Lohkoketjun hyöydyntäminen, sekä erilaiset lohkoketjut

2018

alvarmahlberg
@alvarmahlberg

KERTAUSTA EILISELTÄ

1. Lohkoketjut
mahdollistavat verkostojen
luomisen ja **ylläpitämisen**,
ilman hallitsijaa ja
ilman rahaa.

2. **Kryptoekonomiassa** yhdistetään **kryptografiaa** ja **taloutta**, jotta voidaan luoda vahvoja hajautettuja vertaisverkkoja, jotka menestyvät ajan myötä, vaikka vastustajat yrittävät häiritä verkkoa.

3. Lohkoketjuteknologian avulla voidaan avata valtavasti potentiaalista **taloudellista arvoa**.

ERILAISET LOHKOKETJUT

Zheng ym. (2017) havainnollistavat tutkimuksessaan kolmen erilaisen lohkoketjun eroja. Kolme erilaista lohkoketjua ovat:

1. Julkinen lohkoketju

2. Yksityinen lohkoketju

3. Hybridi-lohkoketju

1. JULKINEN LOHKOKETJU

Julkinen lohkoketju: on avoin kaikille, tarjoaa läpinäkyvyyttä ja pyrkii estämään vallan keskittymistä tietylle yksittäiselle taholle. Kaikki toimijat voivat osallistua järjestelmän ylläpitoon, käyttämiseen ja transaktioiden hyväksymiseen. Julkisessa lohkoketjussa toimijoiden ei tarvitse luottaa toisiinsa.

2. YKSITYINEN LOHKOKETJU

Yksityinen lohkoketju: Yksityiset lohkoketjut toimivat suljetummissa ympäristöissä ja käyttäjillä on useasti tiettyjä rajattuja oikeuksia. Jokaisella halukkaalla ei ole lupaa osallistua lohkoketjun käyttöön. Yksityinen lohkoketju soveltuu paremmin tietyille toimialoille, yrityksille tai yrityksen sisäiseen toimintaan, jos halutaan toimia ainoastaan luotettujen kumppaneiden kanssa.

3. HYBRIDI-LOHKOKETJU

Hybridi-lohkoketju: jota kutsutaan myös nimellä konsortio-lohkoketju. Hybridi-lohkoketju sijoittuu ominaisuuksiltaan julkisen ja yksityisen lohkoketjun väliin. Hybridi-lohkoketjut ovat soveltuvia tilanteisiin, joissa toimijoiden välillä tulee olla jonkinlaista luottamusta. Hybridi-lohkoketjut soveltuvat esimerkiksi yritysten väliseen yhteistyöhön.

Ominaisuus	Julkinen lohkoketju	Hybridi-lohkoketju	Yksityinen lohkoketju
Konsensus määrittely	Louhijat	Valitut noodit	Yksi organisaatio
Käyttöoikeudet	Julkiset	Julkiset tai rajoitetut	Julkiset tai rajoitetut
Muuttumattomuus	Lähes mahdoton peukaloida	Mahdollista peukaloida	Mahdollista peukaloida
Tehokkuus	Matala	Korkea	Korkea
Keskitetty	Ei	Osittain	Kyllä
Konsensus prosessi	Ei vaadi lupaa	Vaatii luvan	Vaatii luvan

ERILAISET LOHKOKETJUT

Wust ja Gervais (2017) jakaa lohkoketjut karkeammin kahteen ryhmään:

Ensimmäinen ryhmä on **avoimet lohkoketjut**, jotka ovat hajautettuja ja avoimia kaikille. Avoimet lohkoketjut ovat sama asia kuin julkiset lohkoketjut.

Toinen ryhmä on **luvan vaativat lohkoketjut.** Näissä lohkoketjuissa on jonkinlainen keskusyksikkö, joka päättää ja antaa oikeuksia yksittäiselle toimijalle osallistua lohkoketjun toimintaan.

	Avoimet lohkoketjut	Luvan vaativat lohkoketjut
Osallistuminen	Kuka tahansa voi osallistua	Kutsu, tarkastus tai kriteeri
Oikeudet	Kuka tahansa voi lukea ja kirjoittaa	Luku- ja kirjoitusoikeudet saattavat olla rajoitettuja
Identiteetti	Pseudonyymi	Osallistujat mahdollisesti tunnistettava

HAJAUTETUN TILIKIRJAN RATKAISUT

Lohkoketjuteknologia nähdään osana hajautetun tilikirjan (Distributed ledger technology) ratkaisuja.

Näitä kahta ei kuitenkaan pidä täysin sekoittaa toisiinsa, sillä hajauteutun tilikirjan ratkaisuja voidaan toteuttaa myös ilman varsinaista lohkoketjua. (Walport, 2016).

LOHKOKETJUT VS KESKITETYT TIETOKANNAT

Lohkoketju on tietokanta, joka mahdollistaa välittömän datan jakamisen epäluotettavienkin tahojen kesken. Tiedon tallennuksen ja siihen suoritettavien tietokantasiirtojen kannalta lohkoketju ei tarjoa mitään uutta, mutta jos järjestelmän keskeiset haasteet liittyvät luottamukseen ja robustisuuteen, tarjoaa lohkoketju uusia mahdollisuuksia. Neljä tarkastelukulmaa:

1. **Välikädettömyys**
2. **Luottamuksellisuus**
3. **Robustisuus**
4. **Suorituskyky**

Referoitu artikkeli: https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

1. Välikädettömyys

Välikädettömyys on yksi lohkoketjujen keskeisimmistä hyödyistä. Tietokanta on myös aineellinen asia, joka on keskitetyssä mallissa aina yhden keskitetyn tahon armoilla. Käyttäjien on pystyttävä luottamaan tähän ylläpitäjä tahoon ja ylläpitäjän on kulutettava resursseja tietokannan turvaamiseen. Lohkoketju voi mahdollisesti tarjota halvempia toteutusmalleja.

2. Luottamuksellisuus

Keskitetyssä mallissa vain yksi taho voi lukea ja muokata kaikkea tietoa. Lohkoketjun arkkitehtuuri on läpinäkyvä, koska kaikki solmut osallistuvat transaktioiden tarkistamiseen ja validointiin. Lohkoketjuja varten on kehitetty tallennettua tietoa salaavia menetelmiä, mutta ne eivät voi koskaan olla yhtä tehokkaita kuin keskitetyn mallin mahdollistama tiedon täydellinen piilottaminen.

3. Robustisuus

Lohkoketjuissa kaikki solmut tarkastavat ja prosessoivat transaktiot, joten yhden solmun kaatumisella ei ole merkitystä. Samoin vertaisverkkoviestintä ei kärsi siitä jos yksi kommunikaatiolinkki tippuu pois. Perinteisiäkin tietokantoja voi replikoida, mutta samanlaista saumattomuutta ja helppoutta ei näin saavuteta.

4. Suorituskyky

Lohkoketjut ovat ja tulevat aina olemaan perinteisiä tietokantoja hitaampia. Lohkoketjuissa normaalien tietokantatehtävien lisäksi aikaa kuluttavat allekirjoitusten tarkistaminen, konsensusmekanismi ja päällekkäisyys (kaikki solmut prosessoivat kaikki siirrot).

LOHKOKETJU UUDENLAISENA HAJAUTETTUNA TIETOKANTA

Verrattuna perinteisiin hajautetun tietokannan hallintajärjestelmiin, voidaan esiin nostaa selviä eroja:

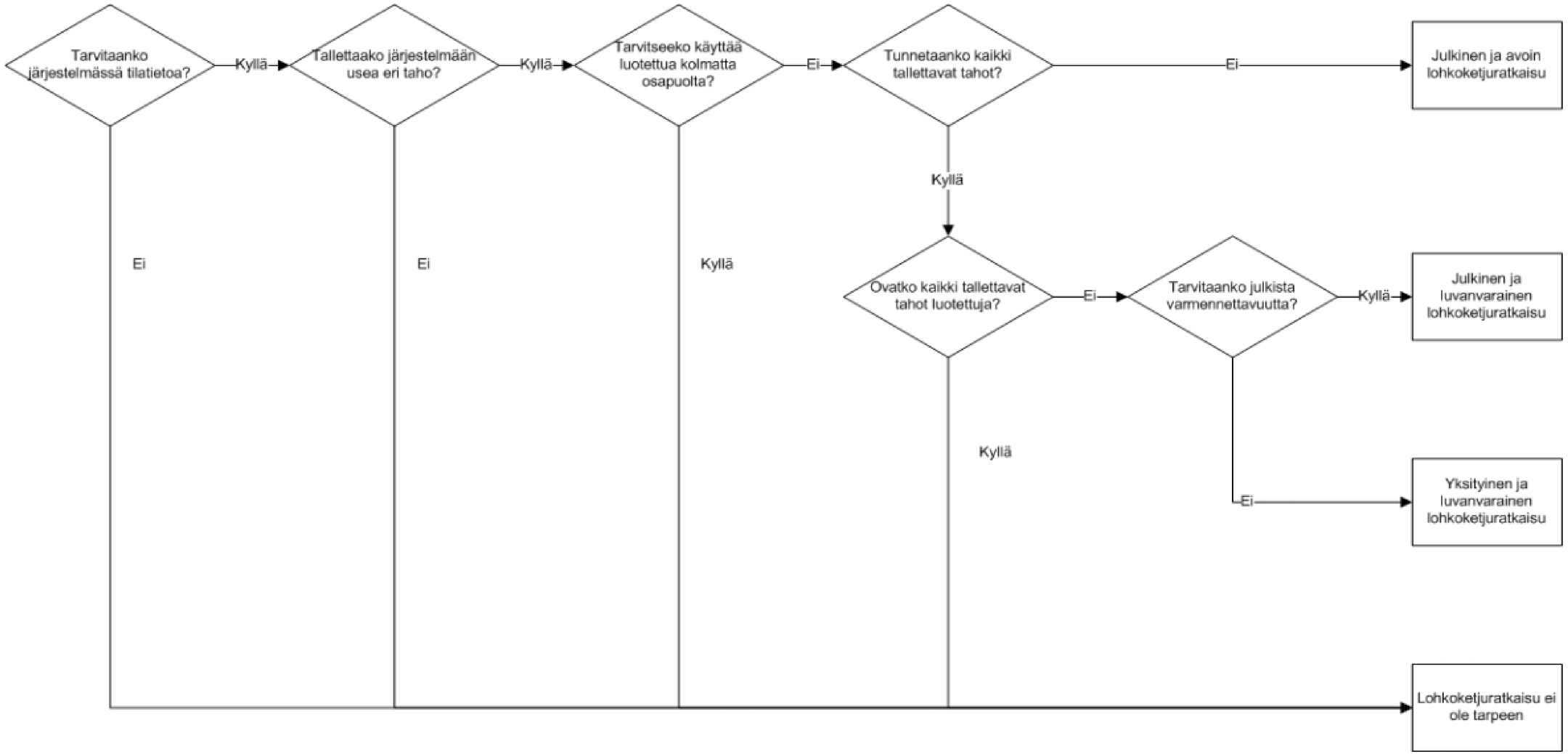
1. Lohkoketjut ovat **hajautetusti hallinnoituja**, kun taas perinteiset hajautetun tietokannan hallintajärjestelmät ovat logiikaltaan keskitetysti hallinnoituja.

2. Kirjausketjun **muuttumattomuudessa on eroja**, sillä perinteiset hajautetun tietokannan hallintajärjestelmät tukevat komentoja luo, lue, päivitä ja poista. Lohkoketjuissa on ainoastaan luo ja lue komennot.

3. Tiedon alkuperää ja varojen omistajuutta ei voi lohkoketjuissa muuttaa **kuin ennalta määritellyin säännöin** (julkiset lohkoketjut). Perinteisissä hajautetun tietokannan hallintajärjestelmissä ylläpitäjä voi muokata tiedon alkuperää tai varojen omistajuutta. (Kuo, Kim & Machado, 2017).

MILLOIN HYÖDYNTÄÄ LOHKOKETJUA?

MILLOIN HYÖDYNTÄÄ LOHKOKETJUA?

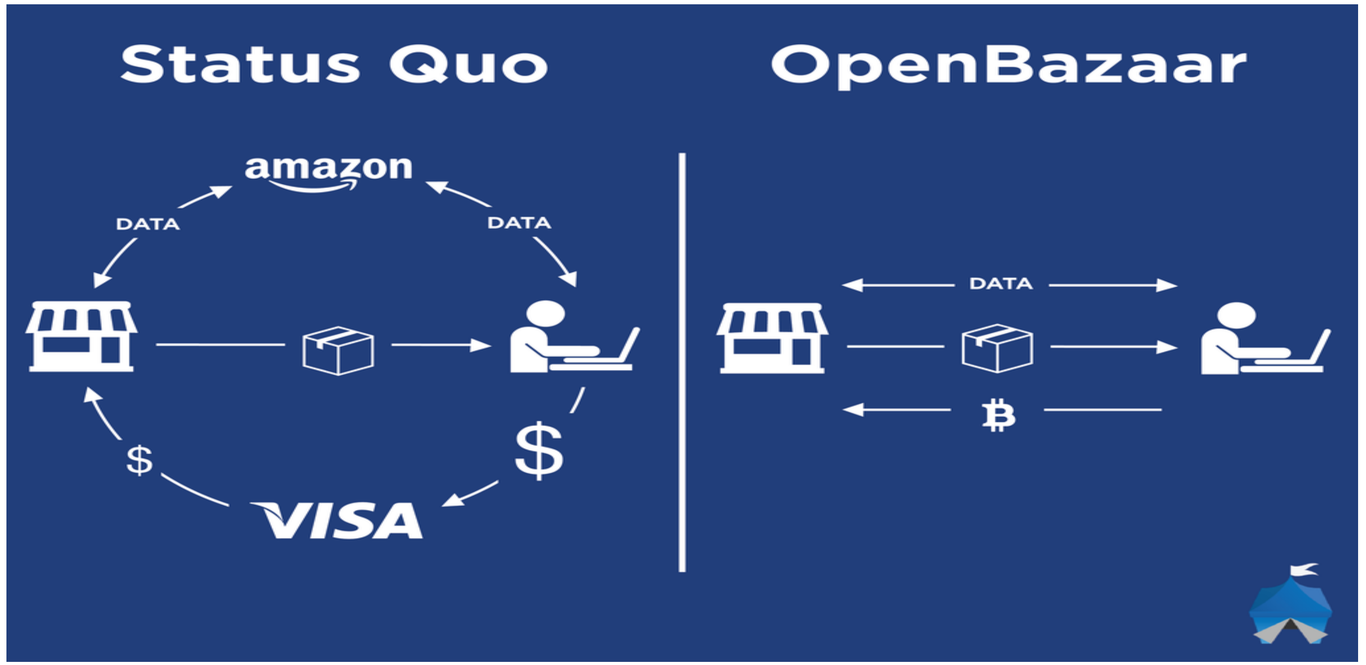


(Wust & Gervais, 2017)

Suomennettu kaavio valtioneuvoston julkaisusta ”Lohkoketjuteknologian mahdollisuudet ja hyödyt sosiaali- ja terveydenhuollossa”.

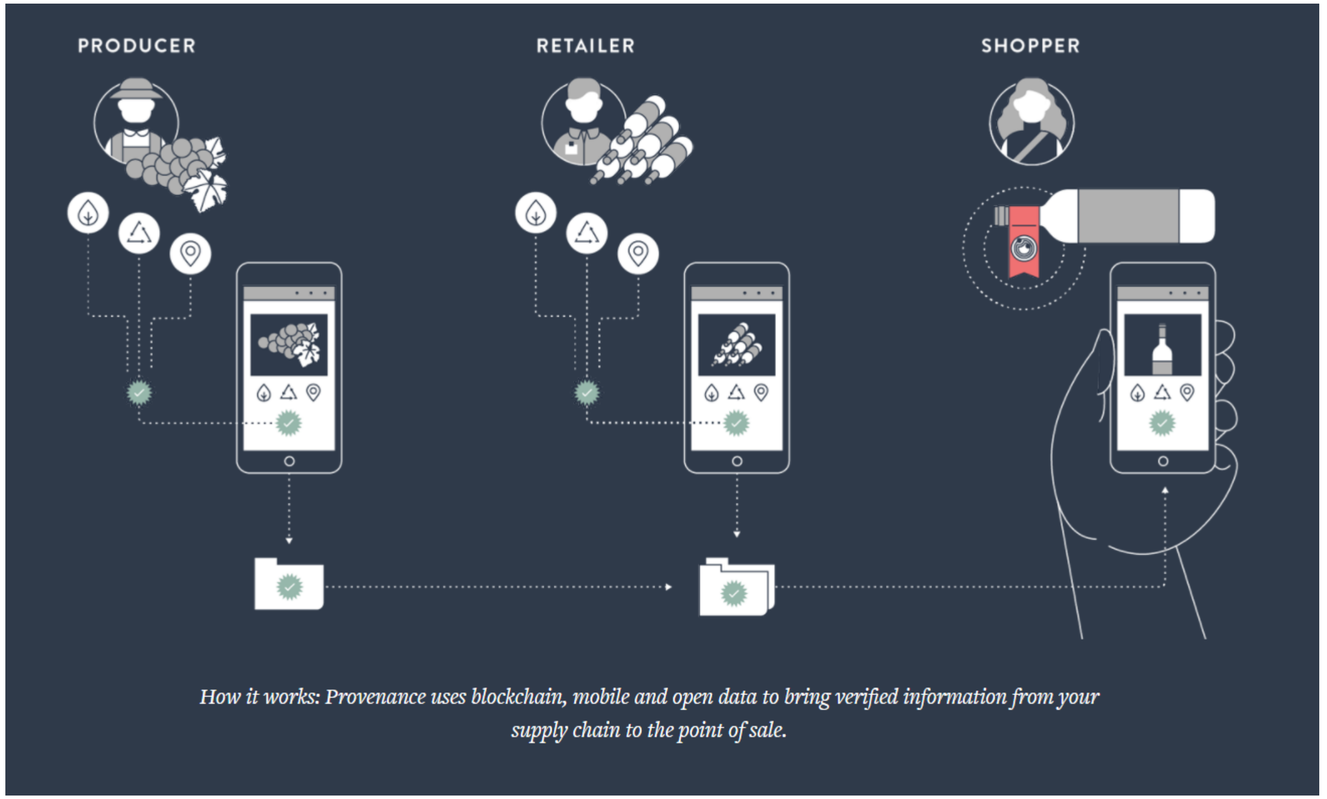
OpenBazaar

OpenBazaar on hajautetusti toimiva markkinapaikka.
Muistuttaa toiminnaltaan Amazonia ja Ebayta.
Uudenlaista alustataloutta.



PROVENANCE

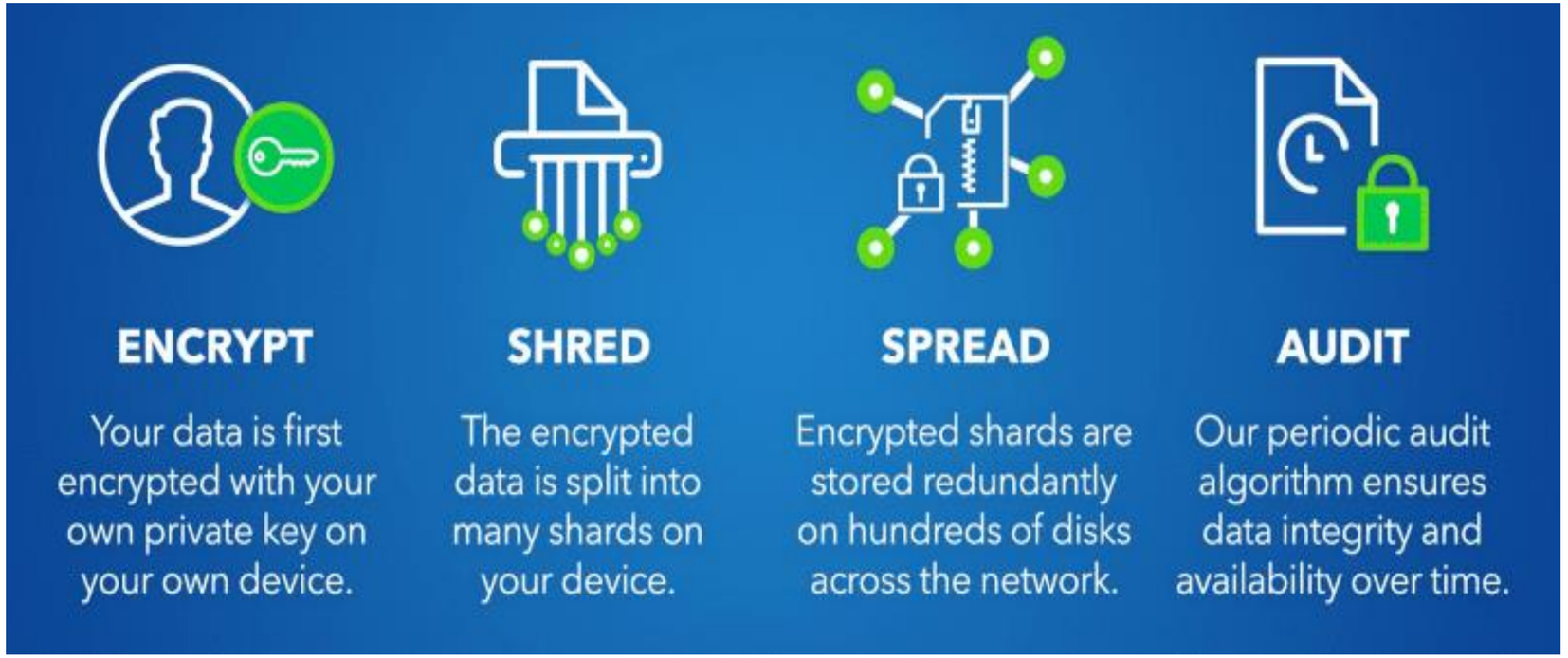
Tuotanto- ja toimitusketjujen todentamiseen kehitetty ratkaisu. Tuottajat ja jälleenmyyjät voivat seurata tuotteita. Asiakkaat saavat lisätietoa tuotteista.



How it works: Provenance uses blockchain, mobile and open data to bring verified information from your supply chain to the point of sale.

STORJ

Storj on hajautettu pilvipalvelu, jossa käyttäjät voivat vuokrata tai tarjota omaa tallennustilaa.



Hyperledger ja IBM

HYPERLEDGER