Älysopimusten kehittäminen

Sopimus suuntautunut ohjelmointi

"There are currently 5,000 blockchain developers. By 2020, we project a global need for over 500,000" **- ConsenSys**

Älysopimus alustat

- Ethereum
  - Älysopimusalustojen standardi, julkinen lohkoketju
  - Ohjelmointikielet: Solidity, Vyper, LLL, Bamboo
- Hyperledger Fabric
  - Älysopimusmoottori, luvanvarainen lohkoketju
  - Ohjelmointikielet: GO (Golang), Java*
- Lisk
  - Keskittyy sivuketjujen rakentamiseen
  - Ohjelmointikielet: Javascript

Sopivan kehitysalustan valitseminen

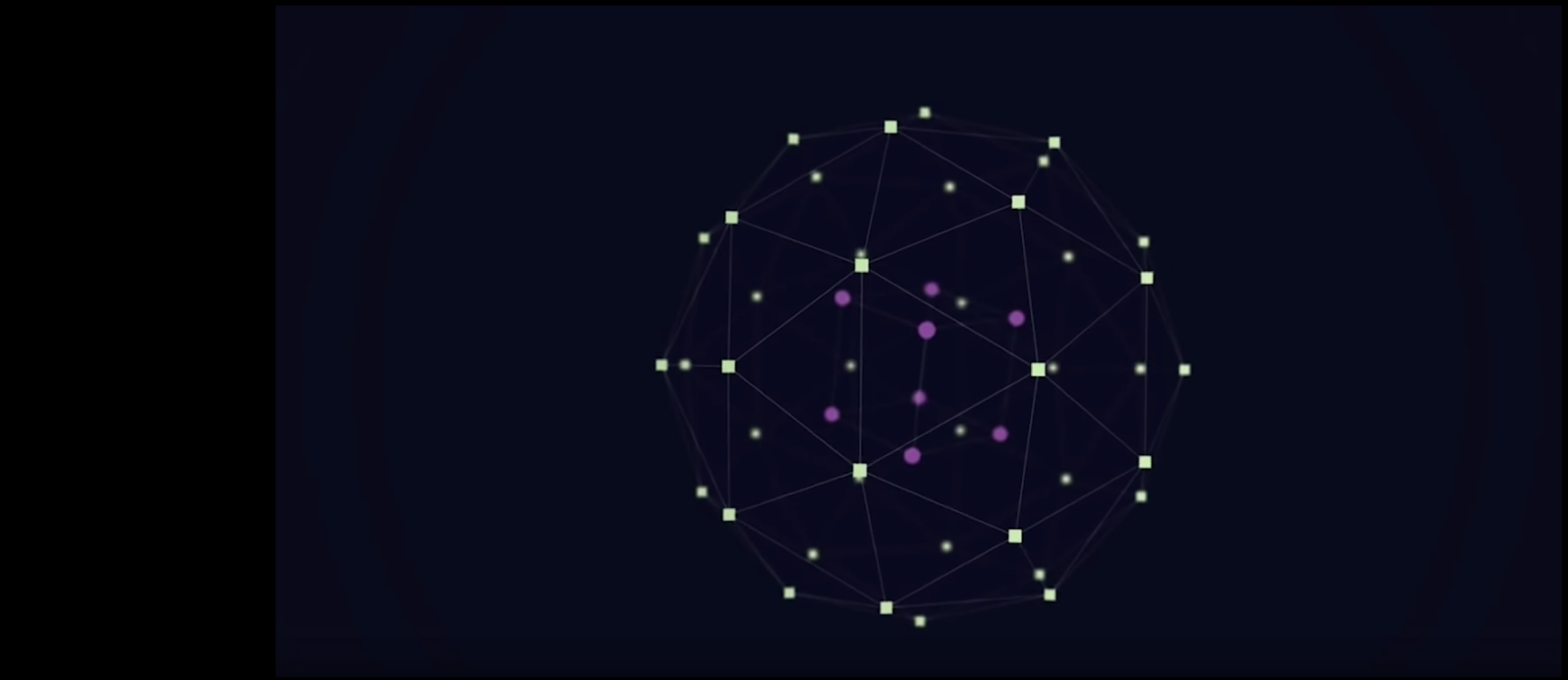
Projektin tarve

Tekninen toteutus

Alustan kypsyys

Kehitysyhteisö

Hyperledger Fabric



Ethereum

Ethereum Virtual Machine (EVM) on suuri hajautettu virtuaalikone, joka sisältää miljoonia tilejä, jotka pystyvät suorittamaan koodia, keskustelemaan keskenään ja ylläpitämään omaa sisäistä tietokantaa

Ulkoinen tili

Tiliä hallinnoidaan yksityisellä avaimella

Sopimustili

Tilillä oleva koodi hallinnoi tiliä

Toimintaympäristössä ei tapahdu mitään ennen kun ulkoinen tili tekee jonkinlaisen herätteen lohkoketjuun.

Sopimukset

- Sopimuskoodi pystyy:
  - Lähettämään Etheriä
  - Lukemaan ja kirjoittamaan muistiin
  - Vastaanottamaan ja lukemaan kutsuja
  - Lähettämään kutsuja toiselle sopimukselle

- Sopimuksia käytetään pääosin neljään eri tarkoitukseen
  - Ylläpitämään dataa
  - Tarjoamaan hyödyllisiä funktioita
  - Toimimaan enemmän säännösteltynä ulkoisena tilinä
  - Ylläpidetyn sopimuksen/suhteen hallitsemiseen

Jokainen verkon täysi solmu suorittaa jokaisen transaktion ja varastoi sen tilan lohkoketjuun

Kaasumaksut

Tahallisten hyökkäysten ja väärinkäytön estämiseksi Ethereum protokolla perii maksun jokaisesta laskentaa suorittavasta vaiheesta ja tilaa vievästä operaatioista

Transaktio

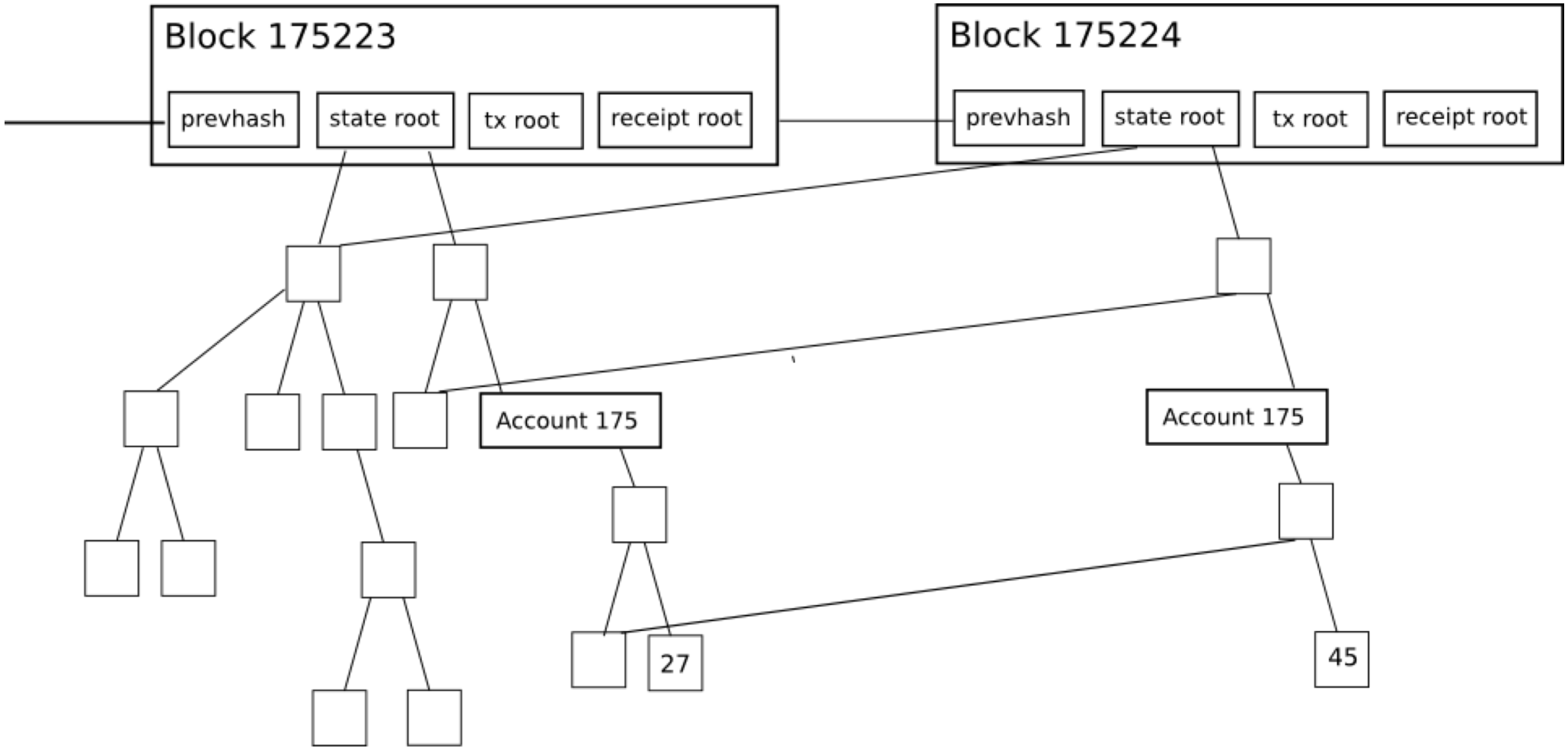
- **nonce:** Pitää yllä transaktioiden määrää ja suojaa toisto-hyökkäyksiltä
- **gasLimit:** Käytettävän kaasun maksimimäärä
- **gasPrice:** Yhden kaasu-yksikön hinta (ether)
- **to:** Transaktion määränpään osoite
- **value:** Lähetettyjen Ethereiden määrä
- **data:** Sopimukselle luettava tieto

Lokit & tapahtumat

- Tapa tallettaa tietoa lohkoketjun tapahtumista halvemmalla
- Append only
  - Sopimukset eivät pysty lukemaan
- Tapa etsiä ja esittää lohkoketjun eri tapahtumien tietoja tehokkaasti
- Bloom suodatus protokolla helpottaa lokien etsimistä tiettyyn aiheeseen liittyen

Merkle-puu

Mahdollistaa tehokkaan tavan varmistaa
lohkon transaktioita


Block 175223
prevhash
state root
tx root
receipt root
Block 175224
prevhash
state root
tx root
receipt root
Account 175
Account 175
27
45

Älysopimusten ohjelmointi

- Sopimus (engl. contract) on uusi abstraktio
- Toimii pohjimmiltaan kuin oliot/objektit muutamalla eroavaisuudella:
  - Pysyvä / Muuttumaton
  - Julkinen (mm. data, funktiot)
- Koodin testaaminen ja auditointi älysopimuksia ohjelmoitaessa on erityisen tärkeää
- Tämän lisäksi on hyvä seurata älysopimusten ohjelmoinnin perusperiaatteita

Uusi abstraktio

Uudet käytänteet

- Peter Borah -

Tuo data näkyväksi

Älä tee erottelua
viestinlähettäjien kesken

Pidä sopimukset lyhyinä

Erottele logiikka ja data

Korkean tason kielet

Solidity, Viper, LLL ja Bamboo kääntyvät EVM koodiksi

Solidity

- Korkean tason älysopimus ohjelmointikieli
  - Muistuttaa olio-ohjelmointia Javalla
- Sopimuskoodi on suunniteltu ajettavaksi Ethereum virtuaalikoneessa (EVM)
- Sopimukset itsessään toimivat yleensä tilakoneina
  - Käyttäytyvät ja toimivat erilailla eri vaiheissa
  - Funktiokutsut yleensä siirtävät sopimuksen eri vaiheeseen
  - Vaiheet voivat myös muuttua automaattisesti ilman herätteitä

Tekninen harjoitustyö

- 1 op suoritus:
  - Luo oma ERC20 rahake käyttäen Solidityä
  - Rakenna hajautettu sovellus, jonka avulla pystyt siirtämään luomaasi rahaketta tililtä toiselle käyttöliittymän kautta
  - Käytä tapahtumalokia hyödyksi rahakkeen siirtotapahtuman kaappaamisessa
- 2 op suoritus:
  - Kaikki tehtävät, jotka vaadittu myös 1 op suorituksessa
  - Luo älysopimus, joka vaatii kahden tai useamman osapuolen hyväksynnän toteutuakseen
  - Suunnittele ja rakenna osapuolten väliseen sopimukseen soveltuva hajautettu sovellus