Departamentul Automatică și Informatică Industrială
Facultatea Automatică și Calculatoare
Universitatea POLITEHNICA din București

RAPORT STIINTIFIC NR. 2

Ethereum Blockchain

George-Aurel Ristoiu

Conducător științific de doctorat: Prof.dr.ing. Alin Iftemi
Tema: Managementul documentelor cu blockchain
Program de masterat: Managementul si Protecția Informației

Cuprins

1 Introducere

Protocolul Ethereum a fost conceput de fundația Ethereum și este o cripto monedă compusă din contracte financiare și a blockchain-ului escrow. Escrow este o entitate separată, imparțială, care se asigură ca toate condițiile tranzacției sunt îndeplinite înainte de a trimite token-urile [2].

Etherium este un mediu public bazat pe o rețea peer-to-peer care acceptă înregistrari imutabile sub forma unor tranzacții pe blockchain. Etherium a fost prima data introdus in 2013 intr-o lucrare scrisă de Vitalik Buterin [1], urmând ca procesul de dezvoltare să ia amploare în 2015, când monedele virtuale au devenit accesibile publicului larg și puteau fi folosite. Etheriem a devenit popular in rândul instituțiilor guvernamentale si a companiilor din domeniul IT sau financiar în 2019 prin apariția contractelor smart. Ethereum este folosit pentru păstrarea și tranzacționarea bunurilor electronice, cele mai populare fiind monedele virtuale si NFT-urile, sau arta digitală, cu ajutorul portofelelor electronice. Portofelele electronice sunt niște interfețe digitale, care îți dau posibilitatea să accesezi ether-ul asociat contului tău, dar nu care nu e stocat în acesta. Portofelul stochează keyle private ce vor fi folosite ca parolă in timpul tranzacțiilor, iar fiecare are a adresă unică pentru a avea un destinatar clar.

2 De ce nu Bitcoin

Bitcoin este cea mai populara moneda virtuala la momentul actual, prin care utilizatorii pot să facă tranzacții fără o parte terță care de validitatea lor. Nodurile de tip miner se ocupă de acest proces prin rezolvarea unor probleme matematice pentru a adăuga blocuri pe Blockchain sau Proof of Work. Costurile de traczacție nu sunt enorme, iar inflația este controlata prin faptul că exista un numar limitat de Bitcoin care poate fi minat [4]. Ethereum în schimb vine cu posibilitatea de a creea seturi de reguli criptografice care se execută atunci când toate condițiile sunt îndeplinite sub forma unor contracte inteligente. Astfel, utilizatorii pot cumpăra atat monede virtuale si NFT-uri, cât și acțiuni și proprietăți imobiliare. În ceea ce privște arloritmul de validare, Etherium folosește Proof of Stake, care presupune utilizarea token-urilor deținute de un cont pentru a valida tranzacții, în urma carora se percep taxe. Astfel, bitcoin este preferat dacă vrem să ne limităm la tranzacții, pe când etheriem este necesar pentru dezvoltarea aplicațiilor distribuite.

In cazul ethereum, partea de compromis a nodurilor se bazează pe protocolul GHOST (Greedy Heaviest Observed Subtree), care abordeaza problema blocurilor neactualizate in rețea. Dacă un grup de noduri intr-o rețea are o putere de procesare mult mai mare ca celelalte, deci contribuie mai mult la retea și devine un sistem centralizat. Această problemă este soluționată prin introducerea blocurilor “unchi”, în urma cărora minerii sunt recompensați chiar dacă blocul lor nu face parte din rețeaua principală. Protocolul susține blocuri de tip unchi pană la 7 generații, iar rația de impărțire este de 87.5%-12.5%.

3 Tehnologii

3.1 Geth

To be done

3.2 Solidity

To be done

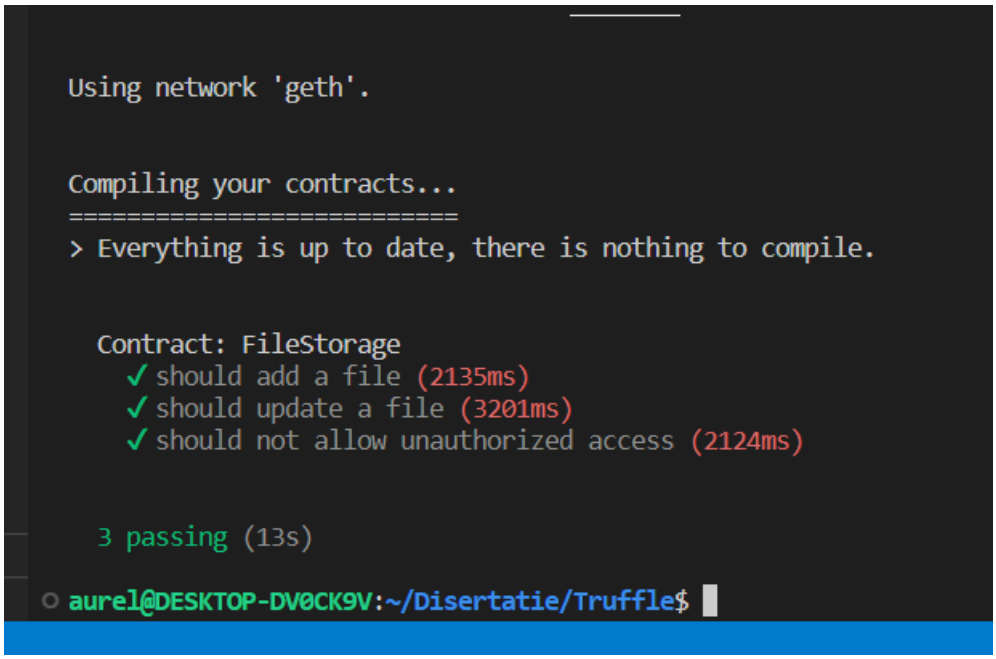
3.3 Truffle

To be done

4 Testare

Din moment de Blockchain este imutabil, este foarte greu sa faci modificări la nivelul contractelor inteligente după ce aceasta se afla pe rețeaua principală. Existe alternative de a le modifica prin efectuarea unei îmbunătățiri la nivelul contractului prin intermediul unei versiuni noi, dar acest proces este greu de implementat și nu este eficient. Crearea unei noi versiuni poate rezolva o problemă după ce aceasta este descoperită, dar exista posibilitatea ca acea breșă de securitate să fie descoperită de către cineva cu intenții malițioase între timp.

Testarea se poate face prin intermediul testelor unitare care presupun verificarea comportamentului contractului inteligent în anumite cazuri de utilizare.



Contractul nostru in cazul de față are 4 funcționalități: crearea unui fișier, modificarea unui fișier prin suprascriere, citirea unui fișier atribuit propriului cont si citirea tuturor fișierelor stocate. În cazul de față, testele se asigură că sunt create și modificate fișiere cu succes, iar acestea nu sunt accesibile decât conturilor cu care au fost create.

5 Concluzie

To be done

6 Bibliografie

[1] Tehnologia Blockchain si Ethereum

https://www.researchgate.net/publication/324791073_Blockchain_technology_bitcoin_and_Ethereum_A_brief_overview

[2] Blockchain in economie

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9273067&utm_source=pocket_saves

[3] Ce este ethereum si cum funcționează

https://www.investopedia.com/terms/e/ethereum.asp

[4] Bitcoin vs Ethereum

https://www.simplilearn.com/tutorials/blockchain-tutorial/ethereum-vs-bitcoin