Integrarea datelor off-chain cu Oraclize

Conf.dr. Cristian KEVORCHIAN

Oracle

- În mediul blockchain, un Oracle este o entitate care furnizează date din cadrul și din afara chain-ului . Necesitatea unei astfel de entități apare din faptul că aplicațiile blockchain, cum ar fi scripturile Bitcoin și contractele inteligente Ethereum, nu pot accesa și prelua direct datele de care au nevoie: fluxuri de prețuri pentru active și aplicații financiare; informații despre vreme pentru asigurarea peer-to-peer; generarea de numere aleatorii pentru jocuri de noroc.

Problema Oracle

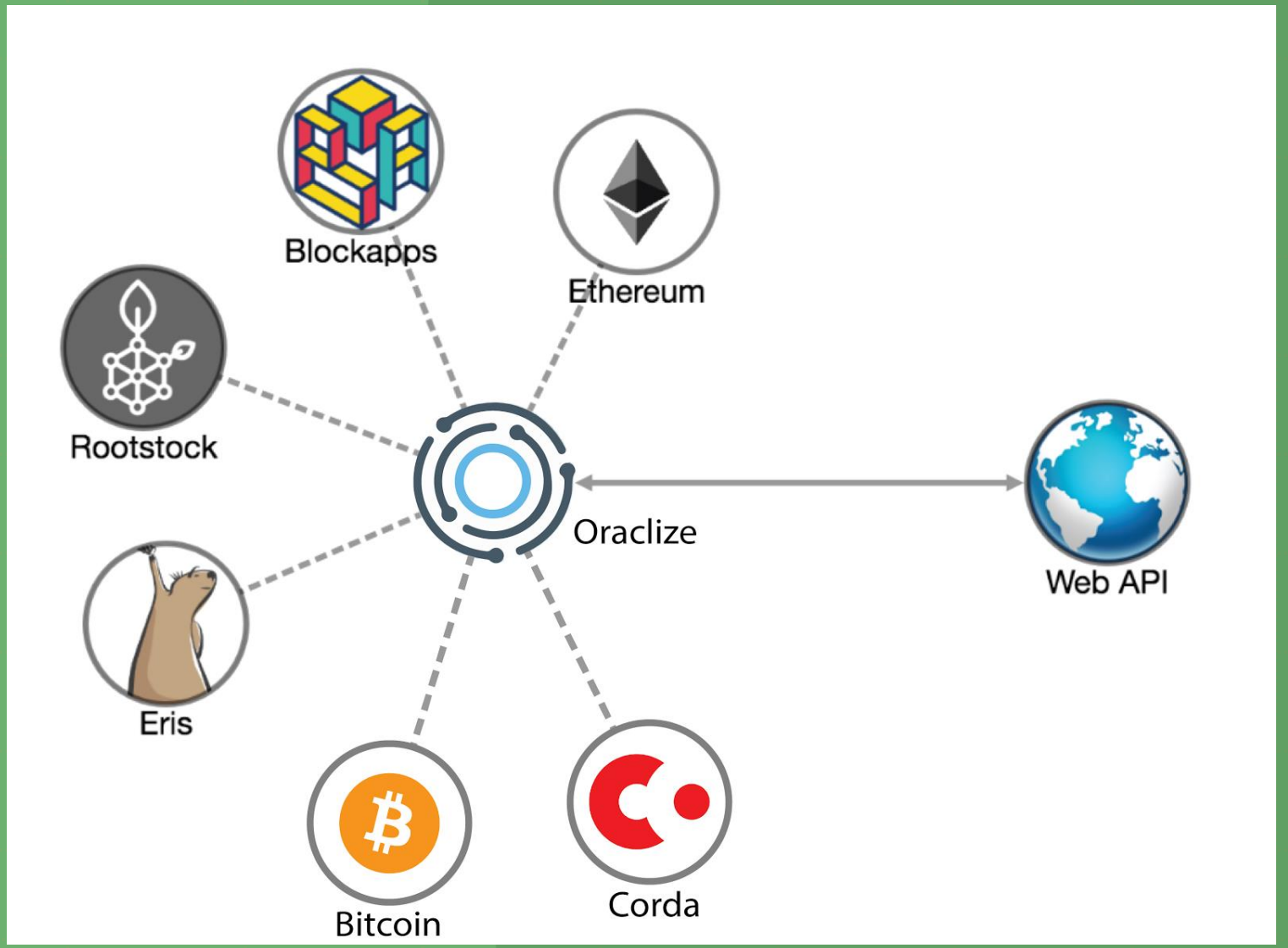
- Furnizorii de date nu trebuie să își modifice serviciile pentru a fi compatibili cu protocoalele blockchain.
- Un Ethereum Smart Contract poate accesa direct date de pe site-uri Web sau API-uri.
- Motorul verificabil poate fi integrat cu ușurință atât cu instanțe private, cât și cu instanțe publice, de diferite protocoale blockchain. În timp ce construia serviciul.
- Echipa de dezvoltare Provable și-a dat seama că conceptul de dovezi de autenticitate are o aplicabilitate mult mai largă decât cea prevăzută inițial. De exemplu, sursa de date aleatorii verificabile poate fi utilizată chiar și de aplicațiile tradiționale de jocuri de noroc pentru a asigura utilizatorilor o echitate continuă a funcționării

Provable

- Provable este serviciul oracle pentru contracte inteligente și aplicații blockchain, care operează mii de cereri în fiecare zi pe platforme precum Ethereum, Rootstock, R3 Corda, Hyperledger Fabric și EOS.

Oraclize

- ERIS- Platforma Ethereum de tranzactionare futures.
- Rootstock-combinatie de minare Bitcoin cu contracte Ethereum
- Blockapps- Blockchain as a Service, impreuna cu Microsoft



Provable Engine

- Alimentează serviciul Provable atât pentru aplicațiile bazate pe blockchain, cât și pentru cele non-blockchain.
- Este implementat un model logic „If This Then That”. Aceasta înseamnă că va executa un set dat de instrucțiuni dacă este îndeplinit un anumit pachet de condiții. De exemplu, poate verifica în mod repetat o condiție și poate returna date sau poate efectua o acțiune numai atunci când condiția a fost îndeplinită.
- Această logică permite utilizarea motorului în multe moduri și contexte diferite, chiar și în afara contextului blockchain.
- O interogare validă asupra unui set de date către Provable, efectuată prin integrarea blockchain-ului nativ sau prin API-ul HTTP, trebui să specifice următoarele argumente:
- Tipul sursei de date,
- Interogarea,
- Opțional, un tip de dovadă de autenticitate

Tipul sursei de date

- O sursă de date este un furnizor(de încredere) de date
- Exemple : un site web sau un web API, cum ar fi Reuters, Weather.com, BBC.com sau o aplicație sigură care rulează
  într-un Trusted Execution Environment (TEE) sau o instanță de mașină virtuală verificabilă, care rulează într-un cloud
- Provable oferă următoarele tipuri de surse de date native:
- **URL**: permite accestul la orice resursă expusă printr-un endpoint HTTP API
- **WolframAlpha**: permite access nativ la computational engine WolframAlpha
- **IPFS** furnizează access la orice content incărcat în fișiere IPFS.
- **Random**: furnizeaza secvente de octeți randomizați proveniți de la aplicații executate pe Ledger Nano S.
- **Computation**: furnizează rezultate derivate dintr-un process de calcul

Tipul sursei de date

- **nested**: permite combinații de ale diferitelor tipuri de surse de date sau cereri multiple solicitate unei singure surse de date întorcând un singur rezultat
- **identity**: intoarce un querry
- **decrypt**: decriptează un șir criptat cu cheia privată Provable

Querry

- O interogare este o serie de parametri care trebuie evaluați pentru a finaliza o cerere specifică de tip sursă de date:
- Querry: [parametru_1, parametri_2, ...];
- Primul parametru este argumentul principal și este de obicei obligatoriu. De exemplu, în cazul tipului de sursă de date URL, primul argument este adresa URL așteptată în care se află resursa.
- Dacă este prezent doar primul argument, atunci sursa de date URL presupune că a fost solicitat un GET HTTP. Al doilea parametru, care este opțional, ar trebui să conțină sarcina utilă de date a cererii HTTP POST. Rezultatul intermediar al unei interogări poate fi necesar să fie analizat: de exemplu, pentru a extrage un câmp precis în răspunsul JSON API.
- Prin urmare, interogarea poate specifica, de asemenea, ajutoare de analiză care trebuie aplicate.

Dezvoltare

- Trecem în revistă câteva instrumente destinate integrării Provable în DApp:
- Test Query (Provable - the provably honest oracle service): poate fi utilizat pentru a testa orice interogare oraclize. Acest lucru nu necesită scrierea vreunui cod și poate fi util pentru a verifica corectitudinea unei interogări date în faza de dezvoltare timpurie.
- Ex:

json(https://minapi.cryptocompare.com/data/price?fsym=ETH&tsyms=USD).USD

Network Monitor

- Network Monitor și Proof Verification Tool pot fi utilizate pentru a verifica integritatea și corectitudinea probelor de autenticitate pe care le-a furnizat Provable. Este foarte important să fie verificate în mod independent validitatea acestor probe, deoarece aceasta este singura procedura prin care se poate verifica dacă Provable a oferit vreodată un răspuns greșit.

Remix IDE - Provable Plugin

- IDE-ul Remix include o varietate de plugin-uri, inclusiv unul pentru utilizarea Provable ca serviciu oracle.
- Plugin-ul este utilizat împreună cu JavaScript VM, care la încărcare implementează toată infrastructura necesară auditării aplicatiei pe tot ciclului de viată al acesteia.
- Pot fi implementate contracte care utilizează Provable prin moștenirea contractului using Oraclize și urmăriți orice solicitare de interogare făcută prin pictograma pluginului de pe panoul lateral al IDE.
- Pentru exemple de contracte, poate fi utilizat github(ethereum-examples).

ETHPM

- Gestionarea pachetelor Ethereum este un proiect care vizează standardizarea, construirea și menținerea unui registru comun de pachete bazate pe contracte inteligente, pentru a ajuta dezvoltatorii de DApp.
- Provable a publicat și menține Ethereum oraclizeAPI sub pachetul „oraclize-api”, Care poate fi instalat cu „truffle install oraclize-api”.

Oraclize-Lib

- Oraclize-lib este o bibliotecă experimentală node.js care poate fi utilizată pentru a construi aplicații non-blockchain folosind Provable.
- Poate fi considerat un simplu nivel de abstractizare pentru API-ul HTTP verificabil.

DEMO
http://faucet.ropsten.be