elastos white paper

Smart-web powered by blockchain

Valmisteltu Elastos-säätiön toimesta

Tammikuu 1, 2018

Kuvaus

Tämä dokumentti on Elastos white paperin verio 0.2, joka sisältää lisätietoja Elastosin strategisista tavoitteista ja teknologian etenemissuunnitelmista. Elastos pitää whitepaperinsa päivitettynä, jotta kehitystä voidaan seurata. Uusimmat tiedot Elastosin white paperista, etenemissuunnitelmista, tiimistä, säätiöstä, sijoittajista ja strategisista kumppaneista löytyvät Elastosin viralliselta verkkosivulta:

https://www.elastos.org

Yhteystiedot

Elastos säätiö:

Elastos (Shanghai)

The 11th floor, Huahong International Building

NO. 463 the Tanggu Road, Hongkou District

Shanghai, China 200080

Elastos (Beijing):

Plug & Play, Building G

Zhongguancun Yingzao Street

No. 45 Chengfu Road, Haidian District

Beijing, China 100084

Sähköposti:

Whitepaper ryhmä: whitepaper@elastos.org

Kansainvälinen yhteisö: global-community@elastos.org

Elastos rahasto: Elastos-fund@elastos.org

PR: pr@elastos.org

IR: ir@elastos.org

Elastos neuvosto : elastos-council@elastos.org

Muut: contact@elastos.org

Elastos-säätiö on rekisteröity Singaporeen.

Tekijänoikeusilmoitus

Vastuuvapauslauseke

Elastos kehittää jatkuvasti teknologiaansa ja organisaatiorakennettaan, mutta pyrkii säilyttämään Elastos-yhteisön nykyiset hallintoperiaatteet sekä Elastos tokeneiden jakelusuunnitelman.

1. Johdanto Elastosiin

Elastos pyrkii luomaan uudentyyppisen internetin, joka toimii lohkoketjuteknologiaa hyödyntäen. Tässä uudenlaisessa internetissä ihmiset voivat omistaa digitaalisia hyödykkeitä (digital assets), mikä mahdollistaa niille arvon. Nykyään tarjolla on rajaton määrä digitaalisia kirjoja, elokuvia, musiikkia ja pelejä, mutta Ihmiset eivät välttämättä omista niitä. Esimerkiksi, voit ostaa digitaalisen kirjan, mutta et voi myydä sitä kenellekkään. Voidaanko silloin puhua todellisesta omistamisesta? Elastos pyrkii mahdollistamaan digitaalisten hyödykkeiden rajallisen määrän, jolloin niitä voi myydä tai vaihtaa. Omistusoikeus taas mahdollistaa varallisuuden luomisen ja Elastosin tarkoitus onkin rakentaa uudenlainen internet, joka kunnioittaa omistusoikeutta.

Tavoitteena on luoda internet, jonka avulla käyttäjät pääsevät käsiksi artikkeleihin, elokuviin ja peleihin ilman välikäsiä. Elastos käyttää lohkoketjuteknologiaa myöntäessään ID:n digitaaliselle sisällölle, näin voidaan määritellä sisällön omistaja. Elokuvantekijät voivat esimerkiksi seurata kuinka monta kertaa heidän elokuvaansa on katsottu. Elastosin ja lohkoketjuteknologian yhdistelmä luo perustan luotettavalle ja turvalliselle, uudenlaiselle internetille (Internet of Wealth).

Elastos tulee olemaan alusta hajautetuille sovelluksille (Dapps), jotka toimivat vertaisverkossa (peer-to-peer network) ilman keskitettyä valvontaa. Ihmiset voivat käyttää näitä hajautettuja sovelluksia matkapuhelimillaan vaihtamatta käyttöjärjestelmäänsä. Vanha internet on tiedon verkko (Web of information). Kun klikkaat URL-osoitetta, saat tietoa. Elastos luo sovellusten verkkoa (Web of apps). Kun klikkaat URL-osoitetta, saat koodin. Elastos-verkko on uudenlainen ekonominen ympäristö, jossa Elastosin kryptovaluutta (ELA) toimii keskusvaluuttana.

Elastos on avoimen lähdekoodin ohjelmisto, jonka kehitystä ovat sponsoroineet talousjätit, kuten Tsinghua Sciene Park, TD-SCDMA Industrial Alliance ja

Foxconn Group, Yli miljoonalla RMB:llä (n. 26 miljoonaa euroa). Elastos on julkaissut yli kymmenen miljoonaa riviä lähdekoodia, mukaan lukien neljä miljoonaa riviä alkuperäistä lähdekoodia.

2. Tekninen tausta

Bitcoin lohkoketju on hajautettu, muuttumaton kirjanpito, joka mahdollistaa luottamuksen siirtämisen tiedon muotoon. Ethereum toteutti ohjelmoitavan lohkoketjun, joka tukee älysopimuksia (smart contracts). Tämä mahdollisti luottamuksen siirtämisen koodiin. Yksinkertaistettuna, älysopimukset mahdollistavat liiketoimien suorittamisen automaattisesti kun sopimusvelvoitteet täyttyvät. Esimerkiksi, myyjät saavat rahansa vasta kun myytävä tuote on toimitettu ostajalle onnistuneesti. Yritykset jotka järjestävät joukkorahoituksen, kykenevät aloittamaan toimintansa vasta, kun tietty määrä rahaa on kerätty. Muussa tapauksessa rahat palautuvat rahoittajille.

Älysopimusten ansiosta meidän ei tarvitse huolehtia sopimusrikkomuksista tai osapuolten luottoluokituksista, koska lohkoketju suorittaa siirrot vasta kun molemmat osapuolet ovat täyttäneet asetetut ehdot. Tämä järjestelmä poistaa epäluottamuksen myyjän ja ostajan väliltä. Kysymys kuuluu, kuinka voimme soveltaa älysopimusjärjestelmää entistä laajemmalle kirjolle yrityksiä? Voisimmeko käyttää sitä sähköisessä kirjakaupassa, tai videopelien ja elokuvien kaupankäyntialustassa?

Ethereumin älysopimukset ovat hyödyllisiä, kun niitä sovelletaan rahoitus hankkeissa, sekä verkossa tapahtuvassa äänestyksessä. Elastos kuitenkin uskoo, että Ethereumin hajautetut sovellukset sisältävät seuraavia rajoitteita:

- Tallennuskapasiteetti ja nopeus. Tallennuskapasiteetti rajoittuu itse lohkoketjuun, joka pystyy tallentamaan vain rajallisen määrän tietoa ja on hyvin nopeusrajoitteinen. CryptoKitties pelin suosio aiheutti ruuhkan Ethereumin lohkoketjussa. Tämä toi esiin ongelman, joka aiheutuu siitä että älysopimukset suoritetaan pelkästään pää-lohkoketjussa.

- Virheet. Älysopimukset eivät ole pysäytettävissä tai oikaistavissa jälkikäteen. Tämä sinällään on loogista ja suojaa molempia osapuolia. Hyväksyttäessä sopimus, sitä ei voida perua tai muuttaa. Älysopimukset eivät kuitenkaan ole virheettömiä (esim. DAO hyökkäykset). Onkin mahdottomuus todistaa jokin ohjelma täysin virheettömäksi.

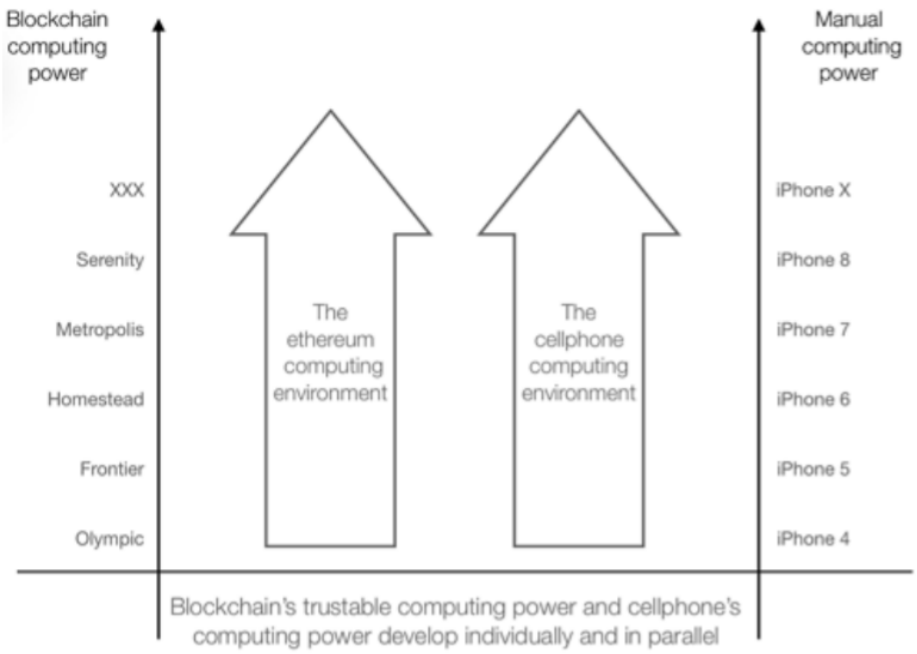
- Hinta. Tällähetkellä älysopimukset, tiedon tallentaminen ja sopimusten toimeksipano tapahtuu lohkoketjussa. Tämä tarkoittaa, että useat nodet toistuvasti suorittavat samoja tehtäviä. Ethereum vaatii maksun jokaisesta suoritetusta tehtävästä, joten tehtävien suorittaminen voi tulla kalliiksi.

- Roskadata. Ethereumin lohkoketjuun tallentuu roskadataa. Julkaisun jälkeen älysopimus tallentuu lohkoketjuun jonka jälkeen sitä ei voi poistaa. Tämä aiheuttaa roskadatan kertymisen lohkoketjuun, josta syystä lohkoketjun tehokkuus pienenee ja se ruuhkautuu.

- Joustamattomuus. Lohkoketjun ja EVM:n (Ethereum Virtual Machine) välinen yhteys, jossa älysopimukset tapahtuu, on erottamaton. Lohkoketjun päivitys vaikuttaa EVM:ään ja toisinpäin.

- Turvallisuus. Älysopimukset, jotka tapahtuvat Ethereumin tai Ethereumin kaltaisissa järjestelmissä ovat alttiita mies välissä -hyökkäyksille (middleman attacks). Tämä voi tapahtua kun tieto siirtyy lohkoketjusta ulkoisille nettisivustoille.

Edellä meinittujen ongelmien vuoksi Elastos uskoo, että on vaikeaa ja epäkäytännöllistä lukea sähköisiä kirjoja, pelata pelejä ja keskustella suojatusti ethereumin älysopimusten kautta. Ihmiset ovat tottuneet käyttämään sovelluksia matkapuhelimissaan. Elastosin tavoite on mahdollistaa pääsy lohkoketjuun perustuviin ohjelmistoihin nykyisillä mobiililaitteilla, joita ihmisillä on jo käytössään.



Kuten yllä olevassa kaaviossa todetaan, käyttäjän matkapuhelimen teho ei nopeuta Ethereumin laskentaa. Ei ole merkitystä kuinka monta päivitystä Ethereumiin tehdään, sen luotettavuus ei ulotu ihmisten päivittäiseen matkapuhelinten käyttöön. Tämä johtuu siitä, että Ethereumin ja matkapuhelimen laskenta on kehitetty rinnakkaiseksi, ei integroiduksi.

Nykypäivän älysopimukset ovat suunniteltu toimimaan lohkoketjussa. Elastosissa lohkoketju mahdollistaa Dappejen (decentralized applications) käytön, mutta Dappejen itsessään ei tarvitse toimia lohkoketjussa. Elastos mahdollistaa käyttäjilleen Dappejen käytön heidän nykyisten käyttöjärjestelmiensä kautta. Dappit toimivat Elastos runtimessa, joka pyörii Androidin, iOS:än tai PC:n päällä.

Yhteenvetona, Ethereum on hyvä älysopimuksien käyttölle, mutta Elastos uskoo ettei Ethereumin virtual machine (EVM) ole sopiva pyörittämään Dappejä seuraavista syistä:

- Lohkoketjut ovat tehty konsensuspohjaiseen tietojen säilyttämiseen, mutta laskentanopeus ja joustavuus ovat puutteellisia.

- Nykyiset lohkoketjut on suunniteltu tallentamaan siirtoja, muttei säilömään dataa. Tällä hetkellä lohkoketjuissa ei ole tarpeeksi tilaa säilömään suuria määriä digitaalista sisältöä kuten elokuvia tai kirjoja.

Ensimmäisen ongelman ratkaisemiseksi Elastos ehdottaa joustavaa lohkoketjujärjestelmää, jossa on pääketju sekä sivuketjuja. Päälohkoketju vastaa vain perustoiminnoista ja maksujen siirroista, kun taas sivuketju suorittaa älysopimuksia erilaisten sovellusten ja palveluiden tukemiseksi.

Toisen ongelman ratkaisemiseksi Elastos ajaa sovelluksia Elastosin runtimessa, täten itse lohkoketju ei ruuhkaudu. Tämä on myös turvallisempi ratkaisu. Elastosissa kaikki verkon data siirtyy luotettavan ja identifikoidun kanavan kautta. Identifikaatio ja todentaminen tulee lohkoketjun ID:stä. Tällä tavalla lohkoketjun luotettavuus voidaan siirtää Elastosin runtimeen. Elastosin runtimella voi olla erilaisia muotoja: itsejäinen käyttöjärjestelmä, virtuaalikone (Virtual machine), tai ohjelmistonkehityspakkaus (SDK), joka integroituu yleisimpien käyttöjärjestelmien ohjelmiin.

Elastos-mallin filosofia on yhdistää matkapuhelinten helppokäyttöisyys lohkoketjuteknologian luotettavuuden kanssa. Tämä mahdollistaa käyttäjille pääsyn sovelluksiin ilman kolmansia osapuolia. Elastos luo ympäristön, jossa digitaalisia hyödykkeitä voidaan kaupata ja vaihtaa käyttäjien kesken.

3. Elastos: lohkoketjuvarmenteinen internet

Elastos-mallin filosofia on peräisin entiseltä Microsoftin ohjelmistosuunnittelijalta, Rong Cheniltä. Microsoftilla saadun kokemuksen pohjalta Chen halusi luoda alustan, jossa sovelluksilla ja palveluilla ei ole suoraa pääsyä internettiin. Ilman pääsyä verkkoon haittaohjelmat eivät pystyisi varastamaan käyttäjätietoja tai hyökkäämään muihin palveluihin internetissä. Chenin visio kehittyi sittemmin avoimen lähdekoodin kevyeksi käyttöjärjestelmäksi virtuaalikoneille (github.com/Elastos). Vuonna 2017 lohkoketjuteknologia yhdistettiin Chenin visioon, mikä mahdollisti Elastosin älyverkon kehittämisen.

Elastosin älyverkko koostuu neljästä pilarista:

- Elastos lohkoketju. Elastos haluaa rakentaa hajautetun älyverkon, jossa jokaisella laitteella, yksilöllä, verkkosivustolla ja digitaalisella hyödykkeellä on luotettava tunnus. Lohkoketjuteknologia mahdollistaa luottamuksen luomisen internettiin.

- Elastos Runtime. Elastos Runtime on kevyt käyttöjärjestelmä, joka estää sovellusten ja palveluiden pääsyn suoraan internettiin. Elastos Runtime toimii asiakkaan mobiililaitteella tai tietokoneella.

- Elastos Carrier. Elastos Carrier on täysin hajautettu vertaisverkko-alusta. Carrier vastaa verkkoliikenteestä virtuaalikoneiden välillä ja välittää tietoa sovellusten puolesta.

- Elastos ohjelmistokehityspakkaus (SDK). Sovellukset tarvitsevat Elastos SDK:ta päästäkseen käsiksi älyverkon tunnisteisiin (ID) sekä Carrier palveluihin.

Elastosilla on seuraavat ominaisuudet:

- Elastosin julkinen ketju on puhdas ja yksinkertainen, sekä piilossa kolmannen osapuolen sovelluksista ja palveluista.
- Elastos estää pääketjun ylikuormitusta asettamalla Elastos Carrier -alustalle muutaman ennalta määritetyn sivuketjun.
- Elastos edistää digitaalisten hyödykkeiden omistusoikeuksia. Elastos pystyy myöntämään tokeneita digitaalisille hyödykkeille ja sovelluksille, sekä antamaan tunnisteen digitaaliselle sisällölle. Nämä onnistuvat älysopimusten kautta.
- Elastos Runtime toimii asiakkaan mobiililaitteen käyttöjärjestelmässä. Sovellusten käyttö on ilmaista ja niiden toimivuus on verrattavissa olemassa oleviin mobiilisovelluksiin. Elastos tukee perinteisiä ohjelmointikieliä, joten koodin kirjoittaminen on suhteellisen helppoa. Elastos tukee myös suosittuja ohjelmointikehyksiä (programming framworks).
- Sovellusten erottaminen verkosta varmistaa, ettei digitaalinen sisältö vuoda ulkopuolelle.
- Vaikka Elastos sovellukset toimivatkin käyttöjärjestelmissä, kuten iOS:sä, Androidissa ja Windowsissa, paikallinen käyttöjärjestelmä ei pysty sabotoimaan digitaalisten hyödykkeiden omistusoikeuksia. Täten digitaaliset hyödykkeet säilyttävät arvonsa.
- Käyttöjärjestelmien (esimerkiksi Anroidin tai iOS:än) omat sovellukset pääsevät Elastosin älyverkkoon SDK:n kautta. Käyttäjä pystyy kirjautumaan näihin sovelluksiin käyttäen Elastosin älyverkko tunnusta. Käyttäjät voivat säilöä näiden sovellusten tiedot Elastosin pilvipalveluun.
- Elastosin älysopimukset, sekä Dapp:it toimivat Elastosin älyverkossa. Tämä muodostaa suljetun alustan ja näin ollen tarve siirtyä pois lohkoketjusta katoaa. Suljettu alusta muodostaa erityisen talousalueen missä käyttäjät voivat vaihtaa digitaalisia hyödykkeitä turvallisesti. Tässä suljetussa piirissä, tuottaminen, vaihtaminen ja kuluttaminen mahdollistaa vaurauden luomisen.

Tässä lyhyt yhteenveto Bitcoinin, Ethereumin ja Elastosin ainutlaatuisista eduista:

- Bitcoin = luotettava kirjanpito
- Ethereum = luotettava kirjanpito + älysopimukset
- Elastos = luotettava kirjanpito + älysopimukset + vaihdettavat ja myytävät Dapp:it, sekä digitaaliset hyödykkeet

Nykyinen lohkoketjutekniikka mahdollistaa omistusoikeuksien tallentamisen, mutta vaikka käyttäjät voivat todistaa että digitaalinen kirja kuuluu heille, he eivät välttämättä voi estää muita varastamasta tai lukemasta sitä ilman lupaa. Tällaisessa ympäristössä digitaalisen omaisuuden kaupallistaminen on hyvin vaikeaa. Elastos pyrkii ratkaisemaan tämän ongelman luomalla ympäristön, jossa digitaalisen sisällön (esim. elokuvan katselu, ostaminen tai myyminen) käyttö tapahtuu älyverkossa ja täten on suojattua älysopimuksilla. Digitaalisen sisällön tekijä voi käyttää Elastosin tarjoamaa työkalua ja määrittää kuinka monta kappaletta tuotetta halutaan valmistettavan. Esimerkiksi tekijät voivat päättää että he haluavat julkaista vain 5000 kopiota kirjoistaan Elastosin älyverkkoon. Rajallinen määrä tuotetta mahdollistaa sille arvon.

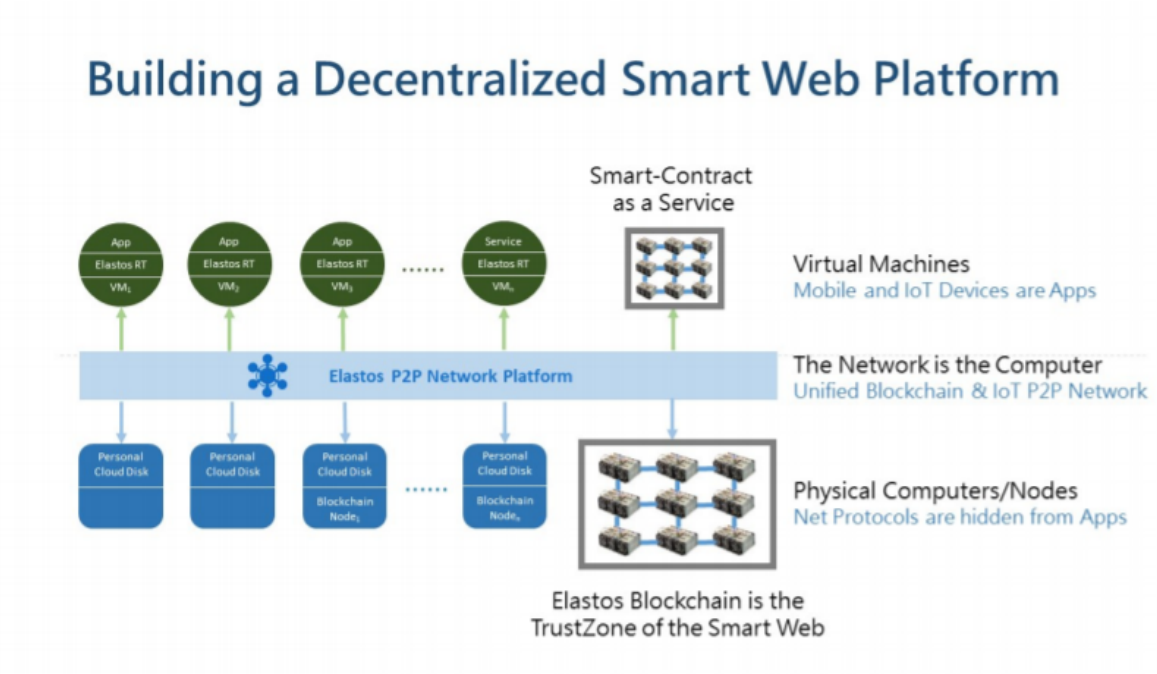
Elastosin avulla kuluttajasta voi tulla sijoittaja. Oletetaan, että liikkeellä olisi vain 5000 kopiota digitaalisesta kirjasta ja kyseinen kirja saavuttaa suuren suosion. Tämä merkitsee että kirjan arvo nousee ja kirjan omistajan varallisuus kasvaa. Luettuaan kirjan, kuluttaja voisi myydä sen eteenpäin korkeammalla hinnalla. Käyttäjä voi myös ostaa rajoitetun version (limited edition) pelisovelluksesta. Pelattuaan peliä Elastosin runtimessä esimerkiksi mobiililaitteellaan, pelin voi myydä eteenpäin toiselle käyttäjälle. Koska kyseessä on rajoitettu versio, pelin arvo voi nousta ajan saatossa.

Toinen esimerkki, elokuvantekijät voisivat kerätä rahaa elokuvalleen järjestämällä joukkorahoituksen laskien liikkeelle tokeneita. He voisivat määrittää älysopimukseen ehdon, joka kerta kun elokuvaa katsotaan, tokeneiden omistajat saisivat osuuden tuotosta. Toinen ehto älysopimukseen voisi olla, että käyttäjät voivat myydä elokuvan eteenpäin sosiaalisessa mediassa tai vertaisverkossa ja saisivat myynnistä komission.

Tämä järjestelmä luo taloudellisia mahdollisuuksia tuottajille sekä kuluttajille ja se kannustaa uusia ihmisiä käyttämään Elastosia. Käyttäjien lisääntyminen taasen kannustaa digitaalisen sisällön tuottajia luomaan ja julkaisemaan lisää sisältöä Elastosin alustalla. Sisällön määrän kasvaminen taasen houkuttelee uusia käyttäjiä joista osa taas luo lisää sisältöä. Tämä kierre tuo suuren määrän arvokasta digitaalista sisältöä, jota voidaan käyttää varallisuuden luomiseen.

4. Hajautettu älyverkko alusta

Alla oleva kaavio kuvaa Elastos alustan keskeisten osien välisiä suhteita:



4.1 Digitaalisten hyödykkeiden oikeanlainen todennus, kaupankäynti ja kierrätys.

Pula-ajan niukkuus on korvautunut informaatioaikakauden suurilla tietomäärillä. Nykyään digitaalisia resursseja voidaan kopioida rajattomasti ilman kustannuksia. Vaikka digitaalisia hyödykkeitä tuotetaan laajalti, kierrätetään ja kulutetaan, ne eivät välttämättä synnytä vaurautta. Digitaalisia resursseja ei ole todennettu ja se johtaa piratismiin sekä uusien innovaatioiden puuttumiseen.

Lohkoketjuteknologia ratkaisee tämän ongelman tehden digitaaliset hyödykkeet todennetuiksi ja niukiksi. Elastos toteuttaa infrastruktuurin digitaalisen omaisuuden todentamiseen, kaupankäyntiin ja levitykseen. Kun digitaalinen hyödyke julkaistaan lohkoketjuteknologiaa käyttäen, se saa todennuksen. Tämän jälkeen hyödykettä voidaan kaupata ja levittää.

Julkaistaessa digitaalisia hyödykkeitä, Elastosin lompakko on välttämätön. Sieltä suoritetaan louhintamaksu. Maksun jälkeen tuottaja voi pyytää tuotteelleen todennuksen, joka sisältää tiedon esimerkiksi käyttäjän lompakon osoitteesta, URI:sta (Uniform Resource Identifier),

tuotteen hinnasta ja määrästä. Tämän jälkeen lasketaan tarkiste numero (hash number) ja transaktio kirjataan lohkoketjuun käyttämättömäksi tapahtumaksi (UTXO, unspent transaction output). Kun tieto vahvistuksesta on julkaistu lohkoketjuun, hyödyke on valmis kaupattavaksi. Kun hyödyke ostetaan, se siirtyy maksajan omistukseen ja on myytävissä eteenpäin.

4.2 Hajautetut sovellukset (Dapps)

Perustuen nykyiseen lohkoketjuteknologiaan, ei ole pystytty luomaan Dappia, joka voisi kilpailla valtavirran sovellusten kanssa. Syynä tähän on se, että dappien laskentateho ja nopeus (IOPS, input/output per second) on suhteellisen heikko. Nykyinen lohkoketju infrastruktuuri rasittuu helposti liian paljon. Elastos ottaa käyttöön uuden tietojenkäsittelyn paradigman ja mahdollistaa hajautettujen sovellusten suoriutumisen valtavirta sovellusten tasoisesti.

Elastos lohkoketju on suunniteltu käyttämään pääketjua ja sivuketjuja. Jotta pääketju ei tukkeudu tarpeettomasta tiedosta, kaikki älysopimukset ja sovellukset toimivat sivuketjuissa. Käyttäjät voivat helposti kehittää turvallisia Dappeja laitteille, jotka käyttävät Elastosin käyttöjärjestelmää. He voivat myös käyttää Elastos Runtime -ympäristöä perinteisten käyttöjärjestelmien (Anroid, iOS, Windows jne.) päällä. Elastos runtimeen pääsee sekä VM:n (virtual machine), että SDK:n (Software Development Kit) kautta.

5. Elastos lohkoketju

Kuten puhelimen käyttöjärjestelmä, myös käyttäjät tarvitsevat luotettavan paikan tärkeiden tietojen tallentamiselle. Elastosin lohkoketju toimii luotettavana paikkana koko Elastosin verkko-käyttöjärjestelmälle.

Elastos lohkoketju käyttää pää- ja sivuketjuratkaisuja älytalouden luomiseen (smart economy) ja tarjoaa terveen ympäristön hajautetuille sovelluksille. Tämä tarkoittaa, että jokainen sovellus voi luoda yksittäisiä sivuketjuja. Elastos lohkoketjuun on sisäänrakennettu helppokäyttöinen tuki sivuketjuille. Sivuketjut ovat myös muokattavissa, jolloin asiakkaat voivat valita erilaisia konsensusmenetelmiä riippuen käyttötapauksesta.

Tokeneita voidaan julkaista sivuketjuissa ja niiden avulla siirtää varoja pää – ja sivuketjujen välillä. Sivuketjuja voidaan louhia yhdessä pääketjun kanssa, jolloin vältytään ylimääräiseltä energian kulutukselta.

5.1 Vaihdon ja lohkon malli

Elastosin lohkoketjurakenne perustuu olemassa olevaan malliin, joka on tuttu bitcoinista. Lohkon varmennukseksi tarvitaan edellisen lohkon otsikoiden tiiviste (hash), Merkle-puun juuren tiiviste, nonssi (nonce) konsensusalgoritmille, aikaleimat, vaikeusaste jne.

Elastos parantaa nykyistä digitaalisen valuutan käyttökokemusta sivuketjumallillaan. Elastos voi muokata sivuketjujen ominaisuuksia parantaen niiden toimivuutta, esimerkiksi poistamalla validointikomentosarjan transaktiorakenteesta. Elastosin sivuketju on perusta Dappeille ja pääketjun rakenne tarjoaa infrastruktuurin ja tuen sivuketjuille, sekä mahdollistaa omaisuuden siirron kätevästi.

5.2 Yhdistetty louhinta

Elastosin lohkoketju käyttää hyväksi yhdistettyä louhintaa Bitcoinin kanssa, täten saavutetaan molempien ketjujen konsensus samanaikaisesti. Bitcoinin lohkoketju toimii emoketjuna ja Elastosin ketju apuketjuna. Louhintapoolit ottavat käyttöön yhdistetyn louhinnan koodin ja louhijat toteuttavat POW:n molemmille ketjuille samanaikaisesti. Yhdistetyssä louhinnassa kokonaisenergiankulutus ei kasva verrattuna siihen, jos louhittaisiin vain toista ketjua erikseen. Tämän mekanismin avulla Elastosin lohkoketjulla on erittäin vahva laskentateho ja se pystyy tarjoamaan lohkoketju innovaatioita maailmanlaajuisesti. Elastos käyttää bitcoinin olemassaolevaa laskentatehoa ja on samaan aikaan ympäristöystävällinen. Yhdistetyn louhinnan lisäetuja ovat:

1. Luottamuksen siirtäminen useille ketjuille. Elastosin pääketjua louhitaan samanaikaisesti Bitcoinin kanssa. Yhdistetty louhinta voidaan ulottaa Elastosin sivuketjuihin jos sivuketju käyttää samaa POW konsensusta. Täten ketjun kerrokset voidaan louhia rekursiivisesti, mikä luo ketjuihin hierarkian.

2. Eristetyt nodet. Yhdistetystä louhinnasta riippuvainen ketju tai sivuketju ei tarvitse konsensusta useista nodeista. Ääriesimerkkinä, yksi ketju tarvitsee vain yhden noden, eikä tämä vähennä pääketjun tai sivuketjujen kirjanpidon luotettavuutta. Minkään muun lohkoketjun konsensusalgoritmilla ei ole tällaista etua.

5.3 Tokeneiden jakauma

ELA on Elastos lohkoketjun olennainen tokeni. Sitä voidaan käyttää kaupankäynnissä, sijoitettaessa digitaalisiin hyödykkeisiin, maksamaan lohkoketjun prosessointipalkkioita ja niin edelleen.ELA on perusyksikkö. Tämän lisäksi, Satoshi Nakamotoa kunnioittaen, Elastos haluaa käyttää Satoshi ELA:a (Sela) pienimpänä yksikkönä. 1 ELA vastaa 10^8 Selaa.

Elastos laskee liikkeelle pienen määrän tokeneitaan. Bitcoinien kokonaismäärä tulee lopulta olemaan 21 miljoonaa ja Elastos haluaisi luoda yhteensä 33 miljoonaa ELA:a. ELA:n jakelusuunnitelma ja käyttötarkoitukset ovat alapuolella:

ELA (units: 10000)	Käyttötarkoitus	Huomautukset
1650 (50%)	Ekosysteemin kehittäminen	Elastosin genesis-lohkon luontiajankohtaan perustuen, Elastos saattaa lähettää ELA:a maksutta Bitcoin haltijoille:

		• Tavoite: Palaute kryptovaluutta yhteisölle ja tehokkaan levikin luominen • Määrä: Bitoinin haltijat voivat saada vastaavan määrän ELA:a. • Jakelu: ELA:t myönnetään vain valtuutettujen kryptopörssien kautta. • Menetelmä: Elastos-säätiö valtuuttaa vaihtopörssit myöntämään tokeneita, kukaan ei saa ELA tokeneita automaattisesti. • Kaikki ELA:t joita ei ole lunastettu, sijoitetaan Elastosiin. Niitä ei käytetä rahoittamaan Elastos-säätiön juoksevia kuluja.
500 (15%)	Enkeli sijoittajat	Elastosin enkeli sijoittajat koostuvat Elastosin perustajista ja avainkumppaneista.
800 (24%)	Yksityinen ja julkinen joukkorahoitus.	Sijoittajayhteisö on Elastosin selkäranka. Se tukee ja vie eteenpäin Elastosin kehitystä. Kaikki kerätty kryptovaluutta kuuluu Elastos-säätiölle ja se tullaan käyttämään Elastosin kehittämiseksi.
350 (11%)	Elastos säätiö	Nämä varat on varattu Elastos säätiön toiminnan tukemiseen sekä Elastosin ekosysteemiin sijoittamiseen.

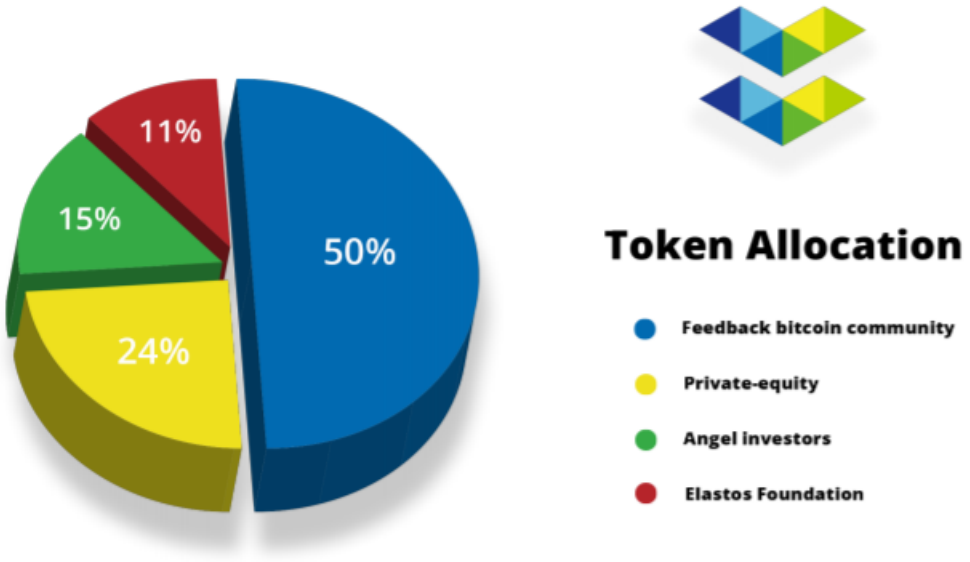


fig2. conversion relationships

Kompensoidakseen tokeneiden luonnollisen katoaminen, kuten käyttäjän kadottaessa lompakon, ja pysyäkseen lievässä inflaatiossa, ELA:n määrä kasvaa vuosittain 4%.

Yksi ELA vapautuu kahden minuutin välein yhdistetyn louhinnan tuloksena. Nämä uudet kolikot jaetaan Elastos säätiölle sekä louhijoille. Elastos säätiö ottaa 30% ja loput 70% kuuluu louhijoille.

5.4 Sivuketjut

Jokainen lohkoketjutekniikalla rakennettu järjestelmä omaa pienemmän laskentatehon kuin perinteinen tietokone, joten ne eivät pysty täyttämään internet-sovellusten (kuten videopelien tai teräväpiirtovideoiden) vaatimuksia. Tämä on perustavanlaatuinen syy sille, miksi lohkoketjuja ei vieläkään voida soveltaa laajasti internetissä. Elastosin tiimi tunnistaa tämän tosiasian ja uskoo ettei lohkoketjun kehittämisen pitäisi pelkästään perustua laskentatehoon. Elastos pyrkii skaalaamaan lohkoketju systeeminsä mahdollistamalla tuen sivuketjuille. Tämä auttaa saavuttamaan vaatimukset, joita korkean IOPS:n sovellukset tarvitsevat.

Elastosin pääketjun rooli on pieni, mutta sitäkin tärkeämpi. Pääketju vastaa ELA:n siirroista ja tarjoaa vakauden lohkoketju systeemiin. Elastos haluaa välttää pääketjun tukkeutumisen tarpeettomilla älysopimuksilla, vain tärkeimmät infrastruktuurin parannukset tapahtuvat pääketjussa. Kaikki muut älysopimukset toteutuvat sivuketjuissa, mikä mahdollistaa skaalautuvuuden.

Tämä hierarkinen ja jäsennelty suunnittelufilosofia avaa tien tulevalle lohkoketjun paradigmalle, kuten edellä mainitulle kehitykselle itsenäisestä laskennasta hajautettuun laskentaan. Tämä on keskeinen innovaatio lohkoketjuteknologiassa ja tärkeämpää kuin yksittäisten konsensusalgoritmien ja ketjujen teknologia.

Elastosin tiimi luo peruspalvelut sivuketjuihin, globaaliin ja julkiseen käyttöön. Näihin palveluihin kuuluvat mm. tunnusten (ID) luominen, tokeneiden jakelu, digitaalisilla hyödykkeillä kaupankäynti ja nopeat maksujärjestelmät. Nämä peruspalvelut ovat tärkeitä komponentteja älyverkon infrasturktuurissa. Lisäksi Elastosin tiimi tarjoaa tuen kolmansien osapuolten sivuketjujen kehittämiseen.

Transaktiot ovat tärkein osa pää- ja sivuketjujen välistä rajapintaa. Transaktion proseduuri lähetettäessä tokeneita pääketjulta sivuketjulle vastaa sitä, että lähetys tapahtuisi käyttäjän pääketjun tililtä sivuketjun vastaavaan monisigneerattuun osoitteeseen. Prosessi tarkistaa automaattisesti, että sivuketju tunnistaa tapahtuman ja tallettaa vastaavan määrän sivuketjun tokeneita käyttäjän sivuketju-tilille.

Pääketjulta sivuketjulle siirron proseduuri:

- Käyttäjä luo satunnaisen salan (the secret), joka vastaa hashia
- Käyttäjä muodostaa monisignatuuri osoitteen pääketjulla. Poistaakseen lukituksen, käyttäjä tarvitsee monisignatuuri osoitteen salan sekä yksityisen avaimen.
- Käyttäjä lähettää transaktion sekä salaa vastaavan hashin sivuketjun siirroista vastaavalle nodelle käsiteltäväksi.

- Sivuketjun tapahtumia käsittelevä node generoi tokenin transaktion sen jälkeen, kun monisignatuurin hash ja yksityinen avain on mahdollistanut tunnistuksen.
- Avatakseen transaktion ja vastaanottaakseen tokenit sivuketjulta, käyttäjä tarvitsee salan.
- Tokenit talletetaan monisignatuuri osoitteeseen.

Sivuketjulta pääketjulle siirron proseduuri on sama, kuin lähetettäisiin ELA:a monisignatuuri osoitteesta pääketjulla käyttäjän tilille, joka on myös pääketjulla.

Sivuketjulta pääketjulle siirron proseduuri

- käyttäjä luo satunnaisen salan, joka vastaa hashia.
- Käyttäjä luo transaktion sivuketjussa. Poistaakseen lukituksen, käyttäjä tarvitsee salan.
- Käyttäjä lähettää transaktion ja salan hashin pääketjun transaktioista vasvaavalle nodelle.
- Pääketjun node luo transaktion sen jälkeen kun se on vahvistettu salan ja yksityisen avaimen avulla.
- Käyttäjä antaa salan avatakseen transaktion ja siten vastaanottaa tokenit pääketjulta.
- Sivuketjua vastaava monisignatuuri osoite avaa noston ja käyttää niitä vastaavat tokenit.

ELA:n turvallisuuden takaamiseksi monisignatuuri osoitteessa, transaktio on mahdollinen ainoastaan yllämainitulla tavalla.

5.5 Älysopimukset

Jos laskennallisesti kuluttavia älysopimuksia käytetään pääketjussa, vaikkei ne olisi aktiivisena, joutuu jokainen verkon nodeista päivittämään jatkuvasti. Tämä on rasite vain vahvistuksia suorittaville nodeille, louhinta nodet saisivat sentään jokaisesta transaktiosta palkkion. Tämän välttääkseen Elastosin pääketju rajoittaa älysopimusten käyttöä ja delegoi

älysopimukset sivuketjuille. Jokainen sivuketju voi suunnitella älysopimusten toiminnan itsenäisesti, samaan tapaan kuin NeoContract tukee NEO:n lohkoketjua.

6. Elastos Carrier: hajautettu P2P verkko.

Elastos Carrier on Elastos-ekosysteemin hajautettu internet-palvelu. Sen nodet voivat suoriutua minkälaisessa ympäristössä tahansa, kunhan internet yhteys on saatavilla. Mukaanlukien kodin tai työpaikan paikallisverkot. Käyttämällä UDP-pohjaista NAT-avoimuustekniikkaa (User Datagram Protocol, Network Address Translator), kaikilla nodepareilla on toimivalta muodostaa yhteyksiä toisiinsa, jopa suoria yhteyksiä. Tämä mahdollistaa jokaisen noden kapasiteetin runsaan hyödyntämisen, mikä parantaa verkon tehoa.

Peruspalveluiden joukkoon kuuluvat hajautetut verkkotunnukset, hajautettu laskenta ja hajautettu tiedontallennus. Dappien kehittämiseen on olemassa perustavaa laatua oleva tuki. Tällaisessa ympäristössä käyttäjä omaa runsaan yksityisyydensuojan datalleen. Samanaikaisesti käyttäjä voi vuokrata oman laitteistonsa haluamallaan tavalla Elastosin lohkoketjun käyttöön ja saada korvauksen riippuen kuinka paljon sitä käytetään.

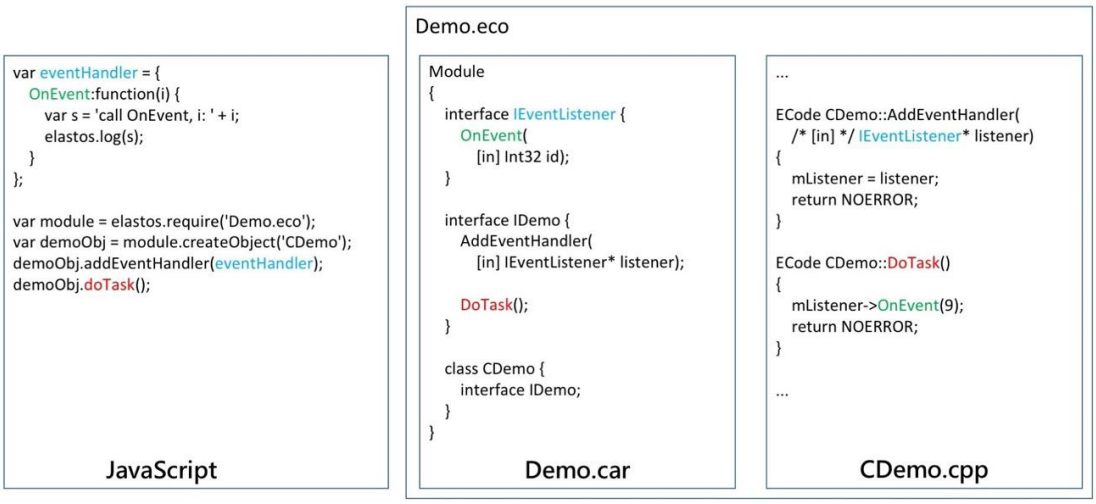
7. Elastos OS: Turvallinen, yleiskäyttöinen käyttöjärjestelmä.

Elastos OS on yleiskäyttöinen käyttöjärjestelmä, jonka aatteena on turvallisuuden vaaliminen. Se on käyttöjärjestelmä, joka on kohdistettu esineiden internetin (IoT) tarpeisiin, sekä esimerkiksi Raspberry Pi:lle ja mobiililaitteille. Viimeisintä, kolmatta versiota, on rakennettu 2013 toukokuusta lähtien. Se on menestyksekkäästi saavuttanut beta-laadun kun sitä on testattu Moto X puhelimessa sekä Lamobo-R1S älyreitittimessä. Käytetyn koodin kokonaismäärä on ylittänyt 10 miljoonaa riviä.

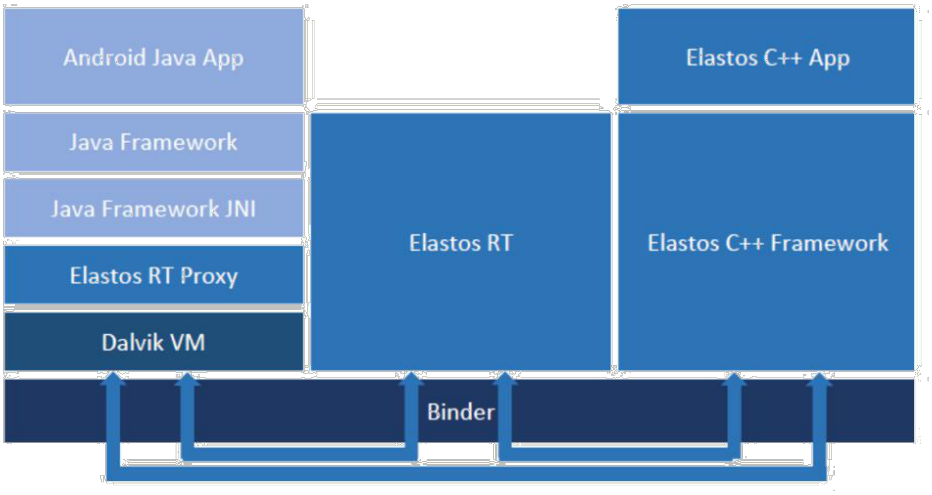
Turvallisuuden suhteen Elastos OS estää suoran prosessin luomisen eikä salli suoraa vuorovaikutusta TCP / IP:n kanssa. Sen sijaan systeemi määrittää paikallisten, viereisten ja kaukaisten (tai pilvipohjaisten) mikropalveluiden sijainnit. Systeemi luo automaattisesti etätoimintopuheluita (RPC) ja tapahtumapohjaisia vasteita, mikä estää mahdolliset haittaohjelmat joko sovellusten tai etäpalvelun kautta ja täten evää mahdollisuuden itseltään lähettää viruksia eteenpäin.

Elastos OS: llä on sisäinen ja paranneltu hajautettu tukijärjestelmä sovellusten kehittämiseksi, mikä helpottaa liittymistä Elastosin peruspalveluihin Elastos Carrierin kautta. Täten Dappit voivat turvallisesti käsitellä samaan aikaan Elastosin transaktioita sekä muita digitaalisia hyödykkeitä, kuten lähdekoodia, dataa, e-kirjoja, videoita, pelejä, tekijänoikeuksia ym.

Järjestelmä hyödyntää C / C ++, Javaa sekä HTML5 / JS ensisijaisina kehittämismoodeina. Elastosin C++ API on samankaltainen Java API:n kanssa, mikä mahdollistaa pilvupalvuiden, monitoroinnin ja rajapinnan yhtenäisen hallinnan. Javalla, HTML5/JS ja C/C++ kirjoitetut komponentit voivat soittaa toisilleen modulaarisesti, eikä JNI:tä tarvitse käsitellä manuaalisesti. Täten järjestelmä noudattaa ”kirjoita kerran, käytä missä vain” ajatusta. Järjestelmä tukee Component Assembly Runtime (CAR) arkkitehtuuria, kuten alla olevassa esimerkissä osoitetaan. Esimerkissä CAR komponentti mahdollistaa C/C++ ja HTML5/JS koodattujen ohjelmien välisen kommunikaation.



Elastos OS:n C++ puitteet hyödyntävät Anroidin sovellusrajapintoja, mikä mahdollistaa siirrettävyyden ja takaa käytänöllisyyden ohjelmoijille. Elastos OS voi käyttää Android ohjelmia jopa suoraan, jolloin saavutetaan seuraavassa kuvattu tilanne:



Voidaan ajatella että Elastos Runtime on C++ versio sekä Java:n virtuaali koneesta, että Java frameworkistä. Tätä voidaan kutsua jopa C virtuaali koneeksi (CVM). Elastos OS palvelut ja sovellukset toteutetaan tämän CVM:n sisällä, mikä mahdollistaa samojen palveluiden olemassaolon sopusoinnussa erilaisten node ja laite -ympäristöjen kanssa.

8. Elastos framework ympäristö Dappeille.

Vaikka Elastos OS:n kautta voidaan käyttää Dappeja, on tilanteita missä käyttäjä haluaisi säilyttää nykyisen käyttöjärjestelmänsä. Näissä tilanteissa voidaan hyödyntää Elastos Runtimea joka tarjoaa täyden tuen Dappien käyttämiselle. Ohjelmoijat voivat valita tarpeidensa mukaan jonkin seuraavista: Elastos Runtime Androidille, Elastos Runtime iOS:lle, tai Elastos Runtime Ubuntu Linuxille.

8.1 P2P verkon käyttöliittymä

Dappien on kommunikoitava toistensa kanssa komponenttirajapintojen avulla koska niillä ei ole suoraa yhteyttä internettiin. Tämä lähestymistapa on helpompi, turvallisempi ja luonnollisempi:

```
5
6  TrustID myfriend = "0xE94b04a0FeD112f3664e45adb2B8915693dD5FF3";
7  IChat * pChat = CChat::New(myfriend);
8  pChat->Chat("hello");
9
```

Yllä olevan koodin ei tarvitse huolehtia sarjoituksesta / sarjoituksen purkamisesta, tai salauksesta / salauksen purkamisesta, eikä ohjelmoijan tarvitse osallistua uusien protokollien kirjoittamiseen. Kaiken tämän hoitaa Elastos Runtimen CAR-rajapinta. Riittää, kun alla olevaa CAR asiakirjaa muokataan ja hahmotellaan vastaavat toiminnot. Verrattuna tavanomaiseen socket pohjaiseen API:n, Elastos Runtime on paljon helpompi käyttää. Digitaalisen hyödykkeen transaktio voidaan toteuttaa seuraavasti:

```
13
14 interface IChat {
15     Chat(String message);
16 }
17
18 class CChat {
19     interface IChat;
20 }
21
```

Alla oleva koodi kuvaa kuinka voidaan toimia:

```
24
25 ECode CChat::Chat(String message) {
26
27     // your code ....
28
29     return NOERROR;
30 }
31
```

Sovellukset jotka on kirjoitettu käyttäen Elastos Runtime:a, ovat yksinkertaisempia kuin P2P sovellukset, jotka on kirjoitettu tavanomaisen socket API:n avulla.

8.2 Digitaalisten hyödykkeiden toiminta

Kuten edellä olevissa esimerkeissä on osoitettu, emme käytä enää IP-osoitteita tai verkkotunnuksia verkkoviestintään, koska nykyinen internet ei ole luotettava. Elastos Runtime kuitenkin suorittaa vahvistuksen toimintansa aikana luottamusalueella (trust zone), Elastosin lohkoketjussa.

```
33
34  ECode _CChat::Chat(String message) {
35
36      ... ...
37
38      //  Check whether ID is exist
39      if (Exist(trustID) == FALSE) {
40          return ERROR;
41      }
42      //  Check whether the current APP ID is on the blacklist
43      if (InBlackList(_Current_App_TrustID) == TRUE) {
44          return ERROR;
45      }
46      //  Check whether the current user ID is on the blacklist
47      if (InBlackList(_Current_User_TrustID) == TRUE) {
48          return ERROR;
49      }
50      //  Check whether the called count has exceeded the upper limit
51      if (Called_Count > MAX_CALL_COUNT) {
52          return ERROR;
53      }
54
55      //  More checks
56      ... ...
57
58      ec = CChat::Chat(message);
59
60      ... ...
61
62      return ec;
63  }
64
```

ässä vaiheessa voidaan suorittaa digitaalisen hyödykkeen transaktio. Seuraava esimerkki vahvistaa digitaalisen hyödykkeen omistajuuden:

```
66
67  TrustID aMovie = "0x32B77CBB265175D1A927c9A3F816de577BDDdE05";
68  TrustID owner = "0xd4fa1460F537bb9085d22C7bcCB5DD450Ef28e3a";
69
70
71  if (Elastos.RT.Trust.CheckOwner(owner, aMovie) == TRUE) {
72      // yes, He is its owner.
73  }
74  else {
75      // error
76  }
77
```

Lopuksi luodaan transaktio:

```
82
83  Elastos.RT.Trust.SendTransaction(buyerID, sellerID, 1000, aMovieID);
84
```

9. Elastos säätiö

Elastos projektilla on pitkä historia. Sen alkuaika sijoittuu vuoteen 2000, jolloin Elastosin perustaja Rong Chen palasi Kiinaan aloittamaan liiketoimensa. Siitä lähtien Rong Chen on kehittänyt turvallista yleiskäyttöjärjestelmää internet-ajalle. Vuonna 2017 Elastos projekti tuli maailmanlaajuiseksi, avoimen lähdekoodin ohjelmistoprojektiksi, jota Elastos yhteisö ohjaa. Ohjelmiston lähdekoodi ja dokumentit ovat julkaistu ”free open-source software” -lisenssillä. Elastos projekti toimii Elastos säätiön kautta. Elastos käsittää avoimen lähdekoodin ja digitaalisen valuutan yhteisön, tukee vastavuoroista oppimista ja ajaa kehittyneen sivilisaation edistymistä.

9.1 Elastosin yhteistö

Elastosin kansainvälisessä yhteisössä on faneja, kehittäjiä, yhteisön puuhamiehiä ja ELA sijoittajia eri puolilta maailmaa. Elastos on sitoutunut rakentamaan tätä kansainvälistä yhteisöä. Elastosilla on myös paikallisia käyttäjäryhmiä, jotka työskentelevät yhteisöllisesti vapaaehtoisina. Nämä ryhmät organisoivat, ylläpitävät ja kehittävät paikallisia yhteisöjä. Niiden tehtävänä on edistää digitaalisten valuuttojen ja lohkoketjun filosofiaa, opiskella Elastos teknologiaa, osallistua Elastos-projektin kehittämiseen, kirjoittaa ja kääntää asiakirjoja, järjestää kuukausittaisia paikallisen yhteisön kokoontumisia ja auttaa virallisten kansainvälisten aktiviteettien organisoinnissa.

9.2 Elastos talentit

Olemme edelleen digitaalisen valuutan ja lohkoketjuteknologian alkuvaiheessa. Ala kehittyy vauhdilla ja lahjakkaista yksilöistä on pula. Elastosin perustajat käynnistivät Tsinghuan iCenterissä ohjelman ”We are All Satoshi Nakamoto” Distributed Autonomous Coalition Asia (DACA):n kautta. Sen tavoitteena on kasvattaa korkean tason lohkoketjuteknologia asiantuntijoita. Ohjelman perustamisen jälkeen se on kasvattanut suuren määrän alan taitajia, joista osa on siirtynyt työskentelemään Elastosille. Elastos säätiö tukee jatkuvasti DACA koulutushankkeita ja tekee yhteistyötä Tsinghuan iCenterin kanssa vauhdittaakseen teknologista kehitystä Kiinan lohkoketjuteknologian hyväksi.

9.3 Elastosin visio

Elastos pyrkii olemaan teknologia, joka tukee älytaloutta (smart economy). Elastos rahasto panostaa hajautettujen sovellusten jatkuvaan kehittämiseen. Elastos haluaa luoda uuden maailmanlaajuisen webin, joka on turvallisempi ja älykkäämpi, ja joka voidaan jonain päivänä tuntea vaurauden internettinä (Internet of Wealth).