teknologioiden kypsyysvertailu: markkinakypsyys vs. Suomen valmiustaso

1.2 Keskeiset havainnot

- Teknologioiden käyttöönotto mahdollistaa uudenlaista arvonluontia, tehokkuutta ja läpinäkyvyyttä sekä julkisella että yksityisellä sektorilla.
- Samalla teknologiat tuovat mukanaan uusia riskejä: tietoturvauhkia, yksityisyyden haasteita, sääntelyn epäselvyyksiä ja osaamistarpeiden kasvua.
- Suomen erityinen vahvuus on korkea koulutustaso, vahva tutkimus- ja kehitystoiminta sekä historia perusteknologioiden (deep tech) kehittäjänä.
- Kvanttiuhka on konkretisoitumassa: EU edellyttää siirtymää kvanttiturvalliseen salaukseen vuoden 2026 loppuun mennessä kriittisessä infrastruktuurissa.
- Suomalainen startup-ekosysteemi on osoittanut kykynsä tuottaa maailmanluokan yrityksiä myös näillä teknologia-alueilla (esim. Aave lohkoketjualalla).

1.3 Pääsuositukset

Osaamisen vahvistaminen: Panostetaan koulutukseen, tutkimukseen ja osaamisen kehittämiseen kaikilla teknologiasektoreilla. Erityisesti kvanttiturvallisen kryptografian osaaminen on kiireellinen prioriteetti.

Kokeilut ja pilotit: Kannustetaan julkista ja yksityistä sektoria kokeilemaan uusia teknologioita osana laajempia kehittämishankkeita (esim. sandbox-ympäristöt), ei pelkkinä irrallisina pilotteina. Pilottien kautta täytyy päästä purkamaan sääntelyn esteitä.

Sääntelyn kehittäminen: Luodaan joustavat ja ennakoivat sääntelykehykset. MiCA-asetuksen implementoinnissa Suomen tulee varmistaa, ettei tulkinta ole kilpailijamaita tiukempi.

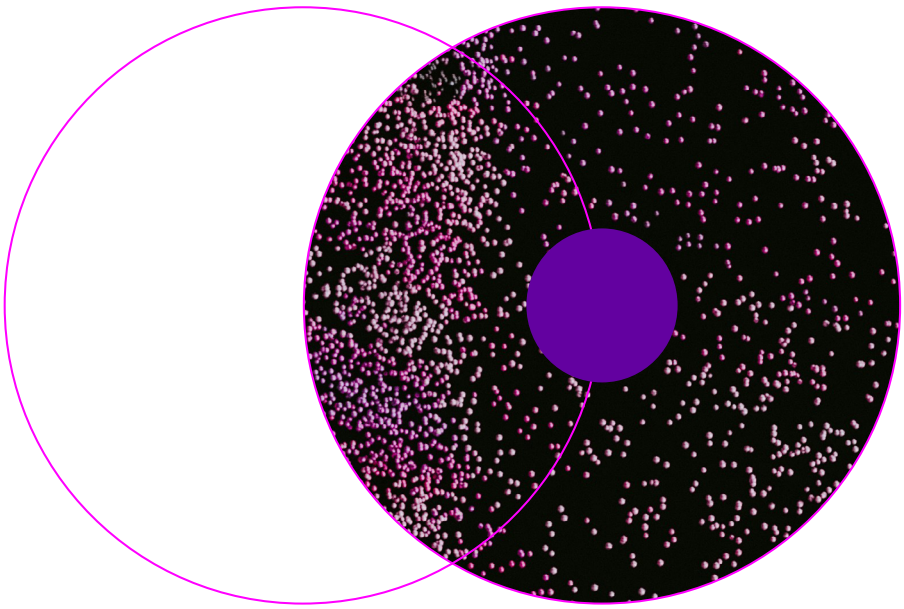
Ekosysteemien tukeminen: Rakennetaan vahvoja yhteistyöverkostoja yritysten, tutkimuslaitosten ja julkisen sektorin välille. Hyödynnetään EU-hankerahoitusta ja kytketään hankkeet EU-tason tavoitteisiin.

Kyberturvallisuus ja yksityisyys: Kehitetään toimintamalli Suomen olemassa olevan kyberturvallisuusstrategian alle, ei rinnakkaiseksi strategiaksi.

Yksityisyydensuojateknologiat erityistarkasteluun

Valitaan teknologia-alue, joka ei ole liian pitkälle edennyt Suomen voimavaroihin suhteutettuna, jolla voidaan ennakoida olevan kriittistä merkitystä tulevaisuudessa ja mihin panostukset voivat tuottaa merkittävää lisäarvoa: parempaa kansallista resilienssiä, kansainvälisesti kiinnostavaa osaamista ja taloudellista toimeliaisuutta.

Kirjallisen raportin luovutushetkellä tammikuussa 2026 ydinvalinta kohdistuu yksityisyydensuojateknologioihin, erityisesti post-quantum kryptografiaan.



2. Miksi tämä selvitys tehtiin?

2.1 Tarvitsemme tarkempaa digipuhetta

Digitalisaatio ja teknologinen kehitys ovat viime vuosina muuttaneet yhteiskuntien, talouden ja julkisen hallinnon toimintaympäristöä ratkaisevasti. Uudet teknologiat tarjoavat mahdollisuuksia lisätä tehokkuutta, läpinäkyvyyttä ja turvallisuutta, mutta tuovat mukanaan myös uusia riskejä ja haasteita. Suomen kilpailukyvyn ja digitaalisen resilienssin vahvistaminen edellyttää, että näihin teknologioihin liittyvät mahdollisuudet ja riskit tunnistetaan ajoissa ja niihin reagoidaan ennakoivasti.

Tämän selvityksen tavoitteena on tarjota kattava analyysi neljästä keskeisestä teknologia-alueesta, jotka ovat olennaisia Suomen digitaalisen resilienssin ja kilpailukyvyn kannalta. Selvityksen avulla pyritään tukemaan päätöksentekoa, ohjaamaan kansallista teknologiastrategiaa sekä tarjoamaan konkreettisia politiikkasuosituksia eri sidosryhmille.

Selvityksen tarkoituksena on myös edistää rohkeaa julkista keskustelua, luoda poliittista ymmärrystä teknologioiden merkityksestä ja toimia tulevaisuuden vuoropuhelun käynnistäjänä sijoittajien, kasvua hakevien yritysten, vakiintuneiden yritysten, kansalaisyhteiskunnan ja päättäjien välillä.

Tarvitsemme rohkeutta – ja sen lisäksi tarvitsemme tarkkuutta. On pyrittävä tunnistamaan, milloin termejä käytetään markkinointivälineenä ja milloin taas kuvamaan tarkasti itse teknologiaa, sen toimintaa ja tuottamaa lisäarvoa. Silloin, kun kaikissa uusissa kehityshankkeissa, startupeissa ja tuoteprojekteissa korostetaan, että niiden ydintoiminnallisuudet hyödyntävät tekoälyä, menettää sana merkityksensä. Seuraava kysymys on: mitä tekoälyä tarkalleen, miten ja miksi – ja mitä lisäarvoa se tuottaa teknologian käyttäjille? Ellei tähän tarkkuuteen päästä on riskinä kehitettävien teknologioiden, niiden sovellusten ja sovelluksia käyttävien palveluiden etääntyminen käyttäjistään. Välille on muodostunut epätarkan digipuheen kiinanmuuri.

2.2 Neljä ajankohtaista teknologiaa suurennuslasin alle

Selvityksen rajaus perustuu kolmeen kriteeriin. Huomioarvo: tekoäly ja siruteknologia saavat jo runsaasti huomiota muissa selvityksissä ja julkisessa keskustelussa. Täydentävyys: kvanttiteknologiasta käsitellään PQC-siirtymä (luku 8), joka on digitaalisen resilienssin kannalta kriittisin osa-alue. Synergia: valitut neljä teknologia-aluetta muodostavat keskinäisten riippuvuuksien kokonaisuuden

(luku 7) vaikutusten perusteella. Ne on myös tunnistettu sellaisiksi, joista keskustelu julkisuudessa ja poliittisessa valmistelussa on ollut vähäisempää tai sisällöltään liian kapeaa. Lisäksi arvioidaan näiden teknologioiden konvergenssia ja synergioita, sillä yhteydet teknologioiden välillä ovat vahvoja ja osin ilmiselviä, kuten lohkoketjuteknologiaan nojautuvat kryptovaluutat.

2.3 Suomalainen ekosysteemi on vahvalla pohjalla, mutta vaatii kehitystä

Suomi on kärkijoukossa useimmissa EU:n määrittelemissä kriittisissä teknologioissa. Langattomat verkot, tekoäly, puolijohteet, fotoniikka, kvanttiteknologia, avaruusteknologia ja kyberteknologia mahdollistavat sekä älykkäiden laitteiden kehittämisen ja kilpailukykyisen tuotannon että uusien digitaalisten palvelujen ja liiketoimintamallien luomisen.

Suomalaisessa startup-ekosysteemissä toimii vahvoja toimijoita kaikilla selvityksessä tarkastelluilla alueilla. Suomen IoT-infrastruktuurin startup-kenttä käsittää yli 50 yritystä, joista 20 on kerännyt merkittävää rahoitusta ja 10 on edennyt Series A -kierroksen yli. Merkittäviä toimijoita ovat muun muassa Wirepas, Haltian, Tosibox ja Treon.

Case: Aave ja suomalainen lohkoketjuosaaminen

Suomalainen Stani Kulechov perusti vuonna 2017 Aave-protokollan, joka on kasvanut yhdeksi maailman suurimmista hajautetun rahoituksen (DeFi) alustoista. Aaveen kautta on välitetty miljardien eurojen edestä lainoja ilman perinteisiä finanssi-instituutioita. Vuonna 2025 suomalaiset startupit keräsivät yhteensä yli 1,5 miljardia euroa rahoitusta, josta blockchain-sektori sai merkittävän osan – Aaveen menestystarina osoittaa, että Suomesta voi syntyä globaaleja teknologiajohtajia näillä alueilla, kunhan sääntely mahdollistaa kasvun.

Muita suomalaisia lohkoketjuosaajia:

- Token Terminal (Helsinki): Analytiikkayritys, joka tarjoaa reaaliaikaista dataa DeFi-protokollista ja blockchain-sovelluksista – yksi Suomen seuratuimmista työkaluista sijoittajille.
- Tesseract (Helsinki): Säännelty digitaalisten varojen säilyttäjä ja sijoituspalvelut, FIN-FSA:n hyväksymä VASP.
- TX Tomorrow Explored (Helsinki): Blockchain-kehityspalvelut startuppeille ja yrityksille lohkoketjun käyttöönottoon.
- VALEGA Chain Analytics (Suomi): Transaktioiden ja riskien analytiikka blockchain-verkoissa.
- Coinmotion (Helsinki): Kryptopalvelut, jotka ovat laajentuneet DeFi-trendeihin ja isoimpiin volyymeihin Suomessa.

3. Lohkoketjuteknologiat ja hajautetut järjestelmät – luottamusta ilman välikäsiä

3.1 Lohkoketjujen anatomiaa

Lohkoketjuteknologia (blockchain) on hajautettu tietokantaratkaisu, joka mahdollistaa tietojen turvallisen ja läpinäkyvän tallentamisen ja jakamisen useiden toimijoiden kesken ilman keskitettyä hallintoa. Teknologia perustuu kryptografisesti linkitettyihin tietolohkoihin, jotka muodostavat muuttumattoman tapahtumaketjun. Älykkäät sopimukset (smart contracts) ovat lohkoketjussa toimivia ohjelmia, jotka suorittavat ennalta määriteltyjä toimintoja automaattisesti tiettyjen ehtojen täyttyessä.

Hajautettu identiteetinhallinta (Decentralized Identity, DID) on lohkoketjuteknologiaan perustuva järjestelmä, jossa yksilö hallitsee omaa digitaalista identiteettiään ilman keskitettyä palveluntarjoajaa. Web3 viittaa internetin seuraavaan kehitysvaiheeseen, jossa käyttäjät omistavat oman datansa ja osallistuvat suoraan alustojen hallintaan lohkoketjuteknologian avulla. Web3 oli muutama vuosi sitten internetin suurimpia lupauksia, kunnes tekoälyhuuma pyyhki sen mennessään. Kehitys kuitenkin etenee määrätietoisesti kulisseissa ja tähän työhön osallistuminen on Suomelle suuri mahdollisuus.

3.2 Loistava mahdollisuus Suomelle

Lohkoketjuteknologia tarjoaa Suomelle merkittäviä mahdollisuuksia julkishallinnon tehostamisessa, toimitusketjujen läpinäkyvyyden parantamisessa ja uusien liiketoimintamallien mahdollistamisessa. Erityisesti hajautettu identiteetinhallinta voisi täydentää Suomen vahvaa digitaalista infrastruktuuria ja kansalliset rekisterit voisivat hyötyä lohkoketjuteknologian tarjoamasta muuttumattomuudesta ja auditointimahdollisuuksista.

Suomelle tämä on loistava mahdollisuus:

- Suomi on Euroopan kärkimaita lohkoketju-startupeissa: Tesseract ja Token Terminal keräävät globaaleja investointeja, tarjoten toimitusketjujen reaaliaikaista läpinäkyvyyttä metsä- ja teknologia-alalle, missä perinteiset rekisterit kohtaavat haasteita. Suomalainen ScanwAI on tuotteistanut AI-pohjaista tieverkon monitorointia vaurioiden havaitsemiseen, mikä vähentää ylläpitokustannuksia jopa 40 % ja pidentää teiden käyttöikää.
- Sitra rahoittaa seitsemää Web3-projektia, testaten hajautettua identiteettiä julkishallinnon piloteissa – tämä on tehokasta, sillä Suomi yhdistää lohkoketjun kansallisiin rekistereihin hybridimallilla, vähentäen tietomurtoja jopa 90 % verrattuna keskitettyihin järjestelmiin.
- Eduskunnan raportti ehdottaa lohkoketjua globaaliin sähköiseen identiteettiin kehitysmaiden perusoikeuksien edistämiseksi, hyödyntäen Suomen digitaalista infrastruktuuria auditointiin.

Case: Viro – Maailman edistynein e-hallinto

Viro on rakentanut maailman edistyneimmän digitaalisen hallinnon, jonka perustana on KSI (Keyless Signature Infrastructure) -lohkoketjuteknologia. Järjestelmä suojaa kansalaisten terveystietoja, oikeudellisia asiakirjoja ja rekisteritietoja manipuloinnilta. E-Residency-ohjelma on houkutellut yli 103 000 e-kansalaista ympäri maailmaa, ja heidän perustamiensa yritysten kautta Viron verotuloihin on kertynyt yli 100 miljoonaa euroa.

Case: Dubai – Kiinteistörekisteri lohkoketjussa

Dubain maavirasto (Dubai Land Department) lanseerasi maaliskuussa 2025 maailman ensimmäisen lohkoketjupohjaisen kiinteistörekisterin. Toukokuussa 2025 rekisteröitiin ensimmäinen täysin tokenoitu omistuskirja. Järjestelmä mahdollistaa kiinteistöomistuksen jakamisen murto-osiin, mikä avaa kiinteistösijoittamisen piensijoittajille. Suomessa vastaava järjestelmä voisi tehostaa Maanmittauslaitoksen toimintaa ja mahdollistaa uusia kiinteistösijoitustuotteita.

3.3 Riskit on tunnistettava

Lohkoketjuteknologian käyttöönottoon liittyy riskejä, jotka on tunnistettava. Skaalautuvuus on edelleen haaste monissa lohkoketjuratkaisuissa. Energiankulutus, erityisesti Proof-of-Work-konsensusmekanismia käyttävissä järjestelmissä, on merkittävä ympäristökysymys. Sääntelykehyksen epäselvyys luo epävarmuutta yrityksille ja hidastaa käyttöönottoa.

Kvanttiuhka on erityisen kriittinen lohkoketjuteknologioille. Nykyiset lohkoketjut perustuvat kryptografisiin menetelmiin, jotka tulevat olemaan haavoittuvia kvanttitietokoneille. EU edellyttää siirtymää kvanttiturvalliseen kryptografiaan kriittisessä infrastruktuurissa vuoden 2026 loppuun mennessä, ja täydellinen migraatio tulee tapahtua vuoteen 2035 mennessä.

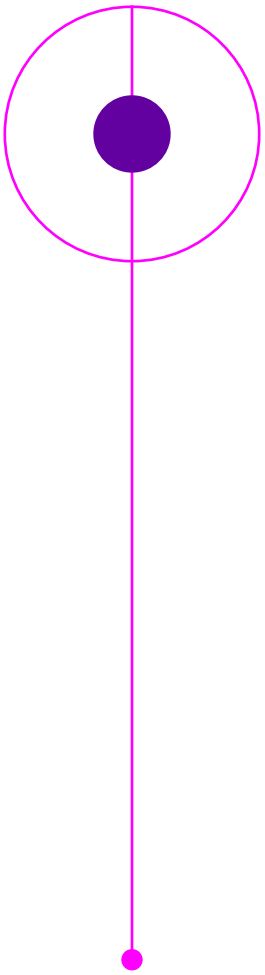
Lohkoketjujärjestelmien kvanttiturvalliseen kryptografiaan siirtymistä käsitellään tarkemmin luvussa 8.3.

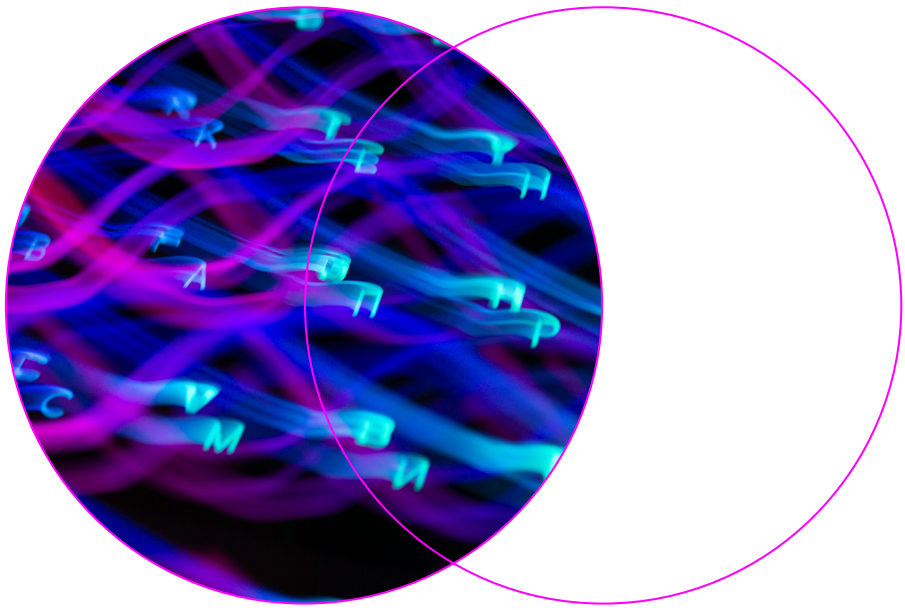
3.4 Mitä yritykset odottavat?

Suomalainen teollisuus on ilmaissut kiinnostusta lohkoketjuteknologian hyödyntämiseen erityisesti toimitusketjujen seurannassa ja alkuperän todentamisessa. Metsäteollisuudessa puuraaka-aineen alkuperän jäljittäminen on enenevässä määrin tärkeää EU:n metsäkatosääntelyyn (EUDR) vastaamiseksi. Konepajateollisuudessa laitteiden huoltohistorian ja varaosien alkuperän todentaminen lohkoketjun avulla voisi vähentää väärennöksiä ja parantaa turvallisuutta. Oheinen case on kahden yhdysvaltalaisen jättiläisen toteuttama, mutta samoja hyötyä – paikallisesti sovellettuna – on saatavissa myös suomalaisin toimin ja meille olennaisille teollisuuden sektoreille.

Case: Walmart & IBM Food Trust – Jäljitettävyys sekunneissa

Walmart otti käyttöön IBM:n lohkoketjuratkaisun elintarvikkeiden jäljittämiseen. Ennen järjestelmää mangon alkuperän selvittäminen kesti 7 päivää – lohkoketjulla sama tieto saadaan 2,2 sekunnissa. Walmart on sittemmin velvoittanut kaikki tuoreiden lehtivihannesten toimittajansa käyttämään järjestelmää. Suomalaiselle metsä- ja elintarviketeollisuudelle vastaava ratkaisu voisi vastata EUDR-vaatimuksiin ja parantaa kuluttajaluottamusta.





4. Tulevaisuuden raha on täysin digitaalista

4.1 Bitcoinista digitaaliseen euroon

Kryptovaluutta on digitaalinen valuutta, joka perustuu kryptografiaan ja toimii usein hajautetussa verkossa ilman keskitettyä hallintoa. Tunnetuin esimerkki on Bitcoin, mutta markkinoilla on tuhansia erilaisia kryptovaluuttoja erilaisiin käyttötarkoituksiin. Stablecoinit ovat kryptovaluuttoja, joiden arvo on sidottu johonkin vakaaseen kohde-etuuteen, kuten dollariin tai euroon.

CBDC (Central Bank Digital Currency) eli keskuspankkien digitaalinen valuutta on keskuspankin liikkeeseen laskema digitaalinen raha. Toisin kuin kryptovaluutat, CBDC:t ovat keskuspankin suoraan liikkeeseen laskemia ja valtion takaamia. Euroopan keskuspankki (EKP) valmistelee parhaillaan digitaalista euroa.

Kryptovaluuttoihin liittyvä tekninen, juridinen ja periaatteellinen keskustelu käy kuumana. Olennainen havainto on, että niiden hyväksyttävyys, käyttöönotto ja merkitys lisääntyy jatkuvasti. On välttämätöntä, että Suomi seuraa kehitystä tarkasti ja ottaa sille teknisen kyvykkyyspotentiaalin tarjoaman roolin.

Case: Standard Chartered – Ensimmäinen systeemisesti merkittävä pankki kryptokaupankäyntiin

Brittiläinen suurpankki Standard Chartered käynnisti heinäkuussa 2025 ensimmäisenä globaalisti systeemisesti merkittävänä pankkina (G-SIB) spot-kryptokaupankäynnin. Tammikuussa 2026 pankki laajensi palveluitaan Hongkongissa Bitcoin- ja Ethereum-säilytyspalveluilla ja valmistelee institutionaalista kryptovälitys- ja prime brokerage -alustaa. Kehitys osoittaa, että MiCA:n kaltainen selkeä sääntely mahdollistaa pankkien tulon kryptomarkkinoille – Suomen tulisi varmistaa, ettei kotimainen tulkinta ole kilpailijamaita tiukempi.

4.2 MiCA-asetus – EU:n uudet pelisäännöt

MiCA-asetus (Markets in Crypto-Assets Regulation) luo ensimmäisen kattavan EU-tason sääntelykehyksen kryptovaroille. Asetus astui kokonaisuudessaan voimaan joulukuussa 2024. MiCA asettaa vaatimuksia kryptovarojen liikkeeseenlaskijoille ja palveluntarjoajille liittyen lupamenettelyihin, pääomavaatimuksiin, kuluttajansuojaan ja markkinoiden väärinkäytön estämiseen.

Suomen tulkinta MiCA-asetuksen implementoinnista on kriittinen kilpailutekijä. Useat suomalaiset kryptoyritykset ovat viime vuosina siirtäneet toimintansa maihin, joissa sääntely-ympäristö on koettu suotuisammaksi, kuten Maltalle, Viroon ja Sveitsiin. VM:n rahoitusmarkkinaosaston näkemysten kartoittaminen ja pyöreän pöydän keskustelut alan toimijoiden kanssa ovat keskeisiä askeleita sääntelyilmapiirin parantamiseksi. Näiden keskustelujen kiireellisyyttä ei voi liikaa korostaa. Myös tavoitteiden asettelun on oltava kunnianhimoista, jotta takamatka voidaan kuroa

Case: Sveitsi – Crypto Valley Zug

Sveitsin Zugin kantoni on kehittynyt ’Crypto Valleyksi’, jossa toimii yli 719 blockchain-yritystä. Zugin menestys perustuu selkeään ja yritysmyönteiseen sääntelyyn: kanton hyväksyi jo 2016 Bitcoinin maksuvälineeksi veroissa, ja Sveitsin finanssivalvonta FINMA on luonut selkeät ohjeet tokenien luokitteluun ja liikkeeseenlaskuun. Vuonna 2025 alueen yhtiöiden yhteenlaskettu markkina-arvo ylitti 500 miljardia Sveitsin frangia.

Case: Singapore – Tiukka mutta selkeä sääntely

Singapore on valinnut tiukan mutta ennakoitavan linjan kryptosääntelyssä. MAS (Monetary Authority of Singapore) asetti kesäkuussa 2025 tiukan määräajan kaikille kryptopalvelujen tarjoajille rekisteröityä tai lopettaa toiminta. Tiukkuudestaan huolimatta Singapore on houkutellut merkittäviä kryptoyrityksiä, koska säännöt ovat selkeät ja johdonmukaiset. Esimerkki osoittaa, että tiukkakin sääntely voi olla kilpailuetu, jos se on läpinäkyvä ja ennakoitava.

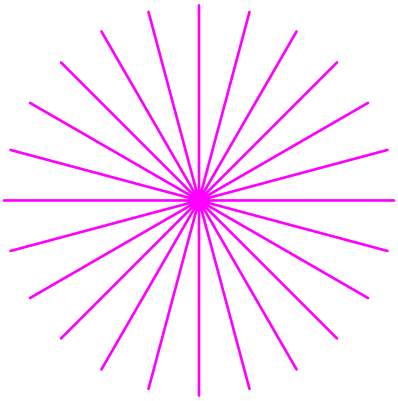
4.3 Euroopan yhteinen digiraha – osa ratkaisua?

Euroopan keskuspankki päätti lokakuussa 2025 valmisteluvaiheesta ja etenee digitaalisen euron pilotointivaiheeseen vuonna 2027. Mahdollinen käyttöönotto tapahtuisi aikaisintaan vuonna 2029. Digitaalinen euro olisi keskuspankkien liikkeeseen laskema digitaalinen raha, joka täydentäisi käteistä – ei korvaisi sitä.

Digitaalinen euro tarjoaisi kansalaisille turvallisen digitaalisen maksuvälineen, joka ei ole riippuvainen yksityisistä maksupalveluista. Se vahvistaisi euron asemaa kansainvälisenä valuuttana ja tarjoaisi vaihtoehdon ulkomaisille digitaalisille maksuratkaisuille. Suomen tulisi osallistua aktiivisesti digitaalisen euron valmisteluun ja varmistaa, että suomalaisten erityistarpeet huomioidaan. Tärkeintä on ymmärtää, ettei kyse ole vaihtoehdosta perinteisille kryptoille vaan enemmän komplementista. Molemmille on rahoitus- ja maksujärjestelmässä paikkansa.

Case: Intia – Aadhaar ja digitaalinen identiteetti

Intian Aadhaar-järjestelmä on maailman suurin biometrinen tunnistusjärjestelmä, johon on rekisteröitynyt yli 1,4 miljardia ihmistä. Järjestelmän kautta on siirretty suoria etuuksia, mikä on säästänyt arviolta 40 miljardia dollaria vähentämällä väärinkäytöksiä ja välikäsiä. Samalla järjestelmä on herättänyt huolta yksityisyydestä ja syrjäytymisestä – ihmiset, jotka eivät pysty rekisteröitymään, jäävät palvelujen ulkopuolelle.



5. Äly verkon reunalle

5.1 Laskentaa lähellä dataa

Reunalaskenta (edge computing) tarkoittaa laskentatehon ja datankäsittelyn siirtämistä lähemmäs tiedon lähdettä, pois keskitetyistä pilvipalvelimista. Tämä mahdollistaa nopeamman päätöksenteon, pienemmät viiveet ja paremman yksityisyyden, kun kaikkea dataa ei tarvitse siirtää keskitettyihin palvelimiin. Reunalaskenta on kriittinen teknologia 6G-verkkojen kehityksessä ja autonomisten järjestelmien, kuten itseohjautuvien ajoneuvojen, toiminnassa.

IoT (Internet of Things) eli esineiden internet viittaa verkkoon kytkettyihin laitteisiin ja sensoreihin, jotka keräävät ja jakavat dataa. Teollinen IoT (IIoT) keskittyy teollisuuden sovelluksiin, kuten tuotannon optimointiin ja ennakoivaan kunnossapitoon.

Molemmilla sektoreilla on teknologian läpimurto ja sen täysimittainen hyödyntäminen vasta edessä ja tähän kilpailuun Suomen on syytä osallistua.

Huawei ja globaali älykaupunki-infrastruktuuri

Huawei on noussut yhdeksi maailman johtavista reunalaskenta-alustojen toimittajista älykaupunkisektorilla. Yhtiön ”City Intelligent Twins” -arkkitehtuuri on otettu käyttöön yli 160 kaupungissa yli 100 maassa. Ratkaisussa reunasolmut käsittelevät kriittisen datan paikallisesti – liikenteen optimoinnista energiaverkkojen hallintaan ja turvallisuusjärjestelmiin – minimoiden viiveen ja parantaen järjestelmien toimintavarmuutta.

Gartnerin arvion mukaan vuoteen 2025 mennessä jopa 75 prosenttia yritysten tuottamasta datasta tullaan käsittelemään reunalaitteissa perinteisen keskitetyn pilvi-infrastruktuurin sijaan. Huawein laaja älykaupunkiportfolio havainnollistaa tätä kehityssuuntaa käytännössä.

Euroopassa ja Suomessa Huawein rooli kriittisessä infrastruktuurissa on herättänyt keskustelua teknologisen riippuvuuden, toimitusketjujen resilenssin ja tietoturvan näkökulmista. Tapaus alleviivaa tarvetta arvioida reunalaskentaratkaisujen toimittajavalintoja osana laajempaa digitaalista huoltovarmuutta.

5.2 Nokia ja 6G – tulevaisuutta tekemässä

Suomi on reunalaskennan ja IoT:n kehityksen eturintamassa. Nokia avasi syyskuussa 2025 Ouluun 55 000 neliömetrin 6G- ja reunalaskentakampuksen, jossa työskentelee noin 3 000 työntekijää. Kampus keskittyy 6G-teknologioiden ja reunalaskentaratkaisujen kehittämiseen ja on yksi Euroopan merkittävimmistä investoinneista alalle. Aika näyttää onko Nokian investointi kaukonäköinen, mutta joka tapauksessa kyseessä on merkittävä päänavaus mikä mahdollistaa erilaisten klustereiden rakentamisen ja strategiset, tukevat investoinnit.

Case: Nokia Oulu – 6G-kampus

Nokian Oulun 6G-kampus avattiin syyskuussa 2025. Kampus on yksi Euroopan suurimmista tutkimus- ja kehityskeskuksista langattoman teknologian alueella. Tavoitteena on kehittää 6G-teknologioita, jotka mahdollistavat jopa 100 kertaa nopeammat yhteydet kuin 5G ja viiveet alle millisekunnin. Reunalaskenta on keskeinen osa 6G-arkkitehtuuria, mahdollistaen tekoälyn ja reaaliaikasovellusten toiminnan verkon reunalla, ja 6G taas on Nokian tulevaisuuden kasvunäkymien ytimessä.

5.3 Wirepas, Haltian ja kumppanit – Suomalainen IoT-ekosysteemi

Suomessa toimii vahva IoT-yritysten ekosysteemi. Wirepas, tamperelainen yritys, on kehittänyt hajautetun mesh-verkkoteknologian, joka mahdollistaa miljoonien laitteiden yhdistämisen ilman keskitettyä infrastruktuuria. Yritys on kerännyt yhteensä 74,9 miljoonaa dollaria rahoitusta ja on keskeinen toimija maailmanlaajuisesti skaalautuvien IoT-verkkojen kehityksessä.

Haltian, oululainen IoT-yritys, tarjoaa kokonaisvaltaisia IoT-ratkaisuja älykkäiden rakennusten ja omaisuuden seurannan alueilla. Yhtiön Thingsee-alusta on käytössä kymmenissä maissa. Haltian ja Wirepas ovat yhdessä kehittäneet reaaliaikaisen paikannusjärjestelmän (RTLS), joka saavuttaa 1–3 metrin tarkkuuden suurissa teollisissa ympäristöissä.

Case: Tampereen älykaupunki-IoT

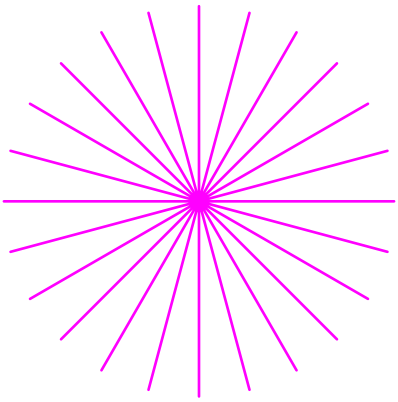
Tampereen kaupunki on rakentanut pilvipohjaiseen alustaan kytketyn IoT-järjestelmän, joka yhdistää paikalliseen reunalaskentapalvelimeen. Järjestelmää käytetään liikenteen seurantaan ja ohjaukseen, ulkovalaistuksen hallintaan, kaupungin kunnossapitoon, televiestinnän turvallisuuteen ja lämmitysjärjestelmien optimointiin.

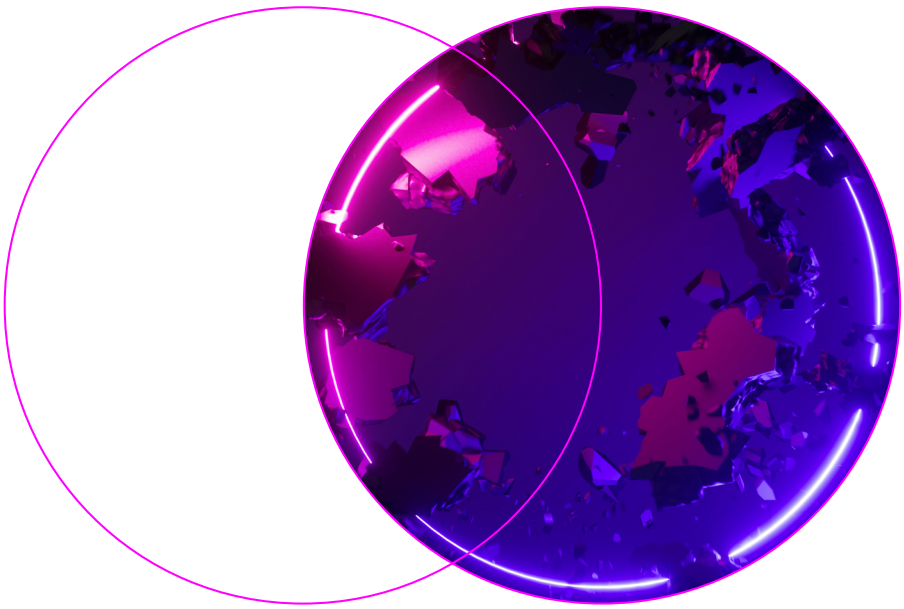
5.4 Turvallisuuskysymykset on ratkaistava

Digitan ja Taloustutkimuksen ’Teollisuuden digitalisaatio nyt’ -tutkimus osoittaa, että suomalaiset teollisuusyritykset ovat laajasti ottaneet käyttöön digitaalisia ratkaisuja tuotannossaan. Suurimmat tavoitteet ovat tehokkuuden parantaminen, joustavampi tuotanto ja parempi päätöksenteko. Samalla 60 prosenttia yrityksistä kokee, etteivät nykyiset verkot tue riittävästi tietoturvallista langatonta tiedonsiirtoa.

IoT-laitteiden integrointi luo laajoja laiteverkostoja, jotka voivat olla huonosti suojattuja. Kyberrikolliset voivat hyväksikäyttää laitteiden haavoittuvuuksia päästäkseen käsiksi arkaluontoisiin tietoihin tai häiritäkseen teollisten järjestelmien toimintaa. 5G-privaattiverkot tarjoavat yhden ratkaisun, mutta niiden käyttöönotto vaatii investointeja ja osaamista.

Saman tutkimuksen mukaan merkittävimpiä haasteita digitalisaatiossa ovat osaamisen ja resurssien puute. Joka neljäs suomalaisyritys (26 prosenttia) on tunnistanut liiketoimintaa haitanneen tietoturvatapahtuman organisaatiossaan viimeisten kahden vuoden aikana.





6. Digitaalinen sinä ja turvallisuuden uudet tarpeet

6.1 Sormenjäljistä nollatietotodistuksiin

Biometrinen tunnistaminen perustuu yksilöllisiin fyysisiin tai käyttäytymiseen liittyviin ominaisuuksiin, kuten sormenjälkiin, kasvoihin, iiriskuvioihin tai kävelytyyliin. Teknologia mahdollistaa turvallisen tunnistautumisen ilman salasanoja tai fyysisiä avaimia. Se mahdollistaa samalla myös seurannan ja yksilöitävien datamassojen keräämisen.

Yksityisyyssuojausteknologiat (Privacy-Enhancing Technologies, PETs) ovat teknologioita, jotka mahdollistavat datan käsittelyn säilyttäen samalla yksityisyyden. Nollatietotodistukset (zero-knowledge proofs) mahdollistavat tiedon todentamisen paljastamatta itse tietoa – esimerkiksi iän varmistamisen ilman syntymäajan paljastamista. Homomorfinen salaus (homomorphic encryption) mahdollistaa laskennan suorittamisen salatulle datalle purkamatta salausta.

Case: HSBC ja Alan Turing -instituutti: Rahanpesun torjunta salatulla datalla

Suurpankki HSBC ja Alan Turing -instituutti soveltavat homomorfista salausta rahanpesun torjuntaan. Teknologia mahdollistaa epäilyttävien transaktiokuvioiden tunnistamisen ilman salauksen purkamista – arkaluonteinen asiakasdata pysyy salattuna myös analyysivaiheessa. HSBC:n 63 maan verkostossa tämä ratkaisee rajat ylittävän tiedonvaihdon tietosuojahaasteet. Homomorfisen salauksen markkinan ennustetaan kasvavan 226 miljoonasta dollarista (2024) 1,12 miljardiin dollariin vuoteen 2030 mennessä.

Case: Google Wallet ja Bumble: Ikävarmennus ilman henkilötietojen paljastamista (2025)

Google otti toukokuussa 2025 käyttöön nollatietotodistuksiin perustuvan ikävarmennuksen Google Walletissa. Deittisovellus Bumble hyödyntää teknologiaa ensimmäisenä: käyttäjä voi todistaa olevansa täysi-ikäinen paljastamatta syntymäaikaansa tai henkilöllisyystodistustaan. Google on julkistanut ZKP-kirjastonsa avoimena lähdekoodina, ja EU:n eIDAS-asetus kannustaa vastaavien teknologioiden integrointia EUDI-lompakoihin vuodesta 2026 alkaen.

6.2 Tuotteita terveydenhuollosta finanssisektoriin

Biometrinen tunnistaminen yhdistettynä yksityisyyssuojausteknologioihin tarjoaa mahdollisuuksia terveydenhuollossa, julkishallinnossa ja finanssisektorilla. Potilaan tunnistaminen biometrisesti voi vähentää virheitä ja parantaa turvallisuutta. Rahanpesun torjunnassa ja asiakkaan tuntemisessa (KYC) biometria voi tehostaa prosesseja säilyttäen samalla yksityisyyden.

Turvallinen ja varma, yksityisyyden säilyttävä tunnistaminen on kriittinen palvelu läpidigitalisoituneessa yhteiskunnassa. Kansalaisten perusoikeuksien suojelu ja tasa-arvo ovat uhattuina ellemme rakenna tähän infrastruktuuria ja ota sitä kattavasti käyttöön. Suomella on tekniset, kulttuuriset ja hallinnon toimintaan liittyvät edellytykset olla tässä edelläkävijä.

Case: Trustly ID – Biometrinen pilotti Suomessa

Trustly käynnisti maaliskuussa 2025 Suomessa biometrisen tunnistautumisen pilotin, joka mahdollistaa pankkitunnistautumisen kasvojentunnistuksella ilman erillistä pankkisovellusta. Pilotti testaa, miten biometrinen tunnistaminen voi yksinkertaistaa digitaalista asiointia säilyttäen samalla turvallisuuden.

Case: Digitaalinen ajamiseen oikeuttava todistus (DTC)

Suomessa kokeillaan digitaalista ajamiseen oikeuttavaa todistusta (Digital Tachograph Card, DTC), joka perustuu EU:n eIDAS-sääntelyyn. Kokeilu testaa, miten viralliset henkilöllisyystodistukset voidaan siirtää mobiililaitteisiin turvallisesti.

6.3 Suomen tie: yksityisyyden ja tehokkuuden tasapaino

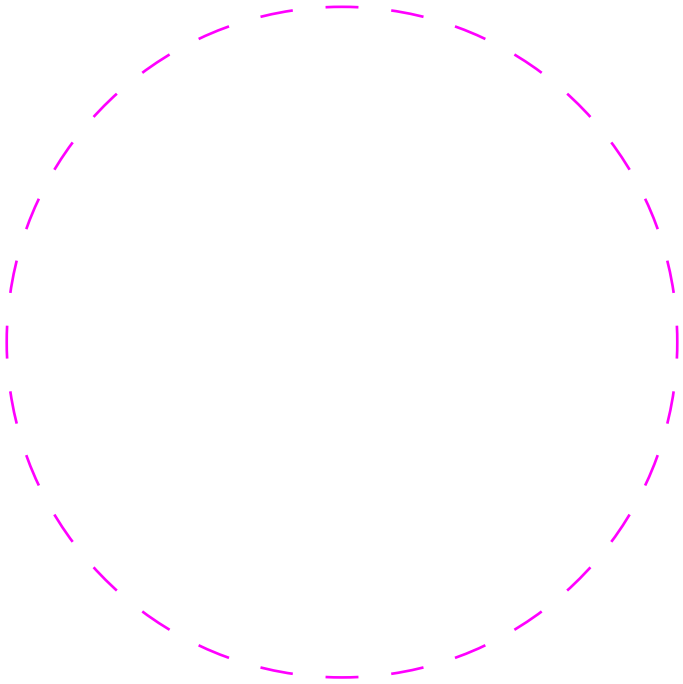
Biometristen järjestelmien käyttöönotto edellyttää huolellista yksityisyyden ja tehokkuuden tasapainottamista. Intian Aadhaar-esimerkki osoittaa sekä suuret mahdollisuudet (40 miljardin dollarin

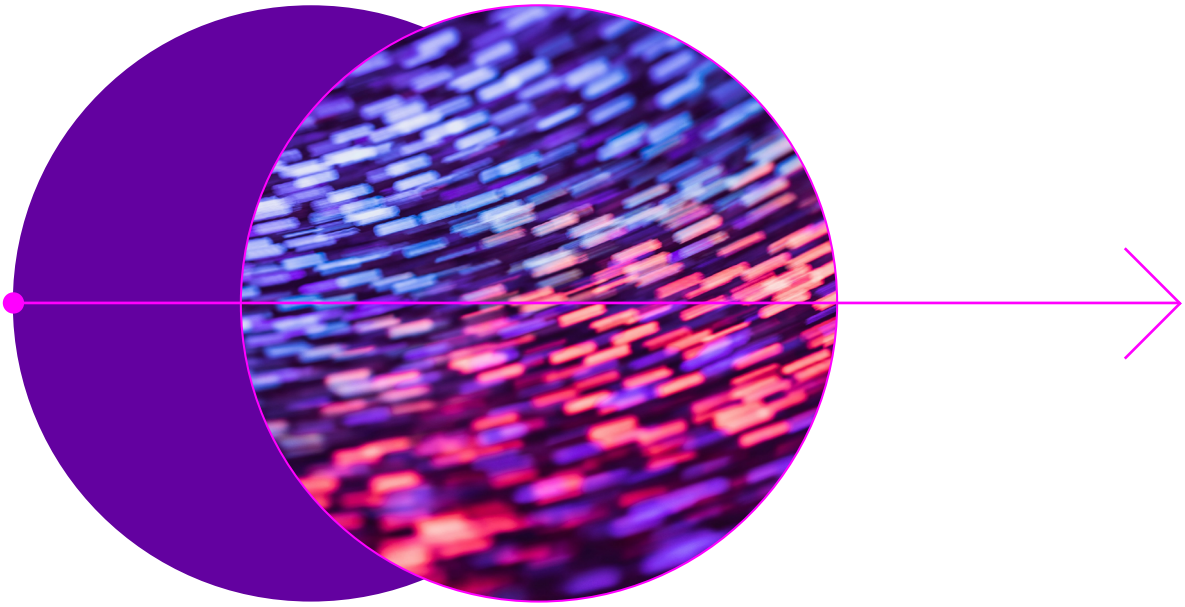
säästöt, väärinkäytösten vähentyminen) että riskit (syrjäytyminen, yksityisyysongelmat). Suomen tulee rakentaa järjestelmiä, jotka hyödyntävät yksityisyyssuojausteknologioita lähtökohtaisesti.

Nollatietotodistukset tarjoavat erityisen lupaavan mahdollisuuden. Niiden avulla voidaan todentaa esimerkiksi ikä, kansalaisuus tai luottotiedot ilman, että tarkkoja henkilötietoja tarvitsee paljastaa. Suomen vahva kryptografiaosaaminen tarjoaa hyvän pohjan näiden teknologioiden kehittämiselle ja käyttöönotolle.

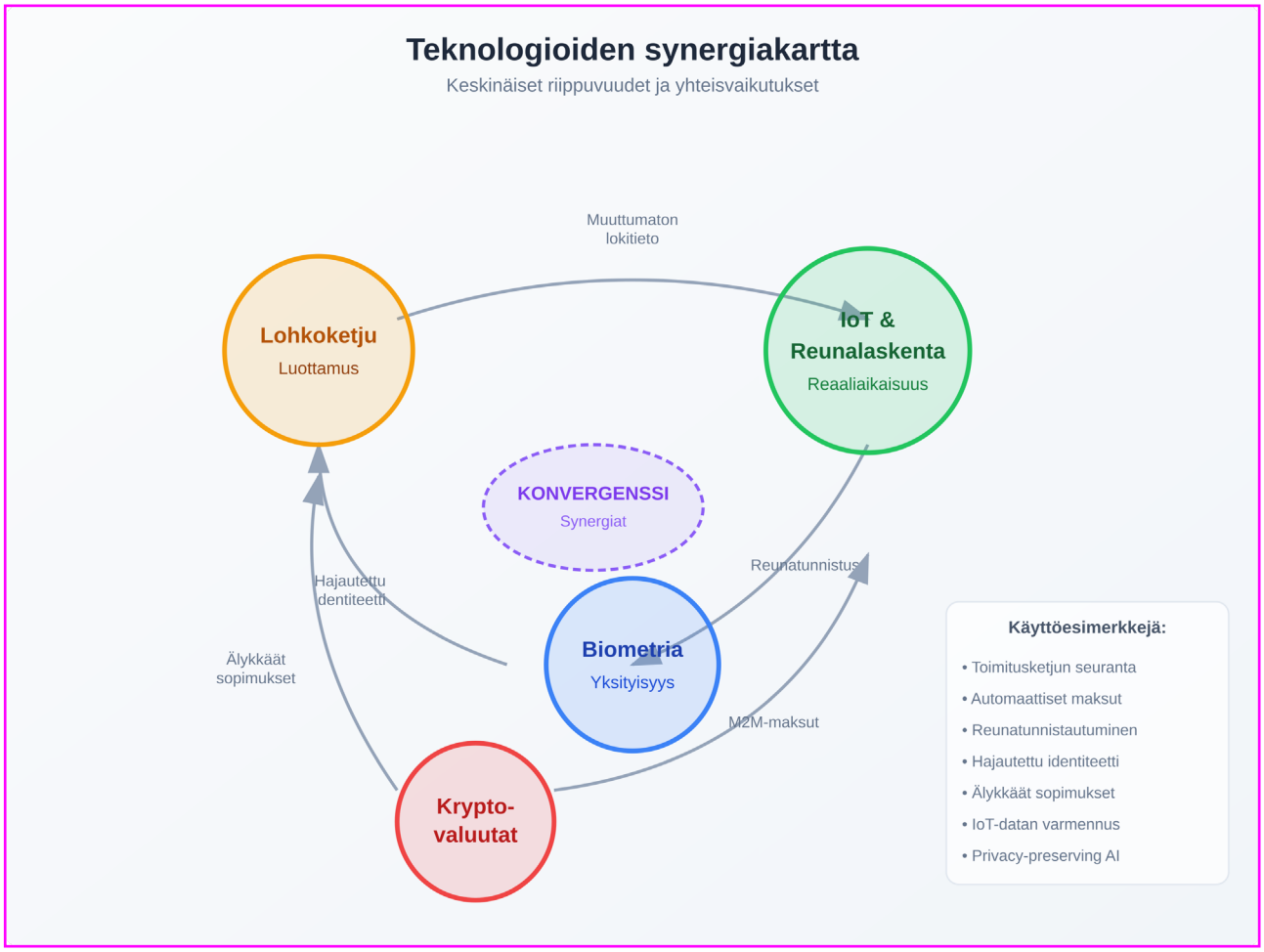
Nollatietotodistukset ja homomorfinen salaus ovat teknologian kehityksen ja adaptaation kehityskaarella vaiheessa, mikä on Suomelle ja suomalaisille yritykselle houkutteleva. Eettinen, periaatteellinen ja historiasta ponnistava kehitysote mahdollistavat niiden nivomisen osaksi Suomen tarinaa. Tämä tarjoaa kaikupohjaa myös liiketoiminnan kasvulle.

EU:n EUDI-lompakkokokeilut ovat jo käynnissä neljän suuren pilottihankkeen kautta, joissa testataan eurooppalaista digitaalista identiteettilompakkoa eri käyttötilanteissa. Suomi osallistuu näihin kokeiluihin Digi- ja väestötietoviraston (DVV) koordinoimana. Tilanne kehittyy nopeasti ja Suomen tulisi varmistaa aktiivinen osallistuminen pilottien seuraaviin vaiheisiin, jotta maa pysyy digitaalisen identiteetin kehityksen eturintamassa.





7. Paljon enemmän kuin osiensa summa: konvergenssi ja synergiat



Kuva 2. Teknologioiden synergiakartta: keskinäiset riippuvuudet ja yhteisvaikutukset

7.1 Teknologiat kietoutuvat yhteen

Selvityksessä tarkastellut neljä teknologia-aluetta eivät kehity erillisinä saarekkeina, vaan ne kytkeytyvät toisiinsa monin tavoin. Tämä teknologinen konvergenssi luo sekä uusia mahdollisuuksia että monimutkaisia haasteita. Politiikan ja sääntelyn näkökulmasta on olennaista ymmärtää teknologioiden keskinäiset riippuvuudet ja yhteisvaikutukset. On osattava arvioida myös lopputuloksia ja säännellä prosesseja. Katvealueet voivat tarjota lyhytaikaista liiketoimintaetua nopeille toimijoille, jotka etsivät voittoja distruptiosta, mutta yhteiskunnan kokonaisetua arvioidessa voi tämä tuottaa merkittäviä tappioita esimerkiksi yksityisyyden ja tietoturvallisuuden saroilla. Avointa vuoropuhelua kaikkien toimijodien välillä ja kapasiteetin vahvistamista tarvitaan.

Sitran teknologioiden konvergenssi -materiaalit korostavat, miten digitaalisen ja fyysisen maailman rajat hämärtyvät. Biometrinen tunnistaminen voi toimia avaimena lohkoketjupohjaiseen identiteettiin, reunalaskenta mahdollistaa IoT-laitteiden älykkään toiminnan, ja kryptovaluutat voivat toimia automaattisten maksujen välineenä älykkäissä sopimuksissa.

Näin dystooppinen tulevaisuudenkuva voidaan korvata realistisemmalla, missä pelot eivät ole liioiteltuja – vaan aitoihin riskeihin ja uhkiin on varauduttu. Digitaalisen ja fyysisen maailman rajojen hämärtyminen voidaan nähdä mahdollisuutena, jos teknologioiden yhteen kietoutumisen prosessi viipaloidaan ymmärrettäviin osakokonaisuuksiin.

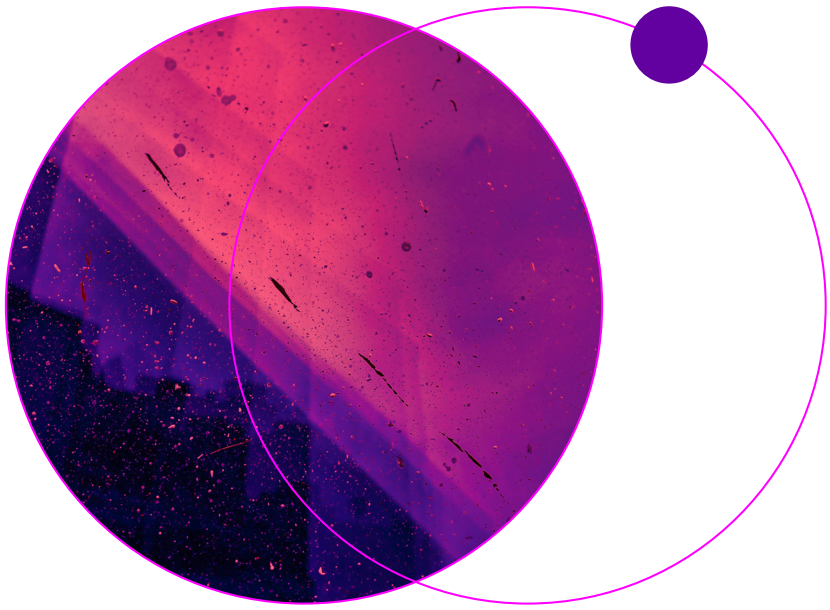
7.2 Neljä konkreettista synergiaa

Lohkoketju + IoT: IoT-laitteet voivat kirjata tietoja suoraan lohkoketjuun, luoden muuttumattoman lokitiedon esimerkiksi toimitusketjun tapahtumista tai ympäristömittauksista. Tämä yhdistelmä mahdollistaa automatisoituja, luotettavia järjestelmiä ilman keskitettyä valvontaa.

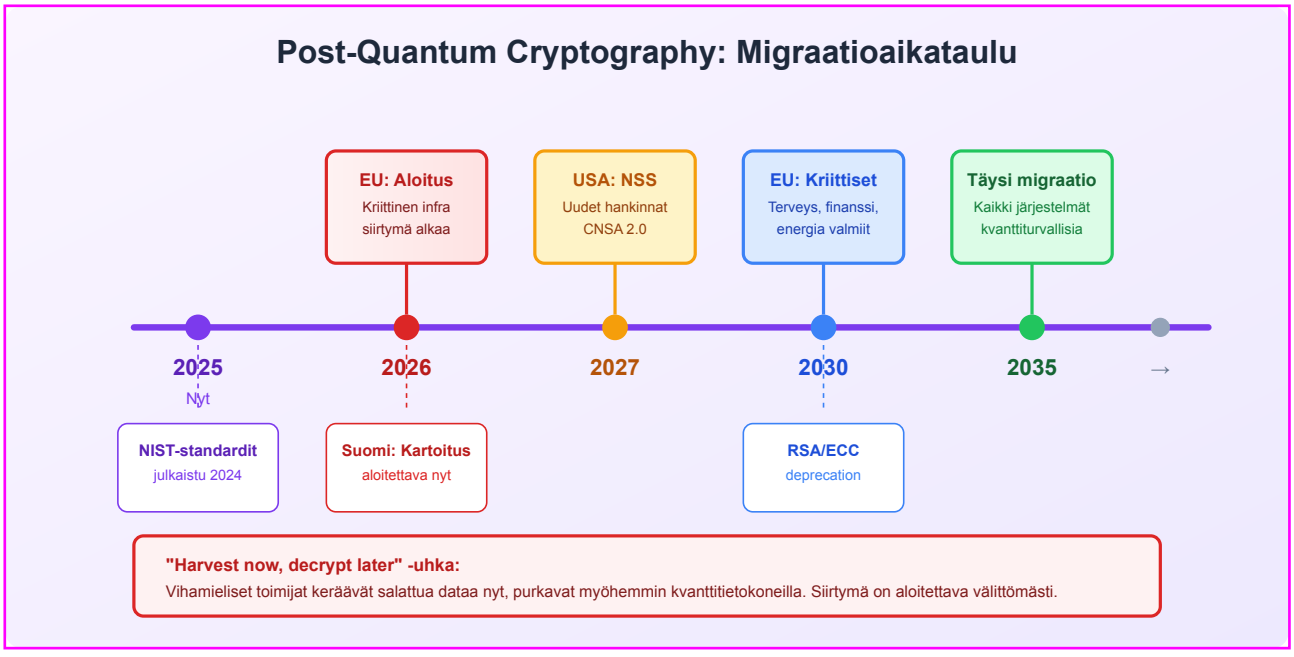
Reunalaskenta + biometria: Biometrinen tunnistaminen voidaan suorittaa reunalaitteessa, jolloin arkaluonteista biometristä dataa ei tarvitse siirtää keskitetyille palvelimille. Tämä parantaa yksityisyyttä ja nopeuttaa tunnistusta.

Kryptovaluutat + älykkäät sopimukset: Digitaaliset valuutat mahdollistavat automaattiset maksut älykkäissä sopimuksissa. Esimerkiksi IoT-sensori voi käynnistää automaattisen maksun, kun toimitus on vahvistettu – ilman inhimillistä välikättä.

Yksityisyyssuojausteknologiat + kaikki: Nollatietotodistukset ja homomorfinen salaus voivat parantaa yksityisyyttä kaikilla tarkastelluilla alueilla. Ne mahdollistavat datan hyödyntämisen ilman sen paljastamista.



8. Kvanttiuhka ja kvanttiturvallinen kryptografia – kauhea ja kiehtova kokonaisuus



Kuva 3. Post-Quantum Cryptography -migraation aikajana: kansainvälinen vertailu

8.1 Kerää nyt, murra myöhemmin

Kvanttitietokoneet tulevat lähivuosina saavuttamaan kykyjä, joilla voidaan murtaa nykyisin käytössä olevia salausmenetelmiä, erityisesti RSA- ja elliptisen käyrän kryptografiaa. Nämä suojaavat suurta osaa internetin tietoliikenteestä, pankkijärjestelmistä ja kriittisestä infrastruktuurista. Vaikka täy-

sin toimivat kvanttitietokoneet ovat vielä kehitysvaiheessa, 'kerää nyt, murra myöhemmin' (harvest now, decrypt later) -hyökkäykset ovat jo mahdollisia: vihamieliset toimijat voivat kerätä salattua dataa nyt ja purkaa sen myöhemmin kvanttitietokoneilla.

Tätä uhkaa kiihdyttää tekoälybuumin synnyttämä laskentakapasiteetin räjähdysmäinen kasvu. Maailmanlaajuiset investoinnit AI-datakeskuksiin ovat moninkertaistaneet saatavilla olevan tallennus- ja laskentakapasiteetin, ja osa analyytikoista arvioi investointien olevan ylimitoitettuja suhteessa lyhyen aikavälin kysyntään. Tämä tarkoittaa, että ylikapasiteetti tulee markkinoille ennennäkemättömän edullisesti – tehden massiivisesta datan keräämisestä ja pitkäaikaisesta säilyttämisestä taloudellisesti mahdollista paitsi valtiollisille toimijoille, myös järjestäytyneelle rikollisuudelle, hacktivistiryhmille ja yksityisille tiedustelupalveluille. "Kerää nyt, murra myöhemmin" -strategian kustannuskynnys on siten merkittävästi laskenut ja uhkamalli laajentunut juuri samalla kun kvanttilaskennan kehitys etenee kohti kryptografisesti merkittävää kyvykkyyttä.

8.2 EU:n määräajat lähestyvät – kello tikittää

EU on asettanut tiukan aikataulun kvanttiturvalliseen kryptografiaan siirtymiselle. Kriittisen infrastruktuurin – mukaan lukien energia, terveydenhuolto, finanssisektori ja julkishallinto – tulee siirtyä kvanttiturvallisiin salausmenetelmiin vuoden 2026 loppuun mennessä. Täydellinen migraatio kaikilla sektoreilla tulee tapahtua vuoteen 2035 mennessä.

Suomi on edennyt kvanttiturvallisen kryptografian (post-quantum cryptography, PQC) valmisteluissa EU:n keskitasoa nopeammin. Traficom on päivittänyt kansalliset kryptografiset vahvuusvaatimukset NISTin standardien mukaisiksi ja on edellyttänyt kvanttiturvallisten menetelmien käyttöä salaustuotearvioinneissa 1.1.2026 alkaen. Siirtymän toteutus organisaatiotasolla on kuitenkin vasta alkuvaiheessa, ja kriittisen infrastruktuurin kattava migraatio vuoden 2030 takarajaan mennessä vaatii merkittäviä resursseja ja koordinaatiota.

Yhdysvaltain NIST (National Institute of Standards and Technology) on standardoinut ensimmäiset PQC-algoritmit, mukaan lukien CRYSTALS-Kyber avaintenvaihtoon ja CRYSTALS-Dilithium digitaalisiin allekirjoituksiin. Nämä algoritmit perustuvat matemaattisiin ongelmiin, joita kvanttitietokoneiden ei uskota pystyvän tehokkaasti ratkaisemaan.

8.3 Vaara uhkaa – ja vaikutukset ovat laaja-alaisia

Lohkoketjut: Nykyiset lohkoketjut perustuvat elliptisen käyrän kryptografiaan, joka on haavoittuva kvanttihyökkäyksille. Lohkoketjujen siirtyminen kvanttiturvalliseen kryptografiaan on teknisesti haastavaa mutta välttämätöntä.

Kryptovaluutat: Bitcoin ja Ethereum käyttävät ECDSA-allekirjoituksia, jotka ovat haavoittuvia. Siirtymä kvanttiturvallisiin allekirjoituksiin edellyttää laajaa yhteisön konsensusta ja voi viedä vuosia.

IoT: Monet IoT-laitteet käyttävät kevyitä salausmenetelmiä, jotka ovat erityisen haavoittuvia. Laitteiden pitkä elinkaari (jopa 10–20 vuotta teollisuudessa) tekee päivittämisestä haastavaa.

Biometria: Biometriset järjestelmät tallentavat arkaluonteista dataa, jonka salaus on kriittistä. Kvanttiturvallinen salaus on erityisen tärkeää biometrisille järjestelmille.

8.4 Työ on aloitettava nyt

Suomen tulee aloittaa välittömästi kartoitus kriittisen infrastruktuurin valmiudesta kvanttiturvalliseen siirtymään. Traficomin tulisi koordinoida kansallista post-quantum cryptography -tiekarttaa yhteistyössä Kyberturvallisuuskeskuksen kanssa. Tutkimusrahoitusta tulisi kohdentaa kvanttiturvallisen kryptografian osaamiseen ja sovelluskehitykseen.

Suomi on investoinut kvanttiteknologiaan merkittävästi – VTT:lle on osoitettu 79 miljoonaa euroa (2024–2027) pilotointiympäristöön ja 70 miljoonaa euroa kvanttitietokoneen skaalaamiseen. IQM on kerännyt yli 600 miljoonaa euroa yksityistä rahoitusta. Kvanttilaitteiston osalta Suomi on Euroopan kärjessä.

Kvanttiturvallisen kryptografian (PQC) osalta Suomella on mahdollisuus nousta globaaliksi edelläkävijäksi. Suomi voisi perustaa 100 miljoonan euron kansallisen PQC-siirtymäohjelman vuosille 2026–2030:

Osa-alue	Rahoitus
Kriittisen infrastruktuurin kryptografinen inventaario ja migraatio	30 M€
PQC-pilottihankkeet julkishallinnossa, terveydenhuollossa ja finanssisektorilla	25 M€
Kansallinen PQC-osaamiskeskus (Center of Excellence)	20 M€
Pk-yritysten ja kuntasektorin siirtymätuki	15 M€
PQC-standardointi ja kansainvälinen vaikuttaminen	10 M€

Miksi 100 miljoonaa? Alankomaat on varannut 615 miljoonaa euroa kvanttiteknologiaan (väkiluku 17,5 miljoonaa), Iso-Britannia 2,5 miljardia puntaa (väkiluku 67 miljoonaa). Suhteutettuna väkilukuun Suomen 100 miljoonan euron PQC-ohjelma ylittäisi molemmat: se vastaisi noin 18 euroa per asukas, kun Alankomaiden panostus on noin 35 euroa ja Britannian noin 30 euroa per asukas koko kvanttisektorille – Suomen ohjelma kohdistuisi puhtaasti kryptografiseen siirtymään, joka on kriittisin ja aikasidonnaisin osa-alue.

Investointi maksaisi itsensä takaisin: yksikin estetty ”harvest now, decrypt later” -hyökkäys kriittiseen infrastruktuuriin tai valtionhallinnon tietojärjestelmiin voisi säästää satojen miljoonien eurojen vahingoilta ja luottamustappioilta. Samalla se viestisi Suomen painopisteistä ei vain kansallisessa teknologiastrategiassa vaan myös siinä, miten kokonaisturvallisuuden mallia ylläpidetään ja päivitetään vastaamaan muuttuvia uhkakuvia.

Vertailukohtana Viron e-Residency-ohjelma on vastaavan suuruusluokan investoinnilla tuottanut yli 100 miljoonaa euroa verotuloja ja houkutellut yli 103 000 e-kansalaista ympäri maailmaa – esimerkki siitä, miten strateginen digitaalinen investointi voi tuottaa merkittäviä suoria taloudellisia hyötyjä.

9. Miten Suomen tulisi toimia muutoksen keskellä?

9.1 Hyödynnetään nykyisiä mekanismeja

Selvityksen suositusten toimeenpanossa tulee hyödyntää olemassa olevia rakenteita ja mekanismeja. Suomen Akatemia vastaa tutkimusrahoituksesta ja voi kohdentaa rahoitusta selvityksen teknologia-alueille. Business Finland tukee innovaatioita ja voi rahoittaa yritysten kehityshankkeita näillä alueilla. Digitaalinen vuosikymmen -tavoitteet ja digitoimisto koordinoivat Suomen digitalisaatiokehitystä EU:n tavoitteiden mukaisesti. Perusrakenne on kunnossa.

9.2 Roolit selkeäksi

Eri toimenpiteille on tunnistettava sopivat koordinoivat tahot:

- Valtiovarainministeriö (VM) toimii julkisen hallinnon pilottien ja digitalisaatiohankkeiden koordinoijana
- Valtioneuvoston kanslian (VNK) strategiatoiminto paneutuu laajempaan sääntelyn uudistamiseen ja kokeilukulttuurin vahvistamiseen
- Traficom koordinoi kyberturvallisuustoimintamallia osana olemassa olevaa kyberturvallisuusstrategiaa
- Tutkimus- ja innovaationeuvosto (TIN) toimii pääministeritasoisena neuvontaelimenä teknologiastrategian linjauksissa
- Liikenne- ja viestintäministeriö (LVM) toimii digitaalisen infrastruktuurin ja datatalouden vastuuministeriönä, koordinoiden viestintäverkkojen, 5G/6G-teknologioiden, pilvipalveluiden ja dataväylien kehittämistä sekä näiden sääntelykehyksen valmistelua. LVM vastaa myös liikenteen digitalisaatiosta ja liikennesektorin kriittisen infrastruktuurin kyberresilienssistä.

9.3 Kokonaisuuden hallinta

Teknologioiden konvergenssi edellyttää ekosysteemistä lähestymistapaa sääntelyyn ja politiikkaan. Yksittäisten teknologioiden erillinen sääntely voi johtaa ristiriitaisuuksiin ja innovaatioiden hidastumiseen. Suomen tulisi kehittää horisontaalista sääntelyosaamista, joka tunnistaa teknologioiden yhteisvaikutukset.

Tutkimus- ja innovaationeuvosto (TIN), pääministerijohtoinen neuvontaelin, voisi toimia koordinoivana tahona teknologioiden konvergenssin hyödyntämisessä. Rahoitusta tulisi kohdentaa hankkeisiin, jotka yhdistävät useita teknologia-alueita ja tuottavat synergiaetuja.

Digitaalinen vuosikymmen -tavoitteet ja digitoimisto koordinoivat Suomen digitalisaatiokehitystä EU:n tavoitteiden mukaisesti. Digitoimiston roolia tulisi vahvistaa erityisesti teknologioiden konvergenssin hallinnassa, jotta Suomi voi hyödyntää eri teknologia-alueiden yhteisvaikutuksia tehokkaasti.

Rahoitusta tulisi myös kohdistaa sellaisiin hankkeisiin, missä pureudutaan konvergenssin yhteiskunnallisiin vaikutuksiin läpileikkaavasti. Eettiset ja filosofiset arviot, teknologiaa ymmärtävä koulutus- ja sosiaalipoliittinen tutkimus sekä sosiologinen kokonaisnäkemys muutoksen vaikutuksista ovat esimerkkejä hankkeista, jotka voivat tukea poliittista valmistelua. Laajempi katsantokanta vahvistaa myös liiketoiminnan edellytyksiä tuottaa korkeamman lisäarvon tuotteita ja palveluja.

9.4 Kyberturvallisuusstrategia ja Tuutti näyttävät tietä

Suomella on jo olemassa oleva kyberturvallisuusstrategia. Selvityksessä ehdotettu toimintamalli tulee kytkeä sen alle, ei luoda rinnakkaista strategiaa. Kyberstrategia toimii sateenvarjona, johon konkreettinen tekeminen kiinnitetään. Traficomin Kyberturvallisuuskeskus koordinoi toimintamallin kehittämistä yhteistyössä ministeriöiden ja toimijoiden kanssa.

Tuutti-hankkeen (Turvallinen ja uskottava tietoyhteiskunta) tilanne tulee kartoittaa ja varmistaa, että selvityksen suositukset täydentävät jo käynnissä olevia toimia.

Samalla on tunnistettava, että nykyinen kyberturvallisuusstrategia ei välttämättä kata riittävästi uusien teknologioiden – kuten kvanttiturvallisen kryptografian, lohkoketjujen ja tekoälyn – tuomia mahdollisuuksia ja uhkia. Kansainväliset esimerkit osoittavat, että edelläkävijämaat ovat laatineet erillisiä teknologiastrategioita kyberstrategian rinnalle: Iso-Britannia julkaisi kansallisen kvanttistrategian (2023), Alankomaat perusti Quantum Delta NL -ohjelman, ja Singapore on yhdistänyt kyber- ja teknologiastrategiansa Smart Nation -kehykseen. Suomen tulisi osoittaa rohkeutta päivittää kyberstrategian tavoitetasoa vastaamaan 2020-luvun teknologista murrosta – tai tarvittaessa täydentää sitä erillisellä uusien teknologioiden tiekartalla, joka tuo konkretiaa ja kunnianhimoa olemassa olevan kehyksen sisälle.

9.5 Piloteista pysyvään toimintaan

Pelkät pilottihankkeet eivät riitä. Pilottien kautta täytyy päästä juurisyihin purkamaan sääntelyn esteitä, muokkaamaan toimintaympäristöä ja luomaan pysyviä toimintamalleja. Pilotit tulisi ajatella osana laajempaa kokonaisuutta, kuten sandbox-ympäristöinä tai kehittämishankkeina, joiden tulokset siirtyvät osaksi normaalia toimintaa.

Suomen tulisi ottaa käyttöön ”pilotista pysyväksi” -malli (pilot-to-permanent framework), jossa onnistuneiden kokeilujen siirtyminen normaalitoiminnaksi on sisäänrakennettu prosessiin alusta alkaen. Mallissa määritellään etukäteen selkeät kriteerit – esimerkiksi käyttäjämäärä, turvallisuusvaatimukset, kustannustehokkuus ja yhteensopivuus EU-sääntelykehyksen kanssa – joiden täyttyessä

kokeilu siirtyy automaattisesti seuraavaan vaiheeseen. Samalla käynnistyy nopeutettu säädösvalmistelu, jossa tarvittavat lainsäädäntömuutokset valmistellaan rinnakkain pilotin arvioinnin kanssa, ei vasta sen päätyttyä.

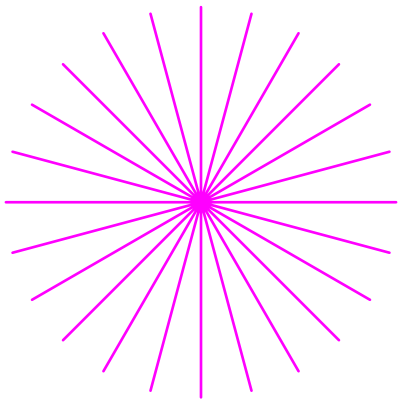
Vertailukohtana voidaan hyödyntää esimerkiksi Iso-Britannian Financial Conduct Authorityn (FCA) regulatory sandbox -mallia, jossa onnistuneet fintech-pilotit ovat siirtyneet täyteen toimilupaan keskimäärin 6–12 kuukaudessa. Vaikka FCA:n malli on sektorikohtainen, sen keskeiset periaatteet – ennalta määritellyt onnistumiskriteerit, aikarajat ja automaattinen etenemispolku – ovat sovellettavissa laajemminkin Suomen julkishallinnon ja teknologiakokeilujen kontekstiin. Tällainen ennustettavuus poistaisi ”pilottihautausmaa”-ilmiön, jossa lupaavat kokeilut päättyvät raporttiin mutta eivät koskaan skaalaudu.

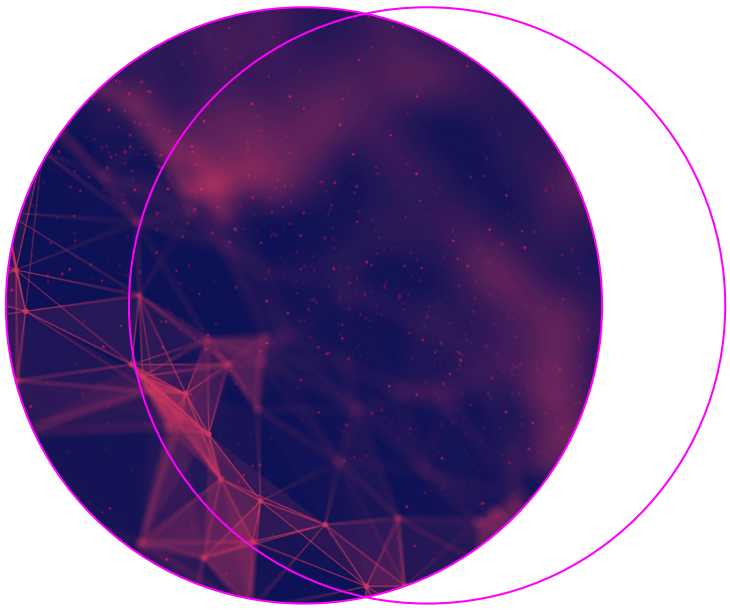
Yhteistyötä tulee etsiä sekä valtion hallinnon että kaupunkien tasolla. EU-hankerahoituksen hyödyntäminen ja hankkeiden kytkeminen EU-tason tavoitteisiin on tärkeää sekä rahoituksen että vaikuttavuuden kannalta.

9.6 Pyöreän pöydän keskusteluista jaettuun tilannekuvaan

Selvitys suosittaa pyöreän pöydän keskustelujen käynnistämistä keskeisillä teknologia-alueilla. Nämä keskustelut kokoaisivat yhteen sijoittajat, kasvuyritykset, vakiintuneet yritykset, tutkijat, kansalaisyhteiskunnan edustajat ja päättäjät. Tavoitteena on luoda yhteinen ymmärrys teknologioiden mahdollisuuksista ja riskeistä sekä tunnistaa konkreettisia toimenpiteitä.

VM:n rahoitusmarkkinaosasto voisi luoda pysyvän toimintamallin kryptovaluuttoihin ja digitaalisiin valuuttoihin liittyvälle sidosryhmäyhteistyölle. Viime aikoina käynnistetyt keskustelufoorumit ovat osoittaneet alan toimijoiden kiinnostuksen ja tarpeen jatkuvalle vuoropuhelulle. Rahoitusmarkkinaosasto voisi institutionalisoida tämän mallin säännölliseksi, esimerkiksi neljännesvuosittaiseksi pyöreän pöydän formaatiksi, jonka tavoitteena on selkeyttää MiCA-asetuksen implementointia, kartoittaa yritysten näkemyksiä sääntelyympäristöstä ja tunnistaa lainsäädännön kehitystarpeita ennakoivasti. Kuten selvityksessä on jo edellä todettu, on kryptovaluuttasektoria koskeva asennemuutos ja rytminmuutos välttämätöntä Suomelle.





10. Suomi Euroopan ytimessä

10.1 EU-tason hankkeet Horizon ja Digital Europe

Suomen tulee aktiivisesti osallistua EU-tason hankkeisiin kaikilla selvityksen teknologia-alueilla. Horizon Europe -ohjelman Digital, Industry and Space -klusteri rahoittaa tutkimusta reunalaskennasta, IoT:stä, lohkoketjuteknologioista ja kyberturvallisuudesta. Digital Europe -ohjelma tukee käytännön sovelluksia ja osaamisen kehittämistä.

EBSI (European Blockchain Services Infrastructure) on EU:n lohkoketjuinfrastruktuurihanke, johon Suomen tulisi osallistua aktiivisesti. Hanke kehittää rajat ylittäviä lohkoketjupohjaisia palveluita, kuten diplomien todentamista ja yritysten rajat ylittävää tunnistautumista.

Case: EBSI ja rajat ylittävä tutkintojen todentaminen

EU:n EBSI-infrastruktuurissa 11 yliopistoa 11 maasta on pilotoinut lohkoketjupohjaista tutkintojen varmentamista vuodesta 2021. Tutkintotodistukset myönnetään kryptografisesti suojattuina ”Verifiable Credentials” -muodossa, jotka työnantaja tai toinen yliopisto voi verifioida välittömästi ilman yhteydenottoa myöntäneeseen oppilaitokseen. Ranskan Lillen yliopisto on jo ottanut järjestelmän tuotantokäyttöön. Suomen korkeakoulut ja Opetushallitus voisivat pilotoida vastaavaa rajat ylittävää todentamista Pohjoismaiden tai Baltian maiden kanssa.

10.2 Pohjoismaat ja Baltia keskeisinä kumppaneina

Pohjoismaat ja Baltia tarjoavat luonnollisen yhteistyökehyksen. Viron e-hallinto-osaaminen, Ruotsin finanssiteknologiaekosysteemi ja Tanskan cleantech-innovaatiot täydentävät Suomen vahvuuksia. Yhteispohjoismaisia pilotteja voitaisiin käynnistää esimerkiksi rajat ylittävässä digitaalisessa identiteetissä ja toimitusketjujen seurannassa.

Suomi voisi ehdottaa Pohjoismaat–Baltia-yhteistyön syventämistä uusien teknologioiden ja digitaalisen resilienssin alueella – ei uutena koordinaatiomekanismina, vaan olemassa olevien rakenteiden (NORDEFCO, Nordic Innovation, NB8) puitteissa. Yhteistyö tulisi fokusoida 1–2 konkreettiseen osa-alueeseen, kuten kvanttiturvalliseen viestintään ja rajat ylittävään digitaaliseen identiteettiin, joissa pohjoinen ulottuvuus luo aitoja turvallisuus- ja skaalahyötyjä.

Siviili- ja puolustussektorin kytkös on luonteva, mutta sen ei tule hidastaa siviilipuolen ketteriä hankkeita. Mallina voi hyödyntää olemassa olevia rakenteita: Patria CAVS osoittaa Pohjoismaiden kyvyn kehittää yhteisiä teknologia-alustoja, ja Joint Expeditionary Force (JEF) tarjoaa operatiivisen yhteistyökehyksen. Käytännössä Suomi voisi ottaa vetovastuun konkreettisesta pilotista – esimerkiksi Suomi–Viro-kvanttiturvallisesta viestintäyhteydestä – ja kutsua muut maat mukaan tulosten pohjalta. Tämä ”pilotista laajenevaan yhteistyöhön” -lähestymistapa välttää pohjoismaisen yhteistyön tyypillisen sudenkuopan, jossa strategiapaperit eivät johda toimintaan.

10.3 Oppeja ja kilpailuetua maailmalta – startti Singaporessa

Kahdenvälinen yhteistyö valittujen maiden kanssa voi edistää osaamisen vaihtoa ja konkreettisten hankkeiden käynnistämistä. Suomen tulisi priorisoida kumppaneita, jotka tarjoavat täydentävää osaamista ja strategista arvoa digitaalisen resilienssin näkökulmasta:

Sveitsi (Crypto Valley, Zug): Zugin kantonissa toimii yli 1 100 lohkoketjuyritystä, ja alueen yhteenlaskettu markkina-arvo on 593 miljardia dollaria. Sveitsin menestys perustuu teknologianeutraaliin sääntelyyn, selkeään verokohteluun ja FINMA:n ennakoiviin linjauksiin. Suomi voisi solmia kahdenvälisen oppimiskumppanuuden sääntelyviranomaisten tasolla – esimerkiksi Finanssivalvonnan ja FINMA:n välille.

Israel: Maailman johtava kyberturvallisuusekosysteemi – yli 450 kyberturvallisuusyritystä, joista monet Unit 8200 -taustaisia. Vuonna 2024 Israel jakoi uhkatiedustelua 42 maan kanssa. Suomi voisi syventää kyberturvallisuusyhteistyötä erityisesti kriittisen infrastruktuurin suojauksen ja kvanttiturvallisen salauksen alueilla. Huomioitava kuitenkin geopoliittiset jännitteet ja EU-Israel-suhteen epävarmuudet.

UAE (Dubai): Kunnianhimoisin lohkoketjun julkisen sektorin soveltaja – tavoitteena maailman ensimmäinen täysin lohkoketjupohjainen kaupunki. UAE on houkutellut yli 70 lisensoitua virtuaaliomaisuuspalveluntarjoajaa ja 25 miljardia dollaria investointeja. Kiinnostava kumppani lohkoketjupohjaisten julkisten palveluiden benchmarkingiin, joskin arvopohjainen yhteistyö vaatii harkintaa.

Kenia (”Silicon Savannah”): M-Pesa-mobiilimaksualusta tavoittaa 61 miljoonaa päivittäistä transaktiota. Yli 70 % aikuisista käyttää mobiilirahaa – maailman korkein penetraatio. Kenian Virtual Asset Service Provider Bill (2025) on luonut oikeudellisen pohjan kryptovaroille. Suomi voisi ottaa oppia mobiilimaksujen käytöstä ja finanssi-inkluusion malleista, jotka soveltuvat myös harvaan asuttujen alueiden digitaalisiin palveluihin.

Ruanda: Kansallinen fintech-strategia 2024–2029, Irembo-alusta tarjoaa yli 100 e-hallinnon palvelua. Startup-rahoitus kasvoi 75 % vuonna 2024. Kiinnostava kumppani kehitysyhteistyön ja digitaalisen hallinnon yhdistämiseen – Suomella on jo vahvat kehitysyhteistyösuhteet alueella.

Nigeria: Afrikan suurin startup-ekosysteemi (9,8 miljardia dollaria), Zone-yritys on kehittänyt Afrikan ensimmäisen säännellyn lohkoketjupohjaisen maksuverkon. Nigeria johtaa Afrikan kryptotransaktioissa (59 miljardia dollaria 2023–2024). Keskuspankki on lanseerannut oman CBDC:n (eNaira). Potentiaalinen kumppani CBDC-kokemusten vaihtoon ja fintech-innovaatioihin.

Ensisijainen bilateraalikumppani: Singapore

Edellä mainitut ovat kaikki hyvin potentiaalisia kumppaneita. Digitaalisen resilienssin vahvistamista silmällä pitäen luontevaa olisi lähteä liikkeelle Singaporesta. Maa on rakentanut maailman edistyneimmän kokonaismallin, mikä yhdistää kyberturvallisuuden, digitaalisen hallinnon ja innovaatioekosysteemin toisiaan tukevaksi kokonaisuudeksi – Smart Nation -kehyksessä.

Suomi ja Singapore jakavat samankaltaisen profiilin: pieni, avoin talous, korkea koulutustaso ja vientivetoinen elinkeinorakenne. Singapore on kuitenkin tehnyt erilaisia strategisia valintoja, joista Suomi voi oppia. Singaporen Cyber Security Agency (CSA) on solminut bilateraalit kyberturvallisuusdialogit muun muassa Yhdysvaltojen, Britannian ja Malesian kanssa, ja maa toiki Counter Ransomware Initiative (CRI) -huippukokouksen isäntänä lokakuussa 2025. Nyt olisi luonteva hetki Suomelle rakentaa tiivimpää yhteistyötä Singaporen kanssa.

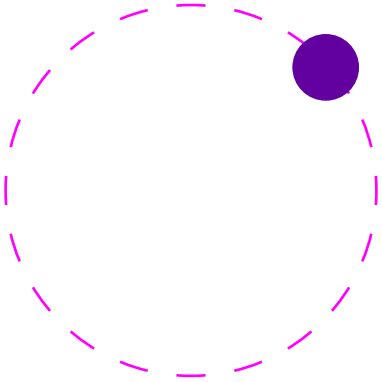
Konkreettisina askeleina Suomi voisi:

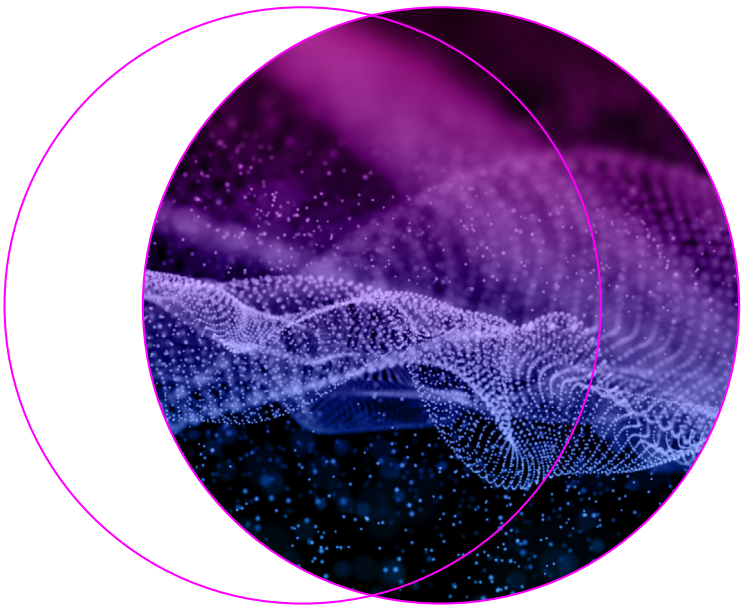
- Ehdottaa kahdenvälisen kyberturvallisuusdialogin käynnistämistä Traficomin Kyberturvallisuuskeskuksen ja Singaporen CSA:n välille
- Käynnistää virkamiestason oppimisvaihdon Smart Nation -mallin soveltamisesta Suomen kontekstiin

On huomioitava, että Singaporen malli ei ole suoraan kopioitavissa – maan hallintokulttuuri ja oikeusjärjestelmä eroavat suomalaisesta. Yhteistyön tuleekin olla oppimiskumppanuus, jossa tunnistetaan Suomeen sovellettavissa olevat elementit.

Täydentävä bilateraalikumppani: Japani

Japani on luonnollinen täydentävä kumppani Suomelle digitaalisen resilienssin vahvistamisessa. Maiden välillä on jo valmiiksi hyvät suhteet, ja Japani on panostanut merkittävästi kyberturvallisuuteen ja kvanttiteknologiaan. Japanin National Institute of Information and Communications Technology (NICT) on kehittänyt edistyneitä kvanttisalausjärjestelmiä, ja maa on sitoutunut kriittisen infrastruktuurin kvanttiturvalliseen siirtymään. Konkreettisia yhteistyömahdollisuuksia ovat kvanttiturvallisen kryptografian yhteiskehitys, IoT-turvallisuusstandardien harmonisointi sekä 6G-tutkimusyhteistyön laajentaminen kyberturvallisuusdimensiolla.





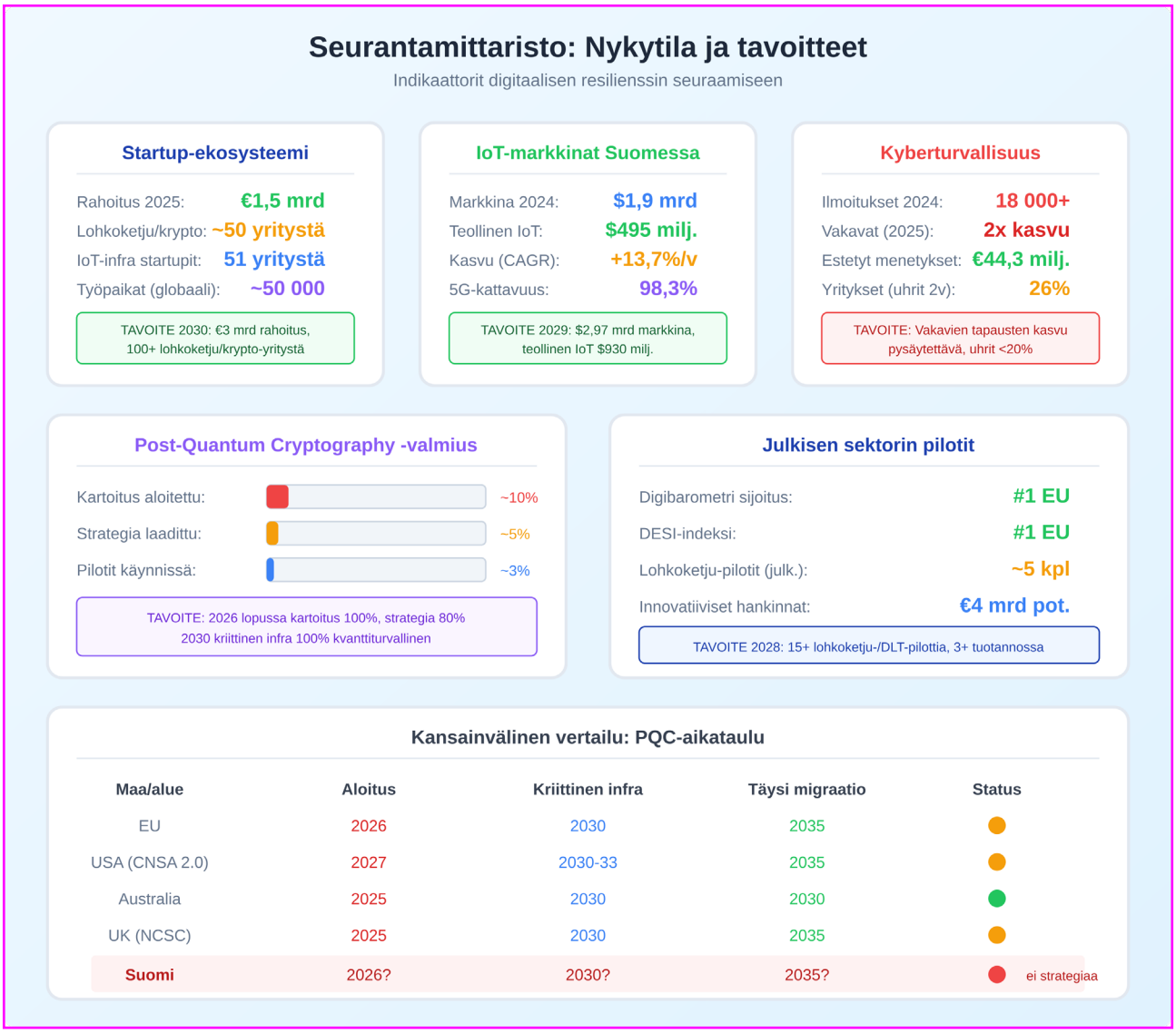
11. Miten mittaamme edistymistämme?

11.1 Tavoitteena prosessi, ei lopputulos

Perinteinen selvitystyö on usein tähdännyt ’lopulliseen’ dokumenttiin, mikä arkistoidaan valmistuttuaan. Teknologioiden nopea kehitys kyseenalaistaa tämän lähestymistavan. Onko tarvetta lopullisuudelle muuttuvassa ajassa?

Tavoitteena on, että tämä selvitys laajenee jatkuvasti päivittyväksi ’eläväksi dokumentiksi’. Työn arvo syntyy prosessista, jossa sidosryhmät kokoontuvat säännöllisesti päivittämään tilannekuvaa ja arvioimaan suosituksia. Dokumentti arkistoidaan vasta kun sen kysymyksenasettelu on vanhentunut ja prosessi – ei vain dokumentti – päätetään lopettaa. Agenttipohjaiset LLM-ratkaisut mahdollistavat jatkuvan arvonluonnin ja prosessin ylläpidon kohtuullisin voimavaroin.

Mittaristo palvelee kahta tarkoitusta: se tarjoaa konkreettisen pohjan keskustelulle ja mahdollistaa edistymisen seurannan ajan yli. Tavoitteet eivät ole kiveen hakattuja – myös ne päivittyvät osana prosessia.



Kuva 4. Seurantamittariston dashboard: nykytila ja tavoitteet

11.2 Kasvun mittarit

Nykytila (2025)

- Suomalaiset startupit keräsivät vuonna 2025 yhteensä 1,5 miljardia euroa rahoitusta – ennätysmäärä
- Startup-lähtöiset yritykset tuottavat yli 12,5 miljardia euroa liikevaihtoa
- Työpaikat: lähes 50 000 maailmanlaajuisesti
- IoT-infrastruktuurin startupit: 51 yritystä, joista 20 merkittävästi rahoitettuja
- Lohkoketju/krypto-yritykset: arvio ~50 yritystä (tarkka kartoitus tarpeen)
- Merkittäviä rahoituskierroksia: Oura 777 M€, IQM 275 M€

Tavoitteet (2030)

- Startup-rahoitus: 3 miljardia euroa vuodessa
- Lohkoketju/krypto-yritykset: 100+ yritystä Suomessa
- Vähintään 3 suomalaista ’unicornia’ (>1 mrd arvostus) tarkasteltavilta teknologia-alueilta
- Suomi top-3 Euroopassa pääomasijoituksissa suhteessa BKT:hen (nyt #1)

11.3 Esineiden internetin kasvu

Nykytila (2024–2025)

- Suomen IoT-markkinan koko: 1,9 miljardia dollaria (2024)
- Teollinen IoT: 495 miljoonaa dollaria
- Kasvu (CAGR 2024-2029): 13,7 % vuodessa
- 5G-kattavuus kotitalouksista: 98,3 %
- Elisan standalone 5G-ydin lanseerattu 2025 – ensimmäinen Suomessa, joka mahdollistaa network slicing -toiminnallisuuden eli virtuaalisten, käyttötarkoituskohtaisten verkkoviipaleiden luomisen samasta fyysisestä infrastruktuurista.
- IoT-palveluyritysten rahoitus: 2,97 miljoonaa dollaria (72 yritystä, Tracxn IoT-Services)

Tavoitteet (2029)

- IoT-markkinan koko: 2,97 miljardia dollaria
- Teollinen IoT: 930 miljoonaa dollaria
- Suomi top-3 EU:ssa teollisen IoT:n hyödyntämisessä
- Network slicing -palvelut laajassa käytössä teollisuudessa

11.4 Kyberturvallisuusuhkien torjunta

Nykytila (2024-2025)

- Kyberturvallisuuskeskukselle ilmoitetut tapaukset 2024: yli 18 000
- Automaattisesti käsitellyt ilmoitukset: noin 185 000
- Vakavien tapausten määrä 2025: yli kaksinkertaistunut edelliseen vuoteen
- Pankkien estämät menetykset 2024: 44,3 miljoonaa euroa
- Yritykset, jotka tunnistaneet tietoturvatapahtuman (2 v aikana): 26 %
- 60 % suomalaisista huolissaan kyberhyökkäyksistä (Digiturvabarometri 2025)
- 51 % uskoo Suomen olevan hyvin varautunut

Tavoitteet

- Vakavien tapausten kasvun pysäyttäminen ja kääntäminen laskuun
- Tietoturvatapahtuman kokeneiden yritysten osuus: alle 20 %
- Estettyjen menetysten nostaminen 100 miljoonaan euroon (pankit)
- Kansalaisten luottamus kyberturvallisuuteen: yli 60 % kokee Suomen hyvin varautuneeksi

Kuva 5. Riskimatriisi: todennäköisyys vs. vaikutus keskeisille riskeille

11.5 Kvanttiturvallinen Suomi

Nykytila (tammikuu 2026)

- Kartoitus aloitettu: arvio ~10 % organisaatioista kriittisessä infrastruktuurissa
- PQC-strategia laadittu: arvio ~5 % organisaatioista
- Pilotit käynnissä: arvio ~3 % organisaatioista
- Suomella ei kansallista PQC-strategiaa tai tiekarttaa
- NIST-standardit (CRYSTALS-Kyber, CRYSTALS-Dilithium) julkaistu 2024

Kansainvälinen vertailu

Eri maiden aikataulut PQC-migraatioon:

- EU: Siirtymä alkaa 2026, kriittinen infra 2030, täysi migraatio 2035
- USA (CNSA 2.0): Uudet hankinnat 2027, ohjelmistot 2030, täysi migraatio 2035
- Australia: Täysi valmius 2030
- UK (NCSC): Tavoite 2035
- Suomi: Ei julkistettua aikataulua – jäljessä verrokkimaista

Tavoitteet Suomelle

- 2026 Q1: Kansallinen PQC-strategia ja tiekartta julkaistu
- 2026 lopussa: Kartoitus 100 %, strategia 80 % kriittisestä infrastruktuurista
- 2030: Kriittinen infrastruktuuri 100 % kvanttiturvallinen
- 2035: Täysi migraatio kaikilla sektoreilla

11.6 Valtio näyttää suuntaa

Nykytila

- Digibarometri-sijoitus: #1 EU (digitalisaation hyödyntäminen)
- DESI-indeksi: #1 EU (Digital Economy and Society Index)
- Lohkoketju-pilotit julkisella sektorilla: arvio ~5 kpl (tarkka kartoitus tarpeen)
- Innovatiivisten hankintojen potentiaali: 4 miljardia euroa
- Julkisten hankintojen kokonaisvolyymi: 47 miljardia euroa (20 % BKT:sta)

Tavoitteet (2028)

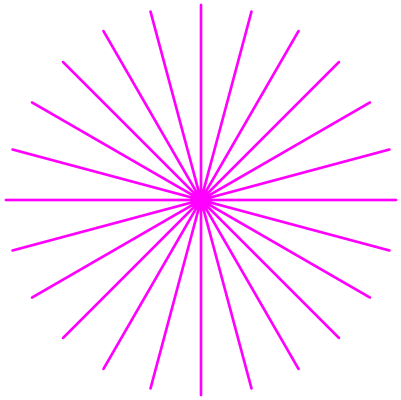
- Lohkoketju/DLT-pilotteja: 15+ käynnissä
- Tuotannossa olevia lohkoketjuratkaisuja: vähintään 4
- Vähintään yksi laaja julkisen rekisterin lohkoketjupilotti käynnistetään – esimerkiksi ajoneuvorekisterissä, missä lohkoketju mahdollistaisi ajoneuvojen omistushistorian, huoltokirjan ja maahantuontitietojen luotettavan seurannan läpi koko elinkaaren
- Sandbox-ympäristö toiminnassa teknologiapiloteille
- Sandbox-kokeiluihin sisäänrakennettu ”pilotista pysyväksi” -automaatio: ennalta määritellyt kriteerit, joiden täyttyessä siirtymä normaalitoimintaan käynnistyy automaattisesti nopeutetun säädösvalmistelun kanssa

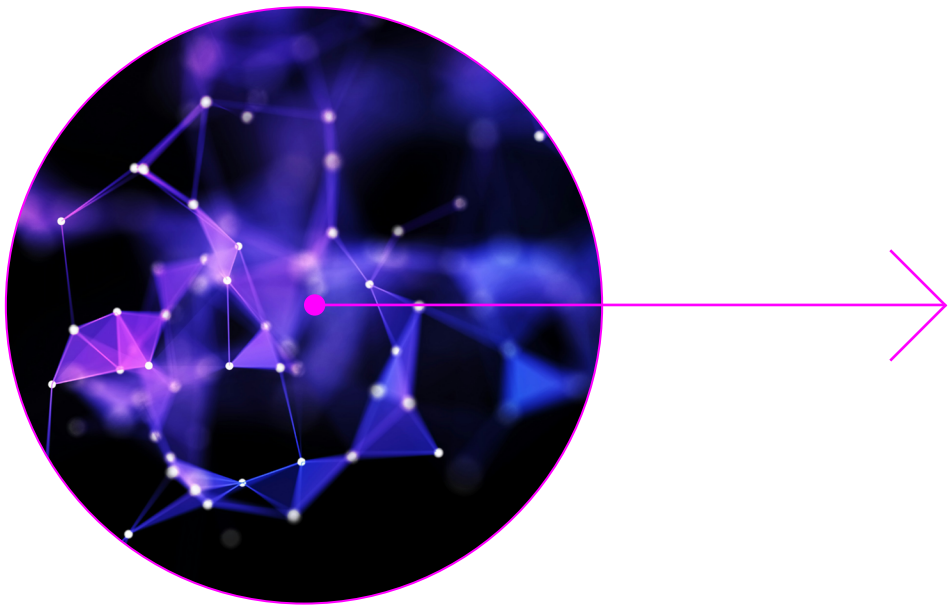
11.7 Mittariston päivitysprosessi

Mittaristoa päivitetään osana selvityksen puolivuosittaista päivitysprosessia. Päivityksessä:

- Kerätään tuoreimmat tilastotiedot Tilastokeskukselta, Traficomilta ja muista lähteistä
- Arvioidaan tavoitteiden saavuttamista
- Tarvittaessa päivitetään tavoitteita muuttuneen tilanteen mukaan
- Dokumentoidaan merkittävät muutokset ja niiden syyt

Mittariston ylläpidosta vastaa LVM yhteistyössä VM:n, Traficomin ja muiden sidosryhmien kanssa.





12. Mitä seuraavaksi

12.1 Käynnistetään heti

- Käynnistä kartoitus kriittisen infrastruktuurin valmiudesta kvanttiturvalliseen siirtymään (Traficom, Kyberturvallisuuskeskus)
- Käynnistä pyöreän pöydän keskustelut kryptovaluuttasääntelystä ja luo pysyvä neljännesvuosittainen foorumi MiCA-implementoinnin seurantaan (VM rahoitusmarkkinaosasto)
- Kytke selvityksen suositukset olemassa olevaan kyberturvallisuusstrategiaan ja arvioi strategian päivitystarpeet uusien teknologioiden osalta (Traficom)
- Kartoita Tuutti-hankkeen tilanne ja synergiat (LVM)
- Ehdota kahdenvälisen kyberturvallisuusdialogin käynnistämistä Singaporen kanssa (Traficom, UM)
- Laadi kansallinen PQC-strategia ja tiekartta (Traficom, Kyberturvallisuuskeskus)

12.2 Käynnistetään vuoden kuluessa

- Käynnistä lohkoketjupohjaisen rekisterin pilotti julkishallinnossa – ensisijaisesti ajoneuvorekisterissä (Traficom) tai tutkintorekisterissä EBSI-yhteensopivasti (Opetushallitus)
- Kehitä sandbox-ympäristö teknologiapiloteille, johon sisäänrakennetaan ”pilotista pysyväksi” -mekanismi: ennalta määritellyt onnistumiskriteerit ja automaattinen siirtymäpolku normaalitoimintaan nopeutetun säädösvalmistelun kanssa (Business Finland, VM)
- Käynnistä koulutusohjelmia post-quantum cryptography -osaamiseen (Suomen Akatemia, yliopistot)
- Varmista aktiivinen osallistuminen digitaalisen euron valmisteluun (Suomen Pankki, VM)
- Ehdota Pohjoismaat–Baltia-yhteistyön syventämistä digitaalisen resilienssin alueella olemassa

olevien rakenteiden (NORDEFCO, Nordic Innovation, NB8) puitteissa, fokusoituna kvanttiturvalliseen viestintään ja rajat ylittävään digitaaliseen identiteettiin (LVM, UM)

- Käynnistä Suomi–Viro-kvanttiturvallisen viestintäyhteyden pilotti lead nation -periaatteella (Traficom, Kyberturvallisuuskeskus)

12.3 Käynnistetään kolmen vuoden kuluessa

- Toteuta post-quantum cryptography -migraatio kriittisessä infrastruktuurissa EU:n aikataulun mukaisesti: kriittinen infra 100 % kvanttiturvallinen vuoteen 2030 mennessä (koordinoi Traficom)
- Perusta 100 miljoonan euron kansallinen PQC-siirtymäohjelma vuosille 2026–2030, kattaen kriittisen infrastruktuurin migraation, pilottihankkeet, osaamiskeskuksen ja pk-yritysten siirtymätuen
- Kehitä kansallinen digitaalinen identiteetti -ekosysteemi EUDI-lompakon ja yksityisyyssuojausteknologioiden (ZKP, homomorfinen salaus) pohjalta (DVV, LVM)
- Rakenna Suomen rooli EU:n lohkoketjuinfrastruktuurissa (EBSI) – erityisesti tutkintojen todentamisessa ja yritystietojen rajat ylittävässä verifioinnissa
- Valmistaudu digitaalisen euron käyttöönottoon (koordinoi Suomen Pankki)
- Vakiinnuta Singapore-kumppanuus strategiseksi digitaalisen resilienssin oppimiskumppanuudeksi, laajentaen Smart Nation -mallista sovellettavat elementit Suomen kontekstiin

12.4 Suomi digitaalisen murroksen edessä

Suomi on kohdannut teknologisia murroksia aiemminkin. Teollistuminen, Nokia-aikakausi ja digitalisaation ensimmäinen aalto osoittivat, että pieni maa voi paitsi sopeutua muutokseen, myös muovata sitä. Sama mahdollisuus on nyt käsillä.

Kvanttilaskennan kehitys haastaa nykyiset salausmenetelmät. Tekoälybuumin synnyttämä laskentakapasiteetti madaltaa kynnystä kerätä ja säilöä dataa ennennäkemättömässä mittakaavassa. Samalla uudet teknologiat – lohkoketjut, reunalaskenta, yksityisyyssuojausteknologiat – tarjoavat työkaluja rakentaa luotettavampaa ja läpinäkyvämpää digitaalista infrastruktuuria.

Suomen kokonaisturvallisuusajattelu on herättänyt kansainvälistä kiinnostusta. Digitaalinen resilienssi on sen luonnollinen jatke – ei erillinen strategia, vaan osa samaa ajattelua, joka yhdistää julkisen ja yksityisen sektorin sekä kansalaiset yhteisen varautumisen taakse.

Tämä selvitys ei ole lopullinen vastaus. Se on prosessin alku – kutsu sidosryhmille kokoontua säännöllisesti arvioimaan tilannekuvaa, päivittämään suosituksia ja pitämään keskustelua elävänä. Dokumentti arkistoituu vasta kun sen kysymyksenasettelu on vanhentunut.

Suomella on osaaminen, instituutiot ja kokemus murrosten kääntämisestä mahdollisuuksiksi. Nyt tarvitaan johdonmukaista toimeenpanoa, rohkeutta priorisoida ja uskallusta toimia ennen kuin muut ehtivät ensin.

Taustamateriaalit

Selvityksessä on hyödynnetty muun muassa seuraavia lähteitä:

- Traficom Kyberturvallisuuskeskus: Vuosiraportit ja viikkokatsaukset
- Tilastokeskus: Yritystilastot
- Statista: IoT Market Forecasts
- NIST: Post-Quantum Cryptography Standardization
- EU Commission: PQC Roadmap ja MiCA-asetus
- Business Finland: Startup-tilastot
- Pääomasijoittajat ry: Rahoitustilastot
- Sitra: Teknologioiden konvergenssi -materiaalit
- Huoltovarmuuskeskus: Kvanttilaskennan tietoturvavaikutukset -raportti 2024
- GSMA: Post Quantum Government Initiatives by Country and Region
- Gartner: Edge Computing Forecasts
- Alan Turing Institute: Homomorphic Encryption in Finance
- Google: Zero-Knowledge Proof Libraries (avoimen lähdekoodin julkaisu 2025)
- Singapore CSA: Singapore Cyber Landscape 2024/2025
- Tracxn: Finland Startup Ecosystem Reports