Hajautetun luottamuksen teknologiat

Digitalisaation suunnannäyttäjien kokoontumisajot

13.02.2018

Janne Pulkkinen & Kimmo Mäkinen

Hallinnon lohkoketjuteknologiaverkosto

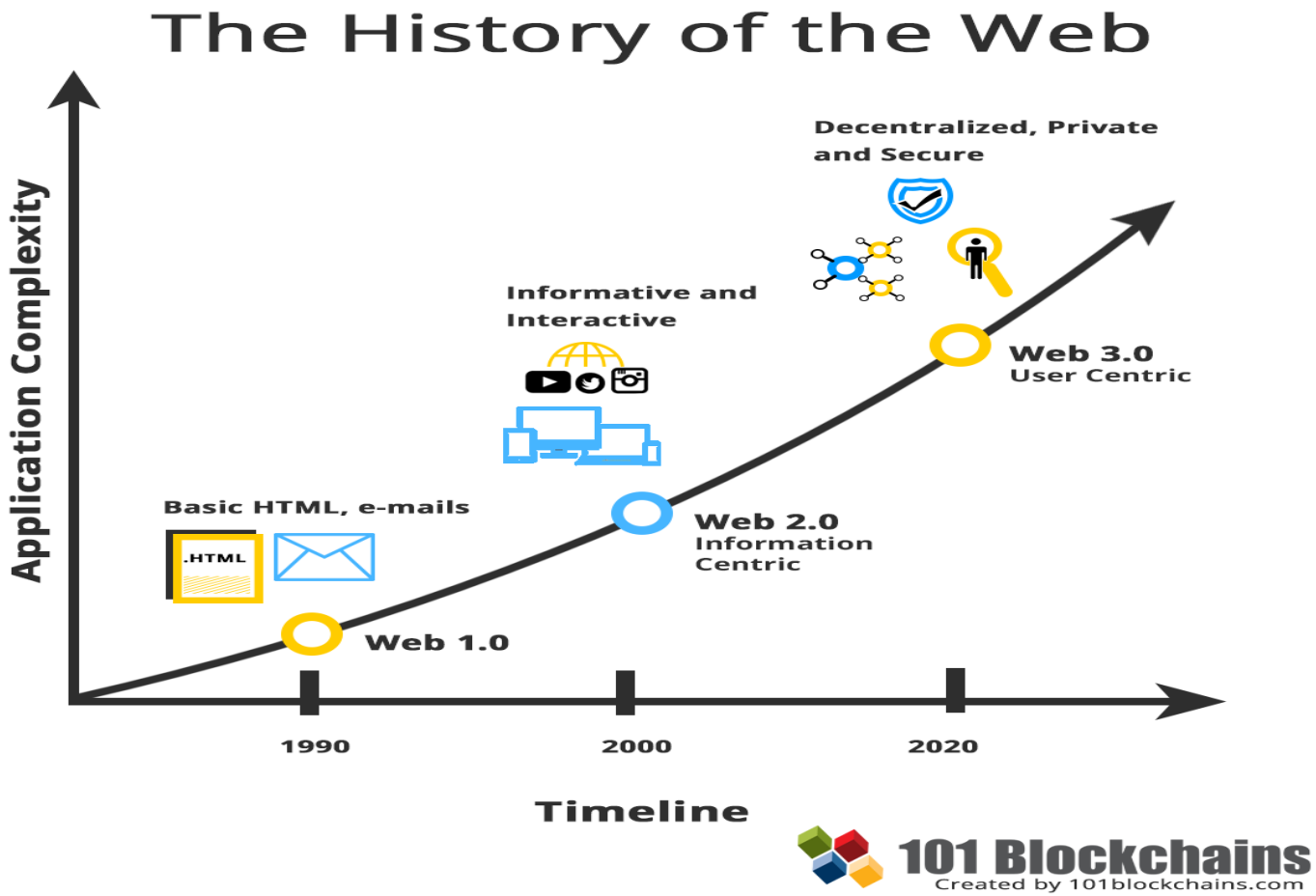
Kela|Fpa

Johdanto

- Internet on mahdollistanut viimeisen kahden vuosikymmenen aikana tiedon vapaan liikkuvuuden.
- Tiedon vapaa liikkuvuus ja erityisesti tiedon määrän suuri kasvuvauhti on tuonut esille erittäin suuren kysymyksen – luottamuksen puutteen.
- Lohkoketjuteknologian ja muiden hajautetun luottamuksen teknologioihin perustuvien ratkaisujen ominaisuudet luovat teknisesti täysin uudenlaisia mahdollisuuksia ratkaista luottamukseen liittyviä haasteita.

Johdanto

- Luottamukseen liittyvien innovaatioiden lisäksi lohkoketjuteknologia mahdollistaa myös arvon tallentamisen ja jakamiseen täysin uudella tavalla.
- Lohkoketjuteknologian onkin sanottu mullistavan nykyisenkaltaisen internetin ja muutosvaikutusten olevan niin suuria, että puhutaan jo internetin seuraavasta sukupolvesta, Lohkoketjujen Internet 2.0:sta.


The History of the Web
Application Complexity
Decentralized, Private and Secure
Informative and Interactive
Basic HTML, e-mails
.HTML
Web 1.0
Web 2.0
Information Centric
Web 3.0
User Centric
1990
2000
2020
Timeline
101 Blockchains
Created by 101blockchains.com

Lohkoketjuteknologia

- Lohkoketju on siis uudenlainen kryptografisesti suojattu hajautettu tietokanta, jossa tapahtumia kirjataan pysyvästi lohkoihin, ja joista tietoa ei pystytä jälkikäteen poistamaan tai muuttamaan, koska tieto säilyy lohkoissa riippumatta yksittäisestä toimijasta.
- Lohkoketjuteknologia onkin uudenlainen ja mullistava tapa yhdistää jo olemassa olevia koeistettuja teknologiaratkaisuja
  - Julkisen avaimen salaus
  - Konsensusmekanismi
  - Verkon hajautus
  - Kryptografia

Lohkoketjuteknologia

- Lisäksi lohkoketjun tiedot ovat halutessa läpinäkyviä ja tarkistettavissa yhtäaikaisesti kaikkien osalta.
- Lohkoketju on siis hajautettu tietokanta, jonka avulla mahdollistetaan teknologisesti luottamuksen rakentamisen tuntemattomien tahojen välille ilman kolmatta osapuolta
- Muuttaa keskitettyjen auktoriteettien ja viranomaisten roolia
  - Luottamusta ei tarvita, koska ketjuun lisättävistä lohkoista päätetään konsensusmekanismin avulla. Konsensusmekanismin tehtävänä on mahdollistaa hajautettu päätöksenteko siten, että transaktiohistorian manipulointi olisi yksittäiselle toimijalle liian kallista ja siksi kannattamatonta.
- Yhteenvetona lohkoketju on siis hajautettu ja suojattu tietokanta, jonka tapahtumat ovat kaikkien nähtävillä

Toimintaprosessi

Toimija aloittaa tapahtuman

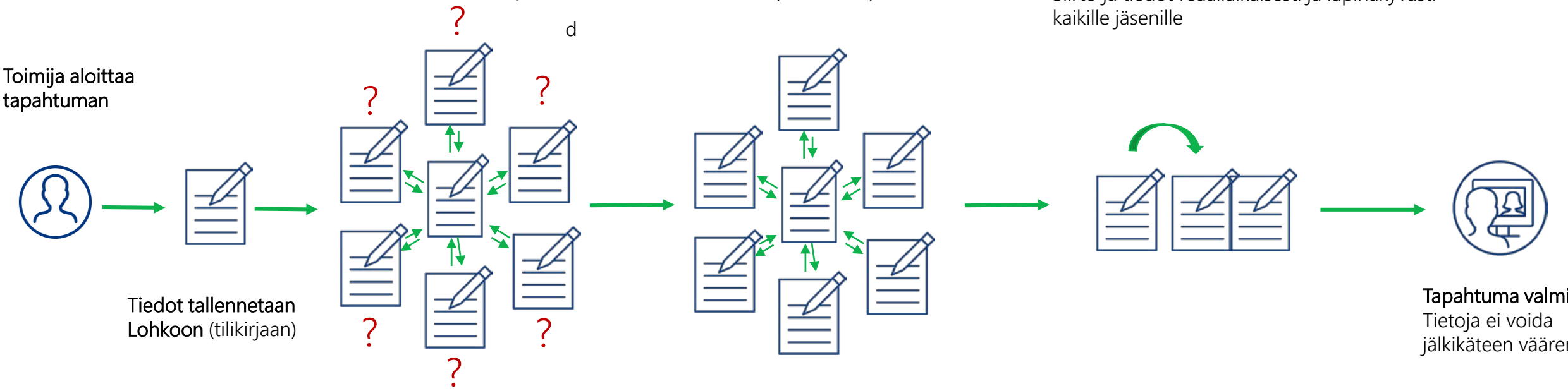
Tiedot tallennetaan Lohkoon (tilikirjaan)

Tilikirja validoidaan ja paikkansapitävyys varmistetaan verkoston jäsenten kesken

d

Verkoston jäsenet vahvistavat siirron (konsensus)

Lohko lisätään osaksi lohkoketjua.
Siirto ja tiedot reaaliaikaisesti ja läpinäkyvästi kaikille jäsenille



Tapahtuma valmis
Tietoja ei voida jälkikäteen väärentää

Kela|Fpa

Avoimet ja suljetut lohkoketjut

- Avoimet lohkoketjut (Lohkoketjut)
  - Kaikille avoin lohkoketju, joka ei ole yhdenkään tahon hallinnoima tai omistama. Julkisessa lohkoketjussa kuka tahansa taho voi lukea ja lähettää transaktioita, sekä osallistua konsensusprosessiin, jossa päätetään uuden lohkon linkittämisestä lohkoketjuun.

- Suljetut/rajoitetut lohkoketjut (Hajautetut tilikirjat, DLT)
  - Lohkoketjun konsensusprosessi on yhden tai useamman tahon hallinnoima yksityinen tapahtumarekisteri. Lohkoketjuun liittyminen ja käyttö edellyttävät hallinnoivan tahon hyväksyntää.
  - Prosessien virtaviivaistaminen

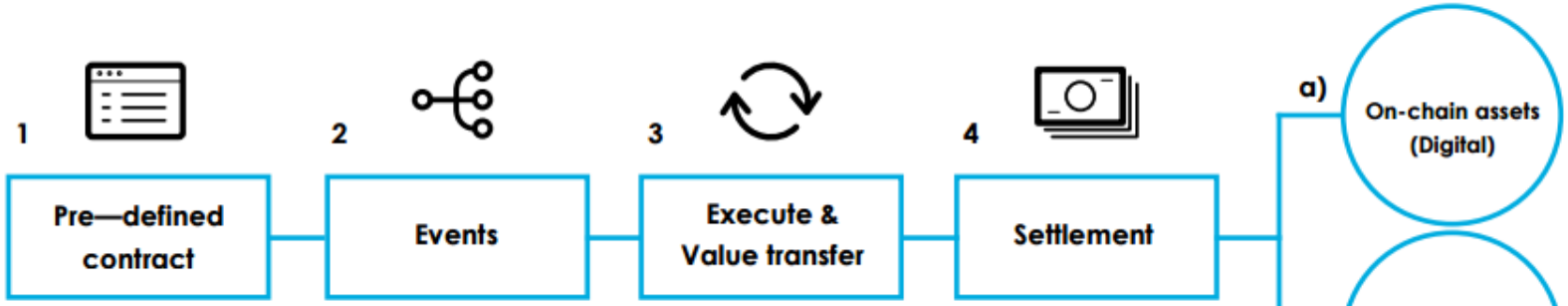
Älysopimukset

- Smart contract on jaetulla alustalla, yleisesti lohkoketjussa sijaitseva tietokoneohjelma
- Älysopimus pystyy toteuttamaan ja solmimaan itsenäisesti sopimuksia
  - Älykäs sopimus on etukäteen tehty ja varmennettu itsensä toteuttava looginen prosessi, joka pystyy toteuttamaan ja solmimaan sopimuksia
  - Pystyy valvomaan sopimuksen noudattamista, sekä asettamaan mahdollisia sanktioita tarvittaessa

Älysopimukset

- Älysopimukset mahdollistavat tuntemattomien osapuolten välisten sopimusten solmimisen ja sopimukseen kirjattujen toimenpiteiden suorittamisen turvallisesti ilman kolmatta osapuolta.
  - Älysopimuksia soveltamalla voidaan mahdollistaa palveluinnovaatioiden ja -prosessien rahoittaminen, koordinointi ja hallinta organisoida hajautetusti.
  - Älysopimuksia hyödyntämällä palveluinnovaatiot voidaan tuottaa asiakkaille entistä suoraviivaisemmin digitaalisista alustoista ja niitä kontrolloivista yrityksistä riippumatta.

Älysopimukset



- Terms are established by all counterparties, such as:
  - ◊ Variable interest rate (e.g LIBOR)
  - ◊ Currency of payments
  - ◊ Currency rate
- Conditions for execution (e.g time and date, LIBOR rate at given value)

- Event triggers contract execution
- Event can refer to:
  - ◊ Transaction initiated
  - ◊ Information received

- Terms of contract dictate movement of value based on conditions met.

a. For digital assets on the chain, such as a cryptocurrency, accounts are atomically settled

b. For assets represented off the chain, such as stocks and fiat, changes to accounts on the ledger will match off-chain settlement instructions

Kela|Fpa

Tokenit (Hyödykkeet)

- Lohkoketjuissa käytettävä arvon mitta
- Mahdollistavat esimerkiksi omaisuuden hajautetun omistajuuden tai palveluiden arvon liikuttamisen

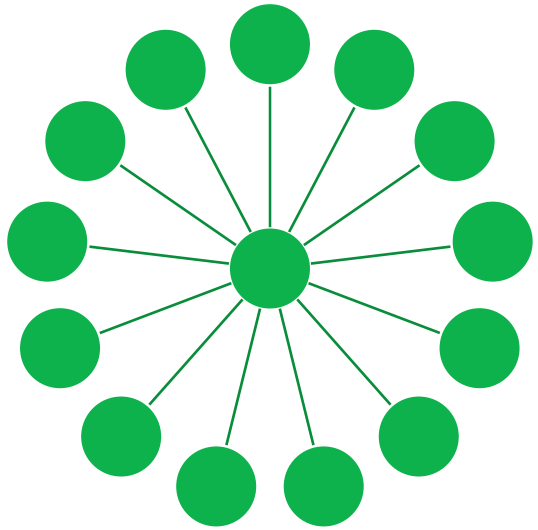
- Utility Token
  - Hyödyke-token, tarkoittaa hyödykettä, jolla on käyttökohteeseen sopivia ominaisuuksia
  - Tokenin omistaja voi olla oikeutettu erilaisten palveluiden tai alennusten hyödyntämiseen, eli kolikoilla voidaan ostaa hajautetun järjestelmän tuottamaa palvelua.
- Security Token
  - Arvopaperi token
  - Lohkoketjussa sijaitseva digitaalinen arvopaperi. Arvo on sidottu johonkin konkreettiseen omaisuuteen tai kohteeseen.
  - Mikromaksut

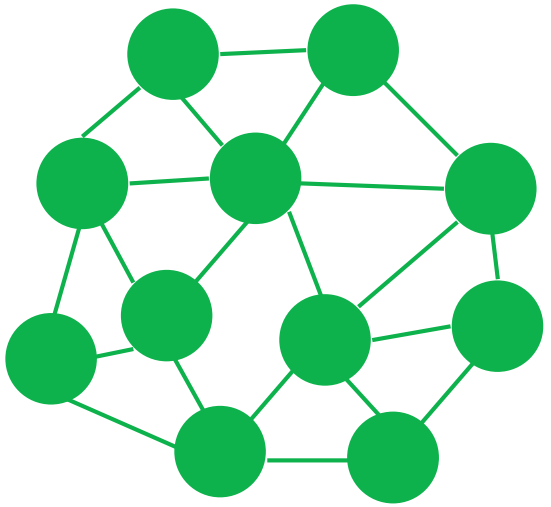
Identiteetinhallinta

- Käyttäjäkeskeinen identiteetti (Self-Sovereign Identity)
  - Ratkaisumallissa luovutaan palvelukohtaisista tunnistautumisratkaisuista ja käyttäjärekistereistä ja siirretään identiteetin hallinta käyttäjälle
- Käytännössä yksilö (tai organisaatio) voi vapaasti luoda itselleen identiteettejä ja liittää niihin attribuutteja, kuten henkilötietojaan ja suostumuksiaan. (Mydata –näkökulma)
  - Eri tasoja
  - Yksi tai useampia varmentajia, jotka vahvistavat tiedot oikeiksi
  - Varmennetut tiedot tallennettaisiin käyttäjän hallintaan siten, että ne ovat esitettävissä palvelujen käytön yhteydessä
  - Yksilön näin ollen mahdollista luovuttaa palveluntarjoajalle vain ne tiedot, jotka kulloinkin tarvitaan palvelun toteuttamiseksi

Miksi meidän pitäisi olla kiinnostunut? Millainen on hyvä käyttötapaus?

- Lohkoketjut muuttavat nykyisiä liiketoimintamalleja, prosesseja sekä organisaatioita keskitetyistä hajautettuihin.
- Disruptio





Lohkoketjujen käyttökohteet Suomessa tähän mennessä

- Maahanmuuttoviraston Moni Prepaid ratkaisu
- Asuntokauppatransaktioiden automatisointi (DIAS)
  - Tomorrow tech, Vero, MML, PRH, OP, Nordea, Danske…
- Listaamattoman yrityksen kaupankäyntialusta
  - Listaamattomien osakkeiden kaupankäynti ja osakashallinta-alusta lohkoketjuteknologian avulla
  - Voidaan hyödyntää osake- ja osakasrekisterin hallintaan, uusien osakkeiden liikkeellelaskuun ja osakkeiden jälkimarkkinakauppaan ostajan ja myyjän välillä.
  - Yhdistetty kaksi erilaista lohkoketjupohjaista alustaa (Hyperledger Indy & R3 Corda)
  - Tieto, PRH, Vero, Tilaajavastuu…
- Toimitusketjut
  - Kouvola Innovation, SmartLog
  - Arla
  - S-ryhmä & IBM Lohitutka

Kansainvälinen yhteistyö