BITCOIN

10

MINUUTISSA

Kaikki mitä olet aina halunnut tietää bitcoinista.

Brought to you by Relai

MIKÄ ON BITCOIN?

Bitcoin, maailman suosituin kryptovaluutta, on jatkuvasti otsikoissa ympäri maailmaa. Monet haluavat hyötyä sen suosiosta, toiset eivät välitä siitä lainkaan ja jotkut ovat skeptisiä sen potentiaalista. Kyseinen virtuaalivaluutta on inspiroinut lukuisia keskusteluita liittyen rahaan, sijoittamiseen ja teknologiaan. Jotkut näkevät sen puhtaana spekulaationa tai ovat julistaneet sen kuplaksi, samalla toiset puhuvat innovaatiosta, rahajärjestelmän vallankumouksesta, ja jopa nykyisen rahajärjestelmän “kohtalon hetkestä”.

Useat valtiot, esimerkiksi Kiina, näkevät Bitcoinin uhkana ja ovat julistaneet sodan kryptovaluuttoja vastaan. Toiset valtiohallinnot, esimerkiksi El Salvadorissa, ovat julistaneet Bitcoinin viralliseksi maksuvälineeksi, toivoen sen lisäävän talouskasvua.

Mutta mikä on Bitcoin? Onko se rahaa? Digitaalista kultaa? Nörttien ja spekuloijien luoma hetkellinen muotiilmiö? Vai onko se jotain ihan muuta? Seuraavissa kappaleissa matkaamme näiden kysymysten syövereihin ja katsomme lähemmin tätä virtuaalivaluutta ymmärtääksemme paremmin sen taustalla olevan filosofian ja toiminnallisuuden. Tehtävämme onnistumiseksi, meidän kannattaa aloittaa tarinalla Bitcoinin synnystä.

BITCOININ TARINA

Bitcoin konseptin syntyhetket voidaan sijoittaa 90-luvun alkuun. 1992, ryhmä koodareita Kaliforniassa aloitti sähköpostilistan vaihtaakseen ajatuksia samanhenkisten ihmisten kanssa koskien kryptografiaa, matematiikkaa, politiikkaa ja filosofiaa. He kutsuivat itseään Kryptopunkkareiksi (Eng. Cypherpunks). Nimi juontaa sci-fi kirjallisuudessa tunnetuksi tulleesta cyberpunk termistä, joka näppärästi muokattiin sopivaan muotoon lisäämällä kryptografiaan viittaava sana termin alkuun.

Kryptopunkkarit

Kryptopunkkarien yhteisö kasvoi nopeasti kirjavaksi joukkioksi. Erilaisista taustoistaan huolimatta, sen jäsenet jakoivat ajatuksen siitä, että internetistä oli tulossa inhimillisen vapauden sotatanner. Suojellakseen internetiä kontrollilta, seurannalta ja sensuurilta, ja taatakseen vapaan ja avoimen internetin, Kryptopunkkarit käyttivät voimakasta asetta: Kryptografiaa, eli tiedon salaamista.

Heidän 1993 julkaistussa manifestissaan he julistivat että “Kryptopunkkarit kirjoittavat koodia. Tiedämme että jonkun pitää kirjoittaa tietokoneohjelmia suojellakseen ihmisten yksityisyyttä, me tulemme kirjoittamaan ne.”

Mutta pelkkä kryptografia ei riittänyt vapaan internetin turvaamiseksi. Syy oli, että internet ei koskaan voi olla todellisesti vapaa ilman omaa rahaa. Rahaa, joka on riippumaton valtioista, keskuspankeista, ja yhtiöistä; Tarvittiin kryptovaluutta, joka on yhtä desentralisoitu kuin internet.

Rahakokeiluja

Itsenäisen digitaalisen rahan luonti toi mukanaan teknisiä haasteita. Jo 1990 kryptologi David Chaum oli luonut eCash kryptovaluutan, joka ei ollut desentralisoitu, mutta tarjosi anonymiteetin käyttäjille kryptogafian avulla. Pidemmällä tähtäimellä Ecash ei kuitenkaan saavuttanut merkittävää asemaa muiden maksujärjestelmien joukossa. Konseptin taustalla ollut yhtiö hakeutui konkurssiin kahdeksan vuoden jälkeen ja eCash katosi markkinoilta.

Uudet kokeilut seurasivat, joista E-Gold erottui joukosta. Se oli kultaa vakuutenaan käyttävä kryptovaluutta. Yhtiö, joka oli perustettu 1996 dot-.com buumin aikana, osui oikeaa markkinarakoon ja prosessoi yli kahden miljardin edestä transaktioita parhaana vuotenaan.

Mutta koska E-Gold oli keskitetyn organisaation hallinnassa, se oli haavoittuvainen hyökkäyksille. Juridiset ongelmat seurasivat ja USA:n hallitus aloitti oikeustoimet yhtiötä vastaan. Vuonna 2008, E-Gold todettiin syylliseksi USA:n oikeudessa rahanpesusta ja Patriot Act:in vastaan toimimisesta. Kaikki yhtiön varat jäädytettiin ja se joutui lopettamaan toimintansa.

Nämä epäonnistuneet yritykset merkitsivät kahta asiaa Kryptopunkkareille. Ensiksi, sekä eCash että E-Gold olivat vakuudella taattuja.Vakuudet osoittautuivat heikkoudeksi, sillä valtiot pystyivät helposti takavarikoimaan ne. Näin ollen, vapaalla kryptovaluutalla ei saisi olla keskitettyjä hyökkäyspinta-aloja, kuten rekisteröityä yhtiötä, pankkitiliä tai keskitettyä palvelinten sijaintia. Toiseksi, hallituksilla ja regulaattoreilla ei ollut sympatiaa valtiosta riippumatonta digitaalista rahaa kohtaan.

Keskeinen kysymys vaivasi edelleen Kryptopunkkareita: Miten riippumaton digitaalinen raha voisi toimia ilman keskitettyä “kirjanpitäjää” ja miten varmistaa, että rahaa ei käytetä kahdesti. Jos niin sanottu tuplamaksuongelma (englanniksi “double-spend problem”) voitaisiin ratkaista ilman riippuvuutta keskitetystä tahosta, voisi olla mahdollista luoda digitaalinen raha internetille.

Mystinen luomisteko

Yllämainituista syistä, Kryptopunkkarit aloittivat keskustelut digitaalisesta rahasta, joka ei ole riippuvainen keskitetystä tahosta tai vakuuksista. Kaksi tärkeimmistä kokeiluista olivat b-money (1998) ja BitGold (2005). Nämä teoreettiset ideat, joita ei koskaan julkaistu käytännössä, olivat jo hyvin lähellä Bitcoinin designia. Julkinen/yksityinen avainpari (englanniksi “public/private key pair”) oli suunniteltu käytettäväksi salaukseen, ja tehdyn työn todistus (englanniksi “Proof-of-Work” tai “PoW”) oli käytössä uusien kolikoiden luomiseksi, Bitcoinin tapaan. Bitcoin konseptin kuvauksessa (englanniksi “white-paper”), Bitcoinin keksijä myös vahvistaa että hän oli tietoinen b-money:stä ja BitGold:ista.

B-money ja BitGold luottivat äänestysjärjestelmään konsensuksen saavuttamiseksi (sopimus siitä kuka omistaa kunkin rahayksikön kyseisellä hetkellä), joten ne olivat haavoittuvaisia vihamielisille hyökkäyksille jotka kykenivät manipuloimaan äänestyksiä ja siten vääristää omistuksia.

Tämä viimeinen ongelma, joka esti uuden internet rahan synnyn, ratkaistiin perjantaina 31.10.2008. Tänä päivänä Bitcoin white-paper, jossa Satoshi Nakamoto esitteli konseptinsa desentralisoidulle maksuverkolle, lähetettiin sähköpostilla Kryptopunkkareille. Kaksi kuukautta myöhemmin, 3.1.2009, Bitcoin tietoverkko aloitti toimintansa.

Ensireaktiot uutta Bitconin verkkoa kohtaan olivat laimeita. Muutamat intoilijat aloittivat verkon testaamisen ja bugien raportoinnin. Alussa, Satoshi Nakamoto oli verkon pääasiallinen ylläpitäjä. Mutta hitaasti uutiset uudesta “internet rahasta” alkoivat levitä tietokone- ja teknologiafoorumeilla ja kiinnostus Bitcoinia kohtaan kasvoi. Vuoden päästä Bitcoin verkolla oli jo käyttäjiä, mutta itse bitcoin kryptovaluutalla ei ollut mitään arvoa. (Kääntäjän huomio: Tässä käännöksessä käytämme sanaa “Bitcoin” kuvaamaan konseptia ja tietoverkkoa ja sanaa “bitcoin” kuvaamaan digitaalista rahayksikköä).

Kuka on Satoshi Nakamoto?

Bitcoin konseptin kuvaus, ja Bitcoin keksijän sähköpostiviestit, olivat allekirjoitettu nimellä Satoshi Nakamoto. Siitä huolimatta, Bitcoinin keksijän todellinen henkilöllisyys on edelleen mysteeri, sillä käytetty nimi vaikuttaa olleen salanimi. Ollessaan yhteydessä Bitcoin yhteisön kanssa, Nakamoto käytti ainakin kolmea kryptattua osoitetta salatakseen identiteettinsä.

Lukuisat ihmiset ovat väittäneet olevansa Satoshi Nakamoto, mutta tähän päivään mennessä kukaan ei ole pystynyt osoittamaan tätä todeksi. Kukaan ei ole esittänyt pitävää todistetta lähettämällä bitcoineja Satoshi Nakamotolle todennäköisesti kuuluneesta osoitteesta.

Lisäksi, vain pieni joukko ihmisiä kommunikoi “henkilökohtaisesti” Satoshi Nakamoton kanssa internetin välityksellä. Satoshi Nakamoto kirjoitti viimeisen viestinsä Bitcoin-yhteisölle 12.12.2010, mutta tämä ei ollut jäähyväisviesti. Hän vain lopetti julkisen kommunikoinnin tämän päivän jälkeen.

Nakamoto jatkoi yhteydenpitoa pienen koodarijoukon kanssa ja piti heidät ajan tasalla tulevasta kehityksestä. Mutta huhtikuussa 2011 hän lähetti viimeisen viestinsä myös tälle ryhmälle. Yhtä salaperäisesti kun hän ilmestyi 2008, hän katosi kolmen vuoden päästä.

Bitcoinin “Pizza päivä”

Miten Bitcoin sai alkuperäisen arvonsa? Aluksi, Bitcoinia saattoi louhia ja lähettää edestakaisin tietoverkon käyttäjien välillä, mutta digitaalisilla yksiköillä ei ollut reaalimaailman arvoa. Lisäksi, Bitcoin oli edelleen vain pienen harrastelijaryhmän käytössä.

Tämä muuttui 22.5.2010, kun erikoinen pyyntö ilmestyi bitcointalk.org keskusteluryhmään. 28-vuotias Laszlo Hanyecz Floridasta tarjosi kymmenentuhatta bitcoinia henkilölle, joka tilaisi kaksi pizzaa hänen kotiinsa. Kalifornialainen opiskelija otti haasteen vastaan ja tilasi kaksi pizzaa 41 dollarin hintaan Hanyeczin kotiin. Vastapalveluksena Hanyecz lähetti opiskelijalle kymmenentuhatta bitcoinia.

Tätä päivästä lähtien, päivää 22.5 on juhlittu “Bitcoin Pizza päivänä”. Tapahtumasta tuli kuuluisa, koska se vahvisti kolme asiaa:

- Bitcoinilla on arvoa
- Bitcoinia voidaan käyttää maksamiseen
- Bitcoin on disinflatorinen. Kiertoon tulevan bitcoinin määrä laskee tasaisesti, joka luo pohjan arvon kasvulle.

Nämä kaksi pizzaa tunnetaan maailman kalleimpina pizzoina. Joulukuun 2021 hinnoilla, niistä maksettiin 460 miljoonaa dollaria. Tämä on paljon rahaa, mutta kymmenen tuhannen bitcoinin vastaanottaja on jo käyttänyt ne. Haastattelussa, hän totesi että hän myi bitcoinit vähän ajan päästä rahoittaakseen autoreissun. Tämän päivän hinnoilla, kyseessä on todennäköisesti yksi maailman kalleimmista autoreissuista.

Bitcoin pizzapäivä demonstroi myös, miksi niin sanottu “hodlaaminen”, sovellettu englanninkielisestä ilmauksesta “to hold”, on niin suosittua Bitcoin yhteisön keskuudessa. Hodlaus tarkoittaa bitcoinin säästämistä pitkäksi ajaksi ja jopa aikomusta olla koskaan myymättä omaa bitcoin omistusta. Kukapa haluaisi käyttää bitcoininsa tänään, kun the voivat olla, kaksi, kolme, tai jopa kymmenen kertaa arvokkaampia tulevina vuosina?

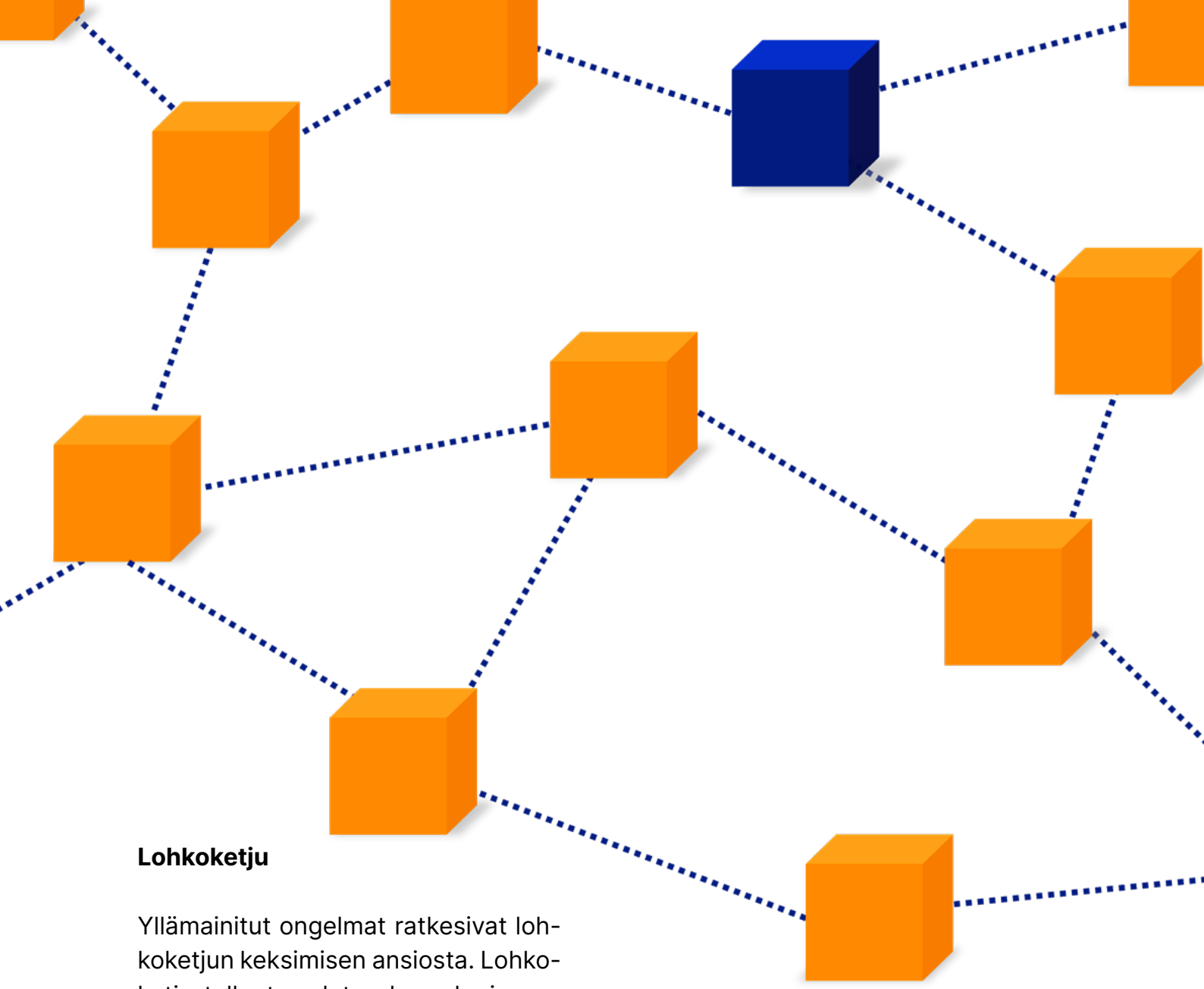
MITEN BITCOIN TOIMII?

Nyt kun olemme tutustuneet Bitcoinin historiaan, sukellamme sen toiminnan syövereihin. Tavoitteena on ymmärtää miten Bitcoin tietoverkko toimii, minkä ongelman se ratkaisee, ja mitkä ovat sen käytännön hyödyt.

Bitcoinin tavoite on olla desentralisoitu, eli uskottavasti hajautettu, tietoverkko. Yhdenkään tietoverkon käyttäjistä ei pitäisi pystyä hallitsemaan sitä itsenäisesti. Päinvastoin, päätöksenteko ja valvonta on jaettu kaikkien aktiivisten käyttäjien kesken. Tämä on tärkeää, koska yksikään henkilö, hallitus tai yhtiö ei voi muuttaa tietoverkkoa itsenäisesti, mutta kollektiivisesti sovitut muutokset ovat mahdollisia.

Bitcoin toimii siten, että jokaisella aktiivisella tietoverkon osallistujalla on identtinen kopio viimeisimmästä bitcoin omistusten tilikirjasta kaiken aikaa. Lopputuloksena, kaikki tietävät kuinka paljon bitcoinia kukin käyttäjä omistaa. Näin ollen kukaan Bitcoin käyttäjä ei voi esittää että hänellä on enemmän bitcoineja kuin todellisuudessa, koska kaikki tietoverkon käyttäjät voivat tarkistaa asian tilikirjasta ja todistaa virheellisen väitteen vääräksi.

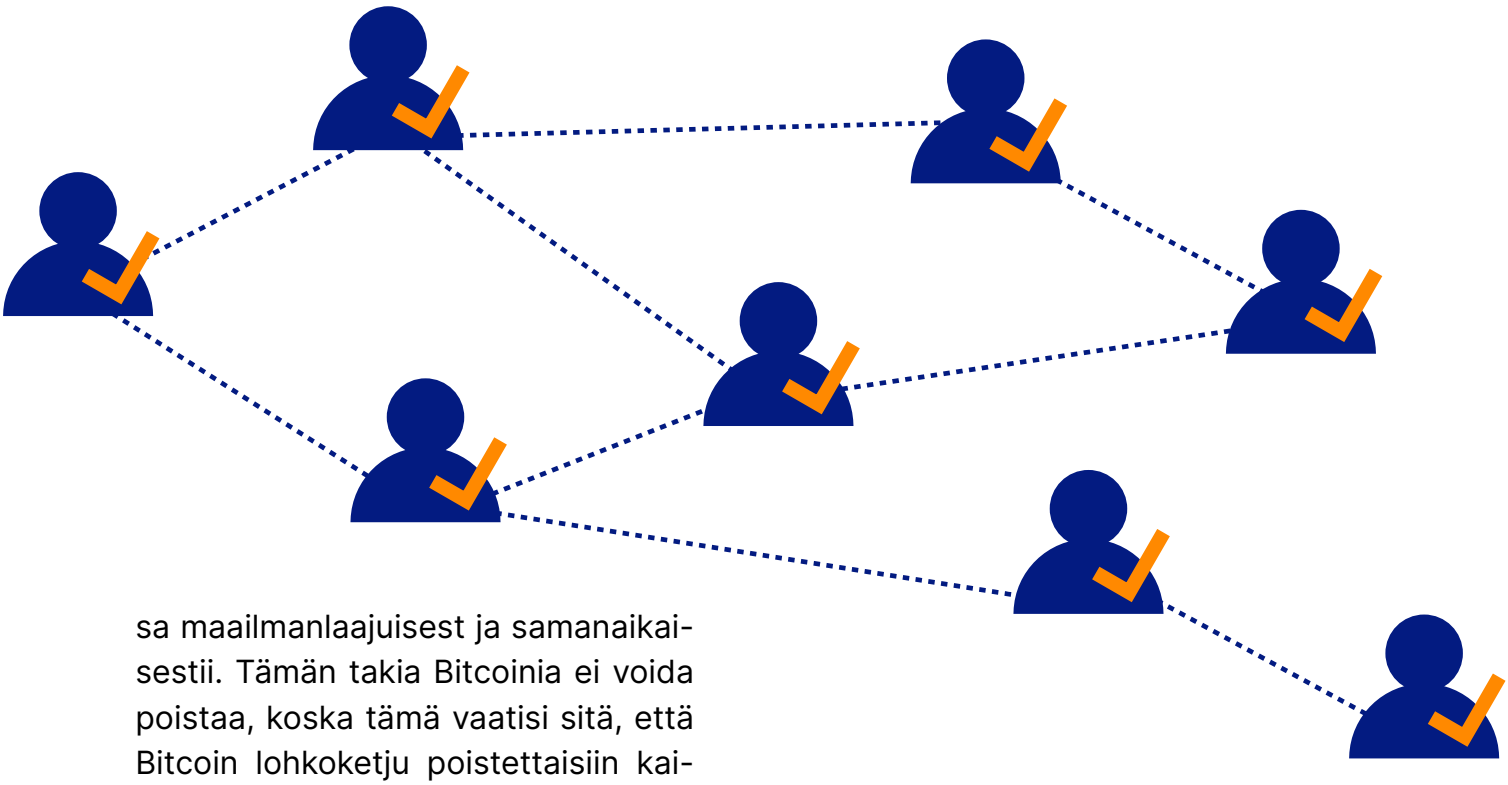
Ennen Bitcoinin julkaisua, desentralisoidut tietoverkot kohtasivat kaksi haastetta. Ensimmäiseksi, miten varmistetaan että kaikki tietoverkon käyttäjät vastaanottavat tiedot viimeisimmistä omistusmuutoksista. Toisin sanoen, tiedon siitä mitä bitcoinit ovat siirtyneet ja kenelle. Toiseksi, tietoverkon osallistujat voivat todistaa absoluuttisella tarkkuudella, että heidän vastaanottamansa tieto on totta.



Lohkoketju

Yllämainitut ongelmat ratkesivat lohkoketjun keksimisen ansiosta. Lohkoketju tallentaa dataa kronologisessa järjestyksessä. Bitcoinin tapauksessa, kaikki sen lanseerauksen jälkeiset transaktiot on tallennettu kronologisessa järjestyksessä sadoiksi tuhansiksi lohkoiksi, jotka yhdessä muodostavat lohkoketjun. Kuka tahansa tietoverkon käyttäjistä, joka haluaa tietää kuka omistaa minkäkin bitcoinin voi seurata transaktiohistoriaa Bitcoin lohkoketjussa ja tietää kuka omistaa minkäkin bitcoinin juuri tällä hetkellä. Näin ollen, jos joku haluaa lähettää bitcoinin, kaikki muut voivat tarkistaa että kyseinen bitcoin kuuluu juuri tälle henkilölle.

Tähän mennessä kuvatussa mekanismissa ei ole mitään uutta, koska pankit käyttävät samanlaista prosessia. Jos käyttäjä haluaa käyttää euron, pankki tarkistaa transaktiohistorian nähdäkseen kuuluuko kyseinen euro asiakkaalle, vai onko se jo käytetty, eli lähetetty jollekin muulle. Bitcoinin ainutlaatuinen piirre on, että tämä informaatio ei ole tallennettu pankin palvelimelle, vaan kaikkien aktiivisten verkon jäsenten tietokoneille (englanniksi “full node”) ja siten se elää kymmenissä tuhansissa tietokoneis-



sa maailmanlaajuisest ja samanaikaisestii. Tämän takia Bitcoinia ei voida poistaa, koska tämä vaatisi sitä, että Bitcoin lohkoketju poistettaisiin kaikista maailman Bitcoin tietoverkon tietokoneista samanaikaisesti.

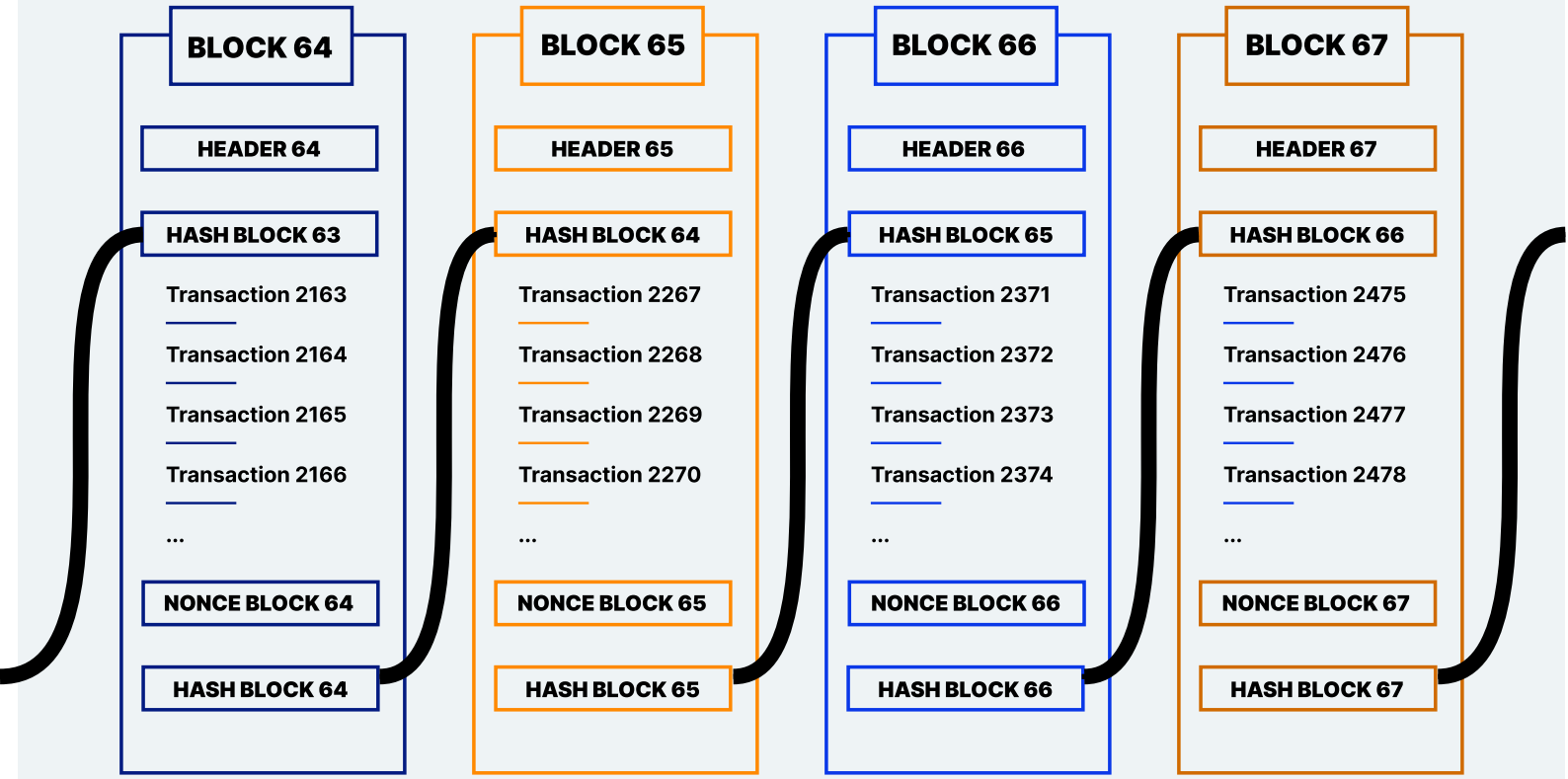
Lohkoketjuun liitettävien lohkojen todenmukaisuus pitää olla kaikkien todistettavissa. Verifiointi tapahtuu Bitcoin tietoverkon ohjelmistokoodin muuttumattomien sääntöjen avulla. Nämä säännöt määrittävät tarkasti mitkä transaktiot ovat sallittuja ja mitkä eivät. Jokainen Bitcoin tietoverkon käyttäjä, joka lataa kopion lohkoketjusta voi täten varmistaa noudattavatko kaikki transaktiot sovittuja sääntöjä. Jos transaktio ei noudata sääntöjä, se hylätään automaattisesti full node instanssien toimesta ja sitä ei liitetä lohkoketjuun.

Tehdyn työn todiste, eli Proof-of-Work louhinta

Bitcoin tietoverkko sisältää myös mekanismin, joka rajoittaa uusien lohkojen lisäystä lohkoketjuun. Jos kuka tahansa voisi lisätä lohkoja lohkoketjuun, tietoverkko vajoaisi kaaokseen, koska lohkoketju ei voisi päivittää itseään maailmanlaajuisesti riittävän nopeasti.

Estääkseen tämän, Bitcoin käyttää niin sanottua tehdyn työn todiste, eli Proof-of-Work (PoW), mekanismia. Yksinkertainen metafora konseptille on joukko ihmisiä joka etsii neulaa heinäkasasta. Se joka löytää neulan ensimmäisenä, saa oikeuden lisätä uuden lohkon lohkoketjuun. Uuden lohkon löytäjä saa palkkioksi bitcoin yksiköitä sekä lohkon sisältämiä transaktiomaksuja. Heti kun uusi lohko on lisätty ketjuun, prosessi alkaa uudelleen.

Käytännössä, louhijat toteuttavat matemaattista häsh-funktiota (SHA-256 algoritmi) etsiäkseen tiettyjä numeroita. Häsh numero edellisestä lohkosta, kyseisen lohkon transaktiot, ja satunnainen numero (englanniksi “nonce”) on niin sanotusti “häshätty” yhteen. Satunnaista numeroa vaihdetaan kunnes häsh-toiminto sylkee



„Header“ eli edellisen lohkon hash-funktion tulos, kaikki nykyisen lohkon tapahtumat ja „Nonce“ (satunnaisluku) asetetaan matemaattiseen funktioon. Nonce muuttuu, kunnes hash-funktion tuloksessa on tarpeeksi nollia. Tätä prosessia kutsutaan louhinnaksi.

ulos tuloksen, jossa on minimimäärä nollia alussa. Esimerkiksi, lohko numero 700000, joka luotiin 11.9.2021, perustui validiin häsh-numeroon 00000000000000000590fc0f3eba193a278534220b2b37e 9849e1a770ca959.

Tällä numeron etsinnällä, jota kutsutaan myös louhimiseksi, on kaksi tarkoitusta: Ensiksi, se liittää lohkot yhteen matemaattis-kyrptografisella tavalla, joka mahdollistaa sen, että kuka tahansa voi varmistaa järjestyksen oikeellisuuden. Samalla PoW mekanismi tekee järjestyksen muuttamisen liki mahdottomaksi. Toiseksi, mekanismi viivyttää uusien lohkojen lisäystä siten, että uusi lohko lisätään lohkoketjuun keskimäärin kymmenen minuutin välein. Tämä mahdollistaa sen, että kaikilla Bitcoin tietoverkon käyttäjillä on riittävä aika päivittää viimeisin lohkoketjun tila.

Yhteenvetona, louhijat pitävät Bitcoin tietoverkon käynnissä. Kiitos heidän, uudet transaktiot prosessoidaan ja lisätään lohkoketjuun. Full node instanssit tallentavat täyden kopion tilikirjasta sekä varmistavat että kaikkia sääntöjä noudatetaan, ja että epärehellisiä transaktioita ei lisätä lohkoketjuun.

21 miljoonaa bitcoinia

Vaikka uusia lohkoja lisätään jatkuvasti Bitcoin lohkoketjuun ja louhijat saavat palkkioksi bitcoineja, bitcoi-

nien lopullinen määrä on rajattu 21 miljoonaan. Maailmassa ei koskaan tule olemaan enemmän kuin 21 miljoona bitcoinia. Mutta nämä 21 miljoonaa bitcoinia eivät olleet jakelussa alusta lähtien. Päinvastoin, Bitcoin koodi lisää bitcoineja jakeluun perustuen tarkasti määriteltyyn aikatauluun.

Kun Bitcoin julkaistiin, koodi julkaisi 50 uutta bitcoinia louhijoille noin joka kymmenes minuutti. Neljä vuotta lanseerauksen jälkeen, kymmenen minuutin välein julistettujen bitcoinien määrä puolittui. Tämän prosessin nimi on puoliintuminen (englanniksi "halving"), joka kuvaa sitä, että louhijoille palkkioksi annettavien bitcoinien määrä puolittuu joka neljäs vuosi. Tällä hetkellä 19 miljoonaa bitcoina on jo louhitttu. Viimeiset kaksi miljoonaa bitcoinia louhitaan vuoteen 2140 asti. Sen jälkeen louhijat saavat palkkionsa vain transaktiomaksujen muodossa.

Tarkkaan rajattu bitcoinien määrä on yksi tämän kryptovaluutan perustavanlaatuisista ominaisuuksista ja tekee Bitcoinista erittäin niukan hyödykkeen. Tämä absoluuttinen digitaalinen niukkuus on myös tärkeä lähtökohta sille, että Bitcoin toimii arvontallennus instrumenttina pitkillä aikaväleillä, ja sitä usein kutsutaan digitaaliseksi kullaksi tai kulta 2.0:ksi.

Lopputulos: Digitaalinen omaisuus

Kun Bitcoinin useita ominaisuuksia tutkii kokonaisuutena, on mahdollista nähdä keksinnön laajempi merkitys. Ensimmäistä kertaa historiassa, maailmassa on digitaalinen hyödyke, jota on tarjolla vain tarkkaan rajattu määrä. Bitcoineja ei voi kopioida tai monistaa.

Tästä saavutuksesta johtuen, Bitcoinia kutsutaan usein "digitaaliseksi omaisuudeksi". Samoin kun jokainen pala maata maapallolla esiintyy vain kerran, jokainen bitcoin yksikkö esiintyy ainutkertaisesti digitaalisessa tilassa.

Lisäksi, bitcoin yksiköt ovat todella omistettavissa. Vain taho, jolla on kyseisen bitcoinin yksityinen avain (englanniksi "private key"), joka on yhdistelmä numeroita ja aakkosia, voi lähettää kyseisiä bitcoineja. Toisin sanoen, ilman tarvittavaa yksityistä avainta, bitcoineja ei voi varastaa, takavarikoida, tai jäädyttää. Tämä antaa omistajalle absoluuttisen hallinnan omiin taloudellisiin resursseihin, riippumatta ovatko he miljonäärejä, katukauppiaita tai poliittisia pakolaisia. Ensimmäistä kertaa tietokoneen keksimisen jälkeen on mahdollista todella omistaa digitaalista omaisuutta.

MIKSI BITCOIN?

Mutta mistä hype Bitcoinin ympärillä johtuu? Mahdollisuus omistaa digitaalista omaisuutta voi olla vallankumouksellinen. Mutta miksi kukaan haluaisi ylipäänsä omistaa bitcoineja?

Yhdistelmä kahdesta erinomaisesta asiasta

Menneinä vuosisatoina, ensin jalometallit ja myöhemmin setelit ja kolikot toimivat maksuvälineinä. Niiden etu oli että niitä voitiin säilyttää ja käyttää itsenäisesti ilman kolmansia osapuolia. Vanha sanonta “käteinen on painettua vapautta” kiteyttää tämän erinomaisesti. Samaan aikaan, kultaa, kolikoita ja seteleitä on vaikea käyttää digitaalisissa palveluissa. Online-shoppailun kasvu kautta, debit- ja luottokortit ovat saavuttaneet merkittävän markkina-aseman.

Nyt kun suurin osa ihmisistä käyttää digitaalista rahaa pankkitileiltään käteisen sijaan, vastapuoli-riskit ovat kasvussa. Esimerkiksi, jos finanssi-instituutio ajautuu maksukyvyttömäksi, asiakkaiden rahat saattavat kadota. Tai, kuten tapahtui Kyproksella 2013, jos käteisnostoja rajoitetaan voimakkaasti, pääomarajoitukset aktivoidaan, ja säästötileihin kohdistetaan pakkkolunastuksia, ihmiset eivät enää hallitse rahojaan.Vastaavasti, useiden länsimaiden asukkaat eivät voi lähettää rahaa omaisilleen jos he asuvat Kuubassa tai Iranissa. He ovat riippuvaisia kolmannesta osapuolesta transaktioiden hyväksymisen suhteen.

Muutos fyysisestä rahasta digitaaliseen rahaan on johtanut tilanteeseen jossa emme enää kontrolloi omaa rahaamme. Tähän päivään asti, se on ollut hinta siitä että voimme osallistua digitaaliseen elämään.

Bitcoin tarjoaa ratkaisun tähän dilemmaan. Digitaalisena rahana, se on ideaali ratkaisu digitaaliseen ma-

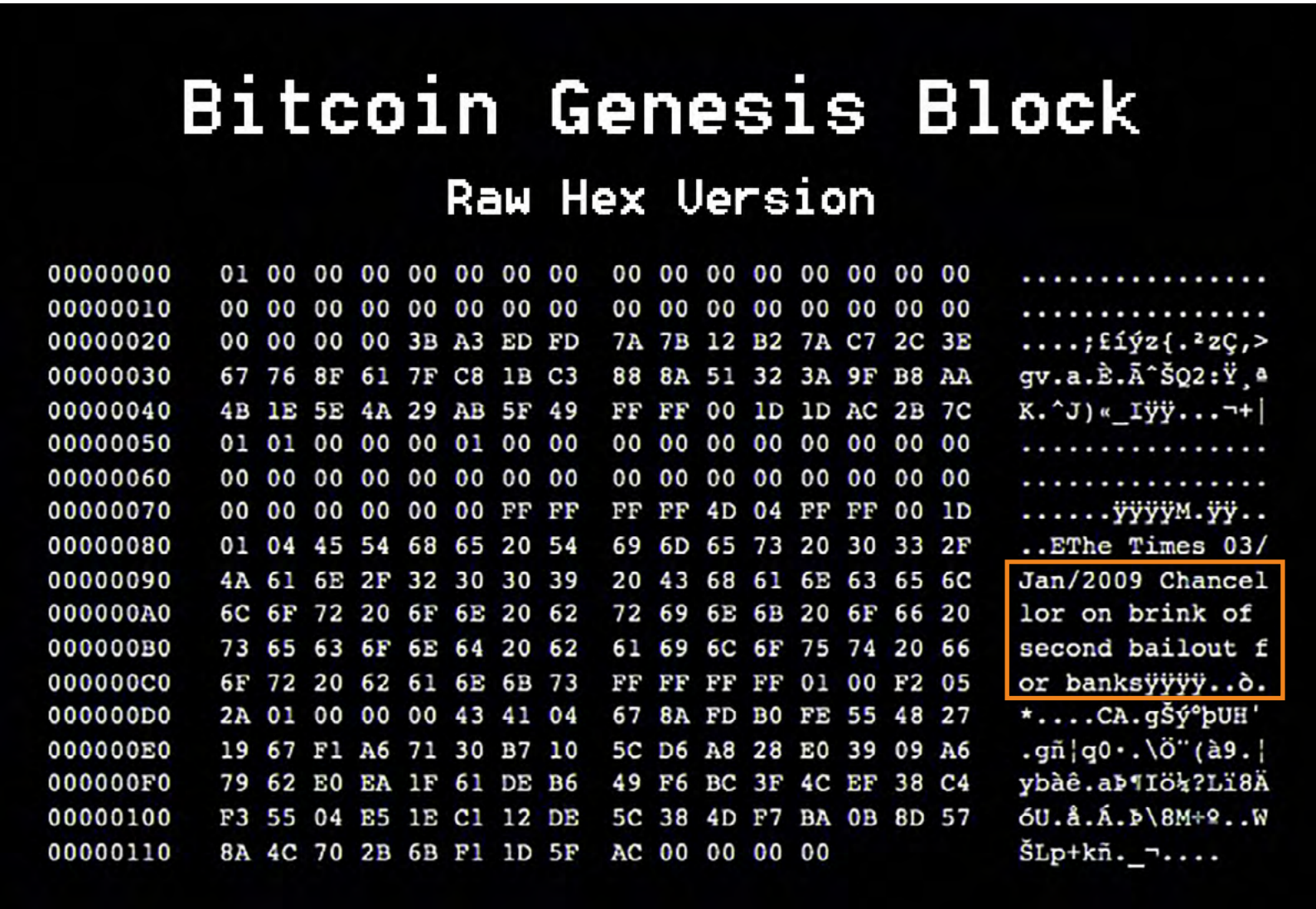
ailmaan. Samalla, Bitcoin voidaan tallentaa digitaalisena omaisuutena ilman riippuvuussuhdetta kolmansiin osapuoliin, kuten esimerkiksi pankkeihin, tallennuksen osalta. Näin ollen, bitcoiniin omistajat voivat tallentaa kolikkonsa - yksityisten avainten muodossa - tyynyn alle tai muuhun turvalliseen säilytyspaikkaan.

Täydellinen ajoitus

Bitcoin luotiin talouskriisin keskellä vuosina 2008 ja 2009. Bitcoinin ensimmäisessä lohkossa, niin sanotussa genesis-lohkossa, Satoshi Nakamoto julkaisi vahvan viestin. Hän viittasi The Times lehden otsikkoon: “Kansleri on toisen pankkien pelastuspaketin kynnyksellä”.

Tällä teolla, Satoshi ilmensi kryptopunkkareiden valtio-kriittistä filosofiaa. 2008 finanssikriisin aikana, keskuspankit ruiskuttivat valtavia määriä rahaa talouteen pelastaakseen pankit. Lopulta, tavalliset pankkien säästöasiakkaat maksoivat siitä, koska heidän säästöjensä ostovoima laski “rahasateen” vuoksi. Nämä tapahtumat vahvistivat kryptopunkareiden uskomusta siihen, että valtioihin ja keskuspankkeihin oli vaikea luottaa ja että valtioista riippumattomalle rahalle oli suuri tarve..

Sama toimintatapa, isommassa mittakaavassa, on toistettu Covid-19 pandemian alun jälkeen. Vuonna 2020 USA:n rahavaranto kasvoi 50%, ja muissa maissa - mukaan lu-



kien Sveitsi - digitaalinen rahaprintteri jauhaa jatkuvasti. Suora seuraus tästä ovat olleet alhaiset korot - jopa negatiiviset korot Sveitsissä - ja suuri arvopapereiden arvonnousu.

Vakuutus valuuttojen devaluaation varalta

Bitcoin lanseerattiin parhaaseen mahdolliseen aikaan. Nykyiseen rahajärjestelmään liittyvät kysymykset ovat harvoin olleet isompia kuin tänään. 21 miljoonan rajatulla lopullisella määrällä, Bitcoin tarjoaa selkeän vastakohdan keskuspankkien ikuisesti kasvaville tasekirjoille. Bitcoinin tarkkaan rajattu määrä tarjoaa suojan ostovoiman laskulle, joka on ollut nähtävissä maailman valuutoissa viime vuosikymmeninä.

Bitcoin on suunniteltu ostovoiman säilyttämiseksi pitkillä aikaväleillä. Koska Bitcoin on niukka hyödyke, sen pitäisi olla parempi tässä tehtävässä kuin kullan, jonka vuosittainen nettolisäys on 1-2%. Lisäksi, bitcoinin lähetys ja säilytyskulut ovat merkittävästi kultaa edullisemmat, joka tekee siitä paremman arvonsäilytyksen työkalun pitkällä aikavälillä.

Omaisuuden suojaaminen

Toinen asia, jonka Bitcoin ratkaisee on omaisuuden suojaus. Samalla kun kulta ja käteinen pitää tavallisesti merkittävin kustannuksin suojata varkauksilta, bitcoineja voi tallentaa ja lähettää lähes ilmaiseksi. Jopa merkittäviä summia voidaan viedä minne tahansa maailmassa 24 sanasta koostuvan koodin avulla. Kun koodi on painettu muistiin ja fyysiset todisteet on tuhottu, tätä koodia ei voi kukaan varastaa. Näin ollen koodin takana oleva bitcoin on turvassa ja sen omistaja voi halutessaan viedä ne jopa hautaansa.

OSTA BITCOINIA

On kaksi tapaa hankkia bitcoinia. Voit joko ansaita bitcoinia louhijana tai ostaa sitä joltain muulta. Koska louhiminen on nykyään liki mahdotonta kotitetokoneilla, jäljelle jäävä käytännöllinen tapa on ostaa bitcoineja.

Kryptopörssit ja -välittäjät

Helpoin tapa ostaa bitcoinia on kryptopörssin tai -välittäjän kautta. Nämä toimivat samaan tapaan kuin osakekauppa palvelut. Kun olet avannut henkilökohtaisen tilin, euroja voidaan siirtää palveluun omalta pankkitililtä tai luottokortilta. Kun raha on saapunut tilille, bitcoinia voi ostaa 24/7 muutamalla klikillä sen hetkiseen markkinahintaan. Euroopassa on mahdollista ostaa bitcoinia ilman rekisteröitymistä, tai ennakkotalletusta, suositulla Relai sovelluksella.

Vertaisverkko

Vaihtoehtona kryptopörsseille, bitcoinia voi ostaa myös vertaisverkkojen kautta. Tämä tarjoaa paremman anonymiteetin, koska mitään henkilökohtaista dataa ei tallenneta prosessin aikana.

Bitcoin pankkiautomaatit

On myös mahdollista ostaa bitcoinia erityisistä Bitcoin-pankkiautomaateista. Niitä on tarjolla useassa maassa, mukaan lukien Suomi, Sveitsi, Saksa ja Itävalta. Bitcoin pankkiautomaateista voi ostaa bitcoinia anonyymisti käteisellä tai luottokortilla. Et edes tarvitse olemassa olevaa tiliä tai kryptolompakkoa etukäteen.

Bitcoinin turvallinen säilytys

Kun olet hankkinut bitcoinia, herää kysymys sen turvallisesta käsittelystä ja säilönnästä. Bitcoin ja kryptovaluutat perustuvat periaatteseen “ei avaimia, ei kolikoita”. Voidaksesi aidosti omistaa bitcoinia sinun tulee omistaa niihin liittyvät yksityiset avaimet. Tämä jokseenkin tekninen ilmaisu tarkoittaa että sinulla todella on bitcoinia vain jos niihin liittyvät yksityiset avaimet on tallennettu itse hallitsemaasi digitaaliseen lompakkoon.

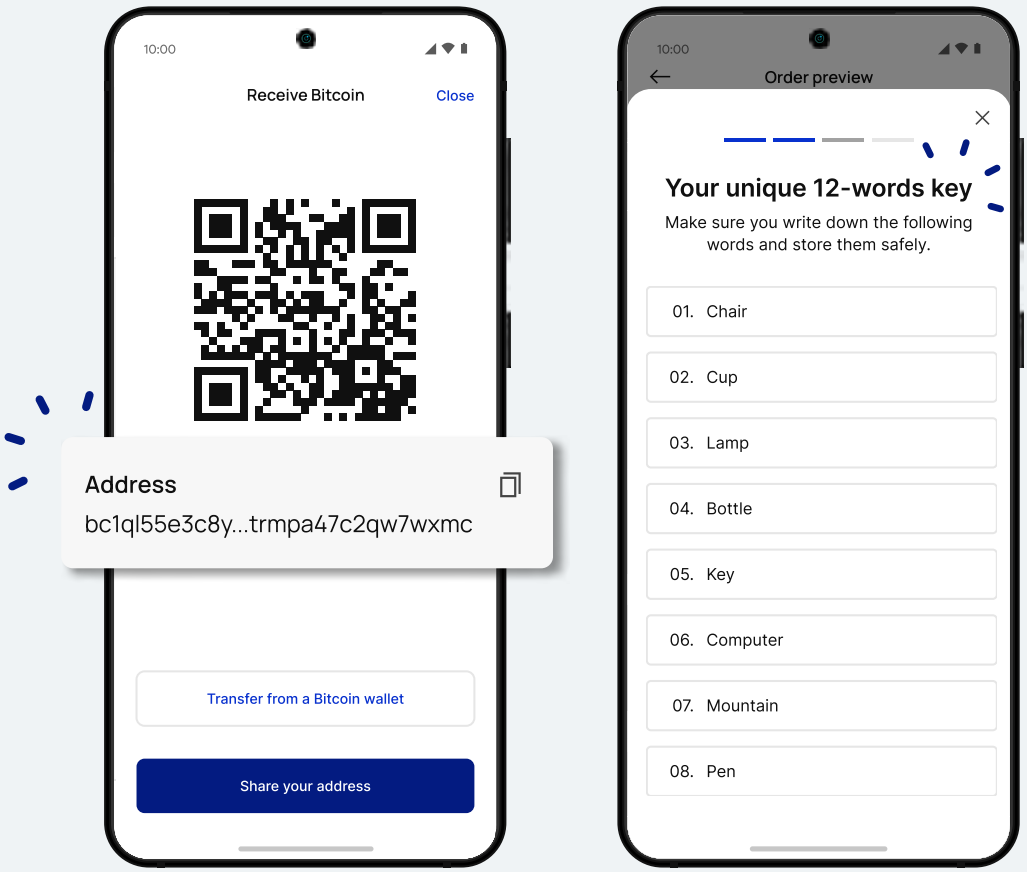
Niin kauan kuin bitcoin on tallennettu kryptopörssiin, ne ovat kyseisen pörssin hallinnassa. Jos pörssi joutuu tietomurron uhriksi, menee konkurssiin tai on huijaus, voit menettää bitcoinisi lopullisesti.

Itsenäinen hallinta

Toisin kuin pankkitilisi, Bitcoin antaa sinulle mahdollisuuden tallentaa rahayksiköt henkilökohtaiseen lompakkoon. Tämä antaa sinulle mahdollisuuden olla oma pankkisi ja täydellisesti oman bitcoinisi hallinnassa. Vastaavasti tämä tarkoittaa merkittävää vastuuta. Yksityinen avain, joka tyypillisesti koostuu 12 tai 24 sanasta, on tärkeää tallentaa turvallisesti. Huolimaton käsittely saattaa johtaa bitcoinin peruuttamattomaan menetykseen.

Lompakot: Digitaaliset lompakot

Digitaalisten lompakoiden avulla voit turvallisesti tallentaa bitcoinisi, tai tarkemmin, niihin liittyvät yksityiset avaimet. Bitcoinit itsessään ovat



aina tallessa lohkoketjussa ja niitä ei voi siirtää lompakkoon. Vain bitcoinin pääsykoodit, eli yksityiset avaimet, voidaan tallentaa lompakkoon.

Lompakot ovat siis tapa tallentaa yksityiset avaimen turvallisesti ja helposti. Lisäksi, ne mahdollistavat bitcoinin lähettämisen ja vastaanottamisen muutamalla napin painalluksella. Toisin sanoen, lompakot ovat hyödyllisiä työkaluja bitcoinin käsittelyyn.

Ohjelmistolompakko

Kaikkein tavallisimmat lompakot ovat ohjelmistolompakoita (englanniksi “software wallet”). Ne voidaan asentaa joko desktop-tietokoneelle tai sovelluksina älypuhelimiin. Käyttöönoton aikana, yksityiset avaimet esitetään 12 tai 24 sanan muodossa (siemenfraasi). Nämä sanat ovat synonyymi lompakossa olevalle bitcoinille. Kuka tahansa joka tietää nämä sanat, saa kyseiset bitcoinin hallintaansa. Siksi, sanat pitää kirjoittaa ylös analogisesti, mieluiten paperille, salassa ja säilyttää turvallisessa paikassa. Jos tietokoneesi tai älypuhelimesi koskaan katoaa, lompakon saa palautettua milloin tahansa näiden siemenfraasi-sanojen avulla.

Ohjelmistolompakoiden etu on nopea asennus ja helppokäyttöisyys. Mutta, koska ne ovat ohjelmistoja ja yhteydessä internettiin, niiden käyttöön sisältyy aina tietomurron riski.

Laitelompakko

Jos arvostat korkeaa turvallisuusastetta, sinun kannattaa käyttää niin sanottua laitelompakkoa (englanniksi “hardware wallet”). Nämä pienet laitteet tallentavat bitcoin pääsykoodit USB-tikun tapaiselle laitteelle joka kytketään tietokoneeseen vain tarvittaessa. Laite on suunniteltu niin, että edes tietokone jossa on haitta-ohjelma-infektio ei pääse yksityisiin avaimiin käsiksi.

Kun laitelompakko asennetaan, luodaan 12 tai 24 sanaa (siemenfraasi), jotka pitää kirjoittaa ylös analogisesti ja säilyttää turvassa. Jos lompakko joskus katoaa, se voidaan palauttaa näillä sanoilla. Esimerkkejä laitelompakoista ovat muun muassa BitBox ja Trezor.

Made in Switzerland

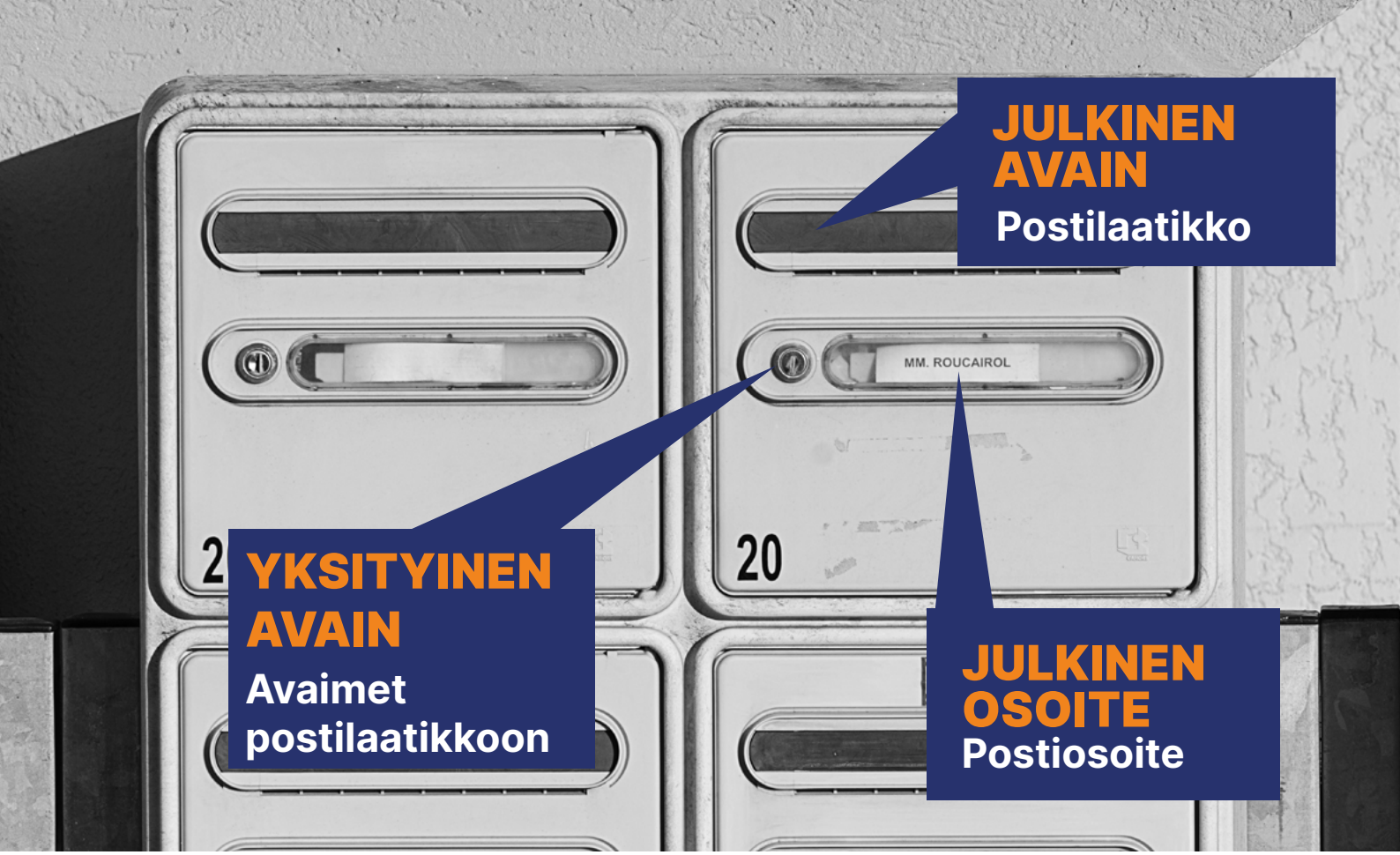
EUROPE'S EASIEST BITCOIN APP

Relai

Download on the App Store

GET IT ON Google Play

Buy bitcoin in 1 minute from as little as 10 EUR/CHF without verification.



Lähetä ja vastaanota bitcoinia

Bitcoinin lähettäminen ja vastaanottaminen on hyvin helppoa. Jokaisella bitcoin lompakolla on julkinen osoite joka on luotu niin sanotusta julkisesta avaimesta. Tämä toimii lähetysosoitteena, samaan tapaan kuin IBAN pankkimaailmassa. Kuka tahansa, jolla on tämä osoite voi lähettää sinne bitcoinia. Osoite esitetään usein QR-koodina, joka helpottaa käyttökokemusta.

Jos haluat lähettää bitcoinia jollekin henkilölle, voit joko liittää vastaanottajan bitcoin osoitteen lompakossasi "lähetä" ominaisuuden alla tai skannata osoitetta kuvaavan QR-koodin. Transaktiomaksut vähennetään automaattisesti lähettäjän lompakosta. Transaktiomaksut vaihtelevat johtuen tietoverkon kulloisesta käyttöasteesta ja voidaan tarkistaa täällä. Jokainen lähetys kestää keskimäärin noin 10 minuuttia, perustuen valitsemaasi transaktiokulujen tasoon. Lähetys voi myös kestää pidempään, jos lähettäjä haluaa maksaa vain vähän transaktiokuluja.

Maksa bitcoinilla

Kun Bitcoin luotiin, monet toivoivat että sitä voitaisiin jonain päivänä käyttää arkipäivän maksutapahtumiin. Joidenkin paikkakuntien vero-toimistot, voittoa tekemättömät organisaatiot, ja kasvava määrä yhtiöitä hyväksyy jo bitcoinin käytön maksuvälineenä. Mutta koska perinteiset bitcoin transaktiot usein maksavat useita euroja ja kestävät noin 10 minuuttia, ne toimivat parhaiten isommissa maksuissa. Bitcoinin halpaan

ja nopeaan lähettämiseen tarvitaan toinen ratkaisu.

Salamaverkko - nopeammin ja edullisemmin

Bitcoin tietoverkon päälle on rakennettu uusi kerros hoitamaan nopeat ja edulliset maksut. Tämä verkko, nimeltään Salamaverkko (englanniksi "Lightning Network"), mahdollistaa maksut sekunneissa ja liki ilmaiseksi. Esimerkiksi El Salvadorissa Salamaverkko on jo aktiivisessa käytössä.

Tulevaisuudessa suuri osa arkipäivän maksutapahtumista tullaan tekemään Salamaverkossa. Kehitys tällä saralla etenee nopeasti. Internet-palvelu Twitter julkaisi hiljattain Salamaverkkoon pohjautuvan juomaraha-ominaisuuden. Lisäksi, USA:lainen Strike sovellus tarjoaa maailmanlaajuisia maksuja eri valuutoissa ilmaiseksi Salamaverkon avulla. Asiantuntijat ennakoivat että tulevaisuudessa isommat transaktiot tapahtuvat Bitcoin tietoverkossa ja pienemmät transaktiot tehdään Salamaverkossa.

Yksi bitcoin koostuu sadasta miljoonasta satoshista. Koska Salamaverkossa tehdään lähinnä pieniä maksuja, mittayksikkönä käytetään satosheja (lyhennys "sat"). Salamerkon käyttö edellyttää Salamaverkkoa tukevan bitcoin-lompakon käyttöönottoa.

KATSE TULEVAISUUTEEN

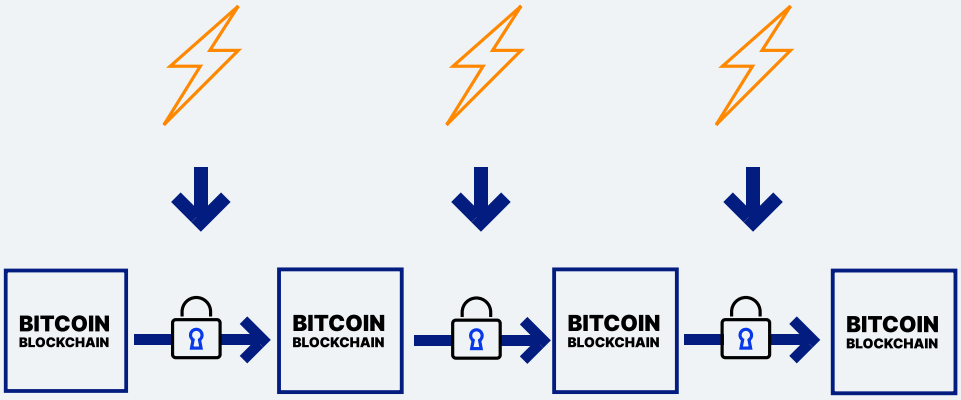
Yli kymmenvuotisen historiansa aikana Bitcoin on läpikäynyt useita huippuja ja pohjia. Tämä kryptovaluutta on julistettu kuolleeksi useita kertoja kun sen hinta on pudonnut radikaalisti. Samalla, Bitcoin on levinnyt peruuttamattomasti ympäri maailmaa.

Bitcoin ja energia

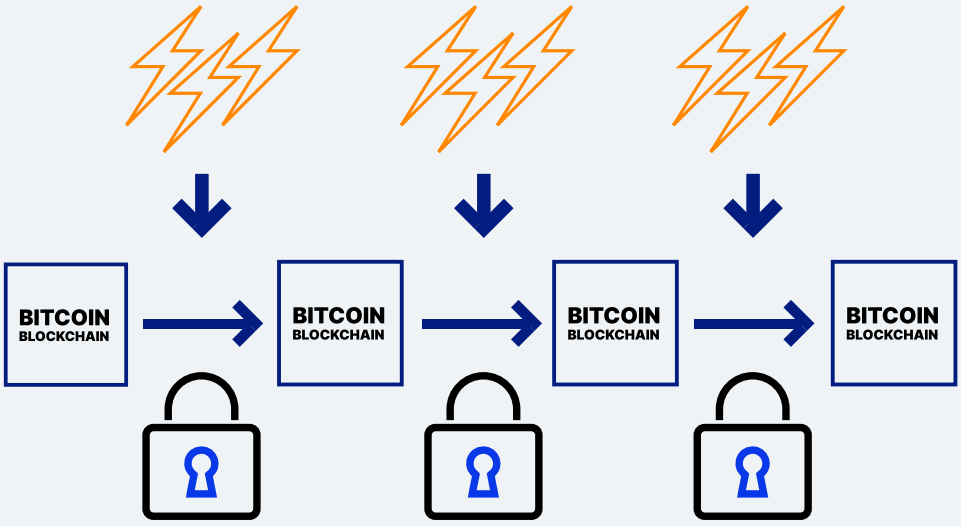
Energiankulutus on yksi tyypillisistä huolista joka nousee esiin koskien Bitcoin tietoverkon kehitystä. Bitcoinien louhinta kuluttaa merkittävän määrän energiaa maailmanlaajuisesti. Ja tämä kulutus todennäköisesti kasvaa kun yhä useampi taho alkaa louhia bitcoinia.

Kun puhutaan Bitcoinin energiankäytöstä, on tärkeää huomioida että tietoverkkoon virtaava energia on välttämätön sen turvallisuuden takaamiseksi. Mitä enemmän energiaa

Mitä vähemmän laskentatehoa käytetään Bitcoin-lohkoketjun rakentamiseen, sitä helpompi sitä on myöhemmin muuttaa.



Mitä enemmän energiaa laskentatehoon käytetään Bitcoin-lohkoketjun luomiseen, sitä vaikeampi sitä on myöhemmin muuttaa.



virtaa verkkoon, sitä turvallisempi se on. Jos joku taho haluaisi muuttaa Bitcoin lohkoketjua vihamielisesti, pitäisi sen käyttää uudestaan sama ohjelmointivoima joka tarvittiin lohkoketjun luontiin ennen hyökkäystä. Koska miljoonat tietokoneet maailmassa tarjoavat laskentatehoa Bitcoin tietoverkolle, yksityishenkilön tai organisaation on liki mahdotonta kasata riittävästi tehoa edes minimaalisten muutosten tekemiseksi. Siksi, valtava häshing-teho ja siihen liittyvä energiankulutus, ovat Bitcoinin välttämättömiä turvallisuusominaisuuksia.

Lisäksi, Bitcoin louhintaan käytettävät tietokoneet voidaan sijoittaa minne tahansa maailmassa. Koska louhijat tarvitsevat edullisinta mahdollista sähkö ollakseen tuottavia, he usein sijoittuvat paikkoihin joissa on merkittäviä ylijäämiä, toisin sanoen hyvin edullista sähköä. Pitkällä tähtäimellä louhinta sijoittuu todennäköisesti paikkoihin joissa on paljon uusiutuvaa energiaa, sillä se on usein edullisin tapa tuottaa sähköä.

Bitcoin Mining Council-organisaation mukaan louhijat käyttävät parhaillaan noin 56% uusiutuvaa energiaa ja trendi on kasvussa. Useat Bitcoin

ekspertit uskovat louhinnan perustuvan 100% uusiutuvalle energialle tulevaisuudessa. Ennen tätä, Bitcoinin energiankulutuksen arviointi kiteytyy kysymykseen onko turvallinen ja väärentämätön raha, ja arvon säilyttäjä, tämän energian kulutuksen arvoista vai ei?

El Salvador - Bitcoin kansallisena valuuttana

Joitain vuosia sitten, vain visionäärit pitivät mahdollisena että Bitcoin voisi joskus olla kansallisvaltion laillinen valuutta. Kesällä 2021 tämä aika koitti: El Salvador oli ensimmäinen maa joka julisti Bitcoinin lailliseksi maksuvälineeksii. Kaupoissa, ravintoloissa ja kaikenlaisissa palveluissa, maksun voi tehdä sekä dollareilla tai bitcoineilla. Tätä tarkoitusta varten kansalaisille tarjottiin bitcoin lompakko, joka mahdollistaa maksut Salamaverkon välityksellä sekunneissa ja liki ilmaiseksi.

Muut maat, kuten Ukraina, Brasilia ja Panama keskustelevat parhaillaan samantyyppisistä laeista. Jos muut maat seuraavat El Salvadorin esimerkkiä, tämä sekä lisäisi Bitcoinin käyttöä että sen uskottavuutta "rahana". Bitcoinin hyväksyminen lailliseksi valuutaksi useammissa maissa edustaa siis merkittävää vaihetta Bitcoinin maailmanlaajuisessa leviämisessä.

Lait ja säädökset

Yllämainittu kehitys on johtanut siihen, että kansallisvaltiot, keskuspankit ja yhtiöt joutuvat ottamaan kantaa kryptovaluuttoihin. Usea maat, kuten Sveitsi, ovat julkaiseet säädöksiä ja ohjeistuksia kryptovaluuttoihin liittyen. Tämä kehitys on ollut tervetullut useiden markkinatoimijoiden kannalta, joska se luo oikeudellista selkeyttä sekä krypto-projekteille että sijoittajille.

Säädökset ovat näköpiirissä myös Yhdysvalloissa, joka on toistaiseksi ottanut laissez-faire-tyyppisen asennoitumisen. Näiden säädösten lopullinen muoto on suuri kiinnostuksen kohde krypto-yhteisölle, sillä niillä on iso vaikutus koko teollisuudenalaan maailmanlaajuisesti.

Muut kryptovaluutat

Bitcoin ei ole ainoa kryptovaluutta, sillä maailmassa on yli 16000 kryptovaluuttaa. Nämä kolikot ja tokenit omaavat erilaisia ominaisuuksia ja toiminnallisuuksia ja suurta osaa ei olla suunniteltu "valuutaksi" tai rahaksi. Osa on lähempänä osaketta koska niiden arvo on sidottu kyseisen krypto-projektin menestykseen. Toisia tarvitaan tietyn palvelun käyttöön. Ja osa tokeneista on luotu pääasiassa huumorilla (englanniksi "meme tokens").

Tappioiden välttämiseksi on suositeltavaa katsoa kutakin kryptovaluuttaa hyvin tarkkaan ennen kuin sijoittaa niihin.

CBDC - Keskuspankkien laskema digitaalinen valuutta

Kryptovaluutat ovat siirtymässä säätelemättömästä villi länsi-vaiheesta säädeltyyn krypto-finanssipalveluiden maailmaan. Tämä kehitys ei ole jäänyt keskuspankeilta huomaamatta, ja esiin on noussut idealuoda omia kryptovaluuttoja keskuspankeille(Englanninkielinen “CBDC” lyhenne on standardi). Nämä CBDC:t pyrkivät yhdistämään kansallisten valuuttojen vakauden ja lohkoketju-pohjaisen virtuaalivaluutan edut. Tavoitteena on siis digitaalinen versio käteisestä.

Riippuen suunnitteluperiaatteista, CBDC:t voivat esiintyä hyvin erilaisissa muodoissa. Monet maat ovat tehneet CBDC-pilotteja ja muutama maa on julkaissut virallisen CBDC:n. Tällä hetkellä odotetaan kiinnostuksella minkälaisia CBDC-projekteja taloudellisesti vahvat talousalueet, kuten USA, EU ja Kiina, julkaisevat tulevaisuudessa.

Kilpailu rahan muodosta

Yhteiskuntamme on perustunut keskuspankkien luomaan rahaan niin pitkään, että poikkeavat rahan muodot olivat hädin tuskin kuviteltavissa ennen viime vuosia. Ennen keskuspankkien luoman rahan aikakautta, oli arkipäivää että erilaiset rahamuodot kiersivät samanaikaisesti taloudessa. Eri pankit julkaisivat omia pankkinoottejaan, kolikoita tehtiin eri metalleista, ja myös muita rahallisia arvoja voitiin käyttää maksamiseen.

Bitcoinin myötä, keskuspankeista riippumaton valuutta on taas vaihtoehto. Tähän asti suurin osa valtioista on hyväksynyt Bitcoinin olemassaolon. Osittain tämä johtuu sen desentralisoidusta luonteesta, joka tekee siitä erittäin hankalasti tuhottavan kohteen. Kansalaisille tämä tarkoittaa sitä, että kullalle ja hopealle on nyt olemassa digitaalinen vaihtoehto. Rahan muotojen kilpailu tulee olemaan mielenkiintoista katsottavaa tulevaisuudessa.

MITÄ SEURAAVAKSI?

Jos kysyt itseltäsi mitä tulisi tehdä kaikella tällä tiedolla, anna minun tehdä suositus: Bitcoin maailmaan astuminen ei maksa mitään, ei aikaa eikä rahaa. Mutta vastineeksi saat tutustua teknologiaan, joka kohta muuttaa maailman tulevaisuuden.

Ehdotan seuraavaa: luo tili kryptopörssiin tai lataa lompakko älypuhelimeen ja ostaa bitcoinia 50 eurolla. Tai pyydä tuttua lähettämään hieman muutaman euron edestä bitcoinia lompakkoosi. Hanki käsiisi hiukan bitcoinia ainakin yhden kerran.

Jos Bitcoin tekee samanlaisen läpimurron kuin internet teki, niin sinulla ei ole pelkkää teoreettista tietoa vaan olet myös käyttänyt bitcoinia itse. Tämä saattaa hyvinkin laittaa sinut edulliseen asemaan verrattuna suurimpaan osaan maailman ihmisistä.

ABOUT

KIRJAILIJASTA

Daniel Jungen on taloustieteilijä ja talousjournalisti, jolla on asiantuntemusta kryptovaluutoista. Daniel on InsightDeFi krypto-asioihin keskittyvän tutkimus putiikin kanssaperustaja. Partnereidensa kanssa he julkaisevat kaksi kertaa kuukaudessa julkaistavaa uutiskirjettä Bitcoinista, DeFi:stä ja kryptosta.

RELAI YHTIÖSTÄ

Sveitsiläinen Julian Liniger ja Adem Bilican yrittäjäparivaljakko perusti Relai yhtiön kun he eivät löytäneet turvallista ja helppokäyttöistä paikkaa ostaa bitcoinsslia. Relai tekee bitcoin säästämisen ja sijoittamisen helpoksi. Tämä ainoastaan Bitcoiniin keskittyvä sovellus on suunniteltu olemaan yksinkertainen ja intuitiivinen. Se antaa jokaisen eurooppalaisen osaa ja myydä bitcoinia minuuteissa, ilman rekisteröitymistä. Riippumattomasti auditoitu, ja yli 35 miljoonaa sveitsin frangia sijoitettu alustan kautta, Relai antaa kuluttajille mahdollisuuden käyttää uusia säästämisen ja sijoittamisen muotoja.

Opi lisää Relai:n sivuilla

Käännös englannista suomeksi @thehigherlow - Acoustic Pleb Rock https://www.thehigherlow.com/