

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE
ZNANOSTI
Ak. god. 2018./ 2019.

Stanislav Šredl

Ethereum – revolucija kroz decentralizaciju

Završni rad

Mentor: Dr.sc. Vjera Lopina

Zagreb, 2018.

Sadržaj

1. Uvod	2
2. Povijest blockchaina	3
3. Nastanak Ethereuma	6
4. Pametni ugovori.....	8
5. Rast Ethereuma	10
6. Inicijalna ponuda tokena (ICO).....	13
7. Problemi i nedostatci	16
7.1 Opasnosti pametnih ugovora	16
7.2 Problemi skalabilnosti.....	18
7.3 Problemi centralizacije	22
8. Budućnost Ethereuma.....	23
8.1 Ethereum u širokoj primjeni.....	25
9. Zaključak	27
10. Literatura	28

1. Uvod

U kolovozu 2008. nepoznati programer (ili grupa programera) predstavljen pod pseudonimom Satoshi Nakamoto je pokrenuo Bitcoin, online valutu i sustav plaćanja koji umjesto oslanjanja na centralni autoritet za verifikaciju transakcija koristi kriptografiju. Bitcoin je u idućem desetljeću ostvario veliku popularnost no njegova primarna primjena ostala je vrlo ograničena i svodi se na slanje i primanje digitalne valute -- bitcoina.

Ipak, blockchain tehnologija, koja je jedan od temelja funkcioniranja Bitcoina, omogućuje izvršavanje drugih vrsta transakcija i pohranu drugih vrsta podataka osim onih financijske prirode.

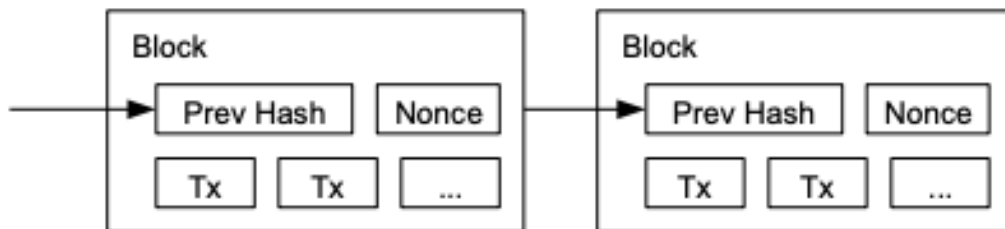
Pet godina kasnije, mladi programer rusko-kanadskog porijekla Vitalik Buterin predstavlja Ethereum, blockchain platformu koja omogućuje izvršavanje znatno kompleksnijih transakcija, tzv. smart contracta ili pametnih ugovora. Ovaj radikalni koncept Ethereum zapravo čini globalnom računalnom platformom za decentralizirane aplikacije (eng. decentralized apps (dApps)).

Ethereum je službeno pušten u pogon u srpnju 2015., a tri godine kasnije na njemu se nalaze na stotine aktivnih dAppova. Uz to, Ethereum se pokazao izuzetno pogodan za crowdfunding kroz prodaju tokena na toj platformi (tzv. initial coin offering ili ICO), što je omogućilo pokretanje više stotina projekata ali i postavilo mnoga pitanja o regulativi ovog posve novog načina financiranja.

2. Povijest blockchaina

Jedna od ključnih tehnologija na koju se Bitcoin oslanja jest blockchain. U Bitcoinu je blockchain implementiran kao baza podataka gdje su zapisi podijeljeni u blokove, pri čemu svaki blok ima zapisano vrijeme nastanka (timestamp) te je kriptografski povezan sa prethodnim blokom. Zapisi u blokovima odnose se na financijske transakcije na mreži te pokazuju koji je korisnik, identificiran putem posebne adrese, kome i koliko poslao bitcoina. Svaka takva transakcija se putem peer-to-peer mreže šalje svim čvorovima (eng. nodes) na mreži. Čvorovi su korisnici koji imaju pokrenut Bitcoin softver i koji posjeduju kopiju kompletnog Bitcoinovog blockchaina, te koji jedni drugima šalju informacije o novim blokovima na mreži.

Posebni korisnici Bitcoin mreže nazvani rudari (eng. miners) skupljaju transakcije u blokove te “pronalaze” nove blokove rješavajući progresivno kompleksan matematički zadatak. Zadatak je definiran na način da je težak za riješiti ali svatko može lako provjeriti točnost rješenja. Kada jedan rudar pronade rješenje, šalje poruku svim čvorovima na mreži, javljajući da ima novi blok. Ukoliko je blok matematički ispravan, te ako su transakcije unutar njega validne (npr., transakcija nije validna ukoliko se bitcoin šalje sa adrese na kojoj nema bitcoina), on postaje dio blockchaina, rudar koji ga je našao je nagrađen novostvorenim bitcoinima, a ostali rudari nastavljaju tražiti rješenje za sljedeći blok. Na ovaj način onemogućuje se varanje na transakcijama te brisanje ili ubacivanje lažnih blokova u blockchain.



Slika 1 - Shematski prikaz Bitcoinovog proof-of-work algoritma. Izvor: <https://bitcoin.org/bitcoin.pdf>

Zbog zaštite od pojedinih vrsta napada na sustav, čvorovi na mreži uvijek prihvaćaju najduži blockchain kao validan, jer je on dokaz da iza njega stoji najveća količina

procesorske snage. Ovaj algoritam se generalno zove proof-of-work. Na taj način je vrlo teško prevariti sustav (primjerice proizvodnjom blokova sa lažnim transakcijama) jer je za to potrebno imati više od 51% procesorske snage cijelog sustava (Nakamoto 2008)¹.

Zahvaljujući ovim karakteristikama, Bitcoin se u narednih deset godina pokazao kao vrlo robusan i siguran sustav za slanje i primanje bitcoina, no mogućnosti su mu ograničene na upravo takve transakcije i još par uskih (neslužbenih) primjena, primjerice slanje jednostavnih poruka (Sedgwick 2018)².

Popularnost Bitcoina je polako rasla, te su se počele pojavljivati burze za kupovinu i prodaju bitcoina te servisi koji primaju bitcoin kao sredstvo plaćanja. S rastom popularnosti počele su se pojavljivati i ideje za drugačije primjene blockchaina. Obzirom da je Bitcoin softver otvorenog koda (eng. open source), relativno je jednostavno pokrenuti novi projekt zasnovan na bitcoinu no sa nešto drugačijim karakteristikama. Jedan od prvih zapaženijih takvih projekata bio je Namecoin³. Umjesto za financijske transakcije, Namecoin koristi blockchain za registriranje posebne vrste internetskih domena s nastavkom .bit. Za razliku od standardnih internetskih domena, koje dodjeljuje neki centralni autoritet, Namecoin je posve decentraliziran i omogućuje bilo kome da registrira bilo koju slobodnu domenu uz plaćanje Namecoinovom digitalnom valutom namecoin.

No, pravu revoluciju u pristupu prema blockchainu napravio je Ethereum. Osnovni parametri funkcioniranja Ethereum su slični kao kod Bitcoina -- također se koristi blockchain te proof-of-work algoritam. No umjesto fokusiranja na neku usku primjenu, Ethereum je omogućio izvršavanje tzv. pametnih ugovora (eng. smart contracts) na samom blockchainu. Ti ugovori "automatski pomiču digitalna dobra prema proizvoljnim,

¹ <https://bitcoin.org/bitcoin.pdf>

² <https://news.bitcoin.com/a-brief-history-of-hidden-messages-in-the-bitcoin-blockchain/>

³ <https://namecoin.org/>

prethodno zadatim pravilima" (Buterin 2013)⁴. Ethereum je ponudio vrlo robustan alat za izradu pametnih ugovora -- novi, Turing-potpuni programski jezik nazvan Solidity.

Na taj se način otvorila mogućnost izrade vrlo moćnih, decentraliziranih aplikacija na Ethereum platformi. Prednost takvih aplikacija nad konvencionalnim aplikacijama, koje se izvršavaju na nekom centralnom serveru, slične su kao i prednosti Bitcoina nad konvencionalnim bankarstvom. One se izvršavaju prema postavljenim pravilima bez potrebe da vjerujete nekom centralnom entitetu, a njihovo izvršavanje je nemoguće spriječiti ili zaustaviti (bez disrupcije ili uništenja čitave Ethereum platforme).

⁴ Originalni dokument je uklonjen; kopija preuzeta sa <https://whitepaperdatabase.com/ethereum-eth-whitepaper/>

3. Nastanak Ethereum

Od Buterinovog "whitepaper" dokumenta pa do pokretanja Ethereum protekle su dvije prilično burne godine. Projekt je okupio nekoliko blockchain stručnjaka, uključujući Gavina Wooda, koji je definirao Ethereum na tehničkoj razini u svom Yellow Paper dokumentu⁵ te izumio programski jezik Solidity⁶, Charlesa Hoskinsona koji je na početku bio direktor projekta, Jeffreya Wilkea, programera koji je izrazito puno doprinijeo projektu⁷, te Josepha Lubina, koji je bio ključan u pokretanju zaklade Ethereum Foundation u Švicarskoj⁸.

Zanimljivo je da su mnogi od spomenutih kasnije napustili projekt; Wood je, između ostalog, pokrenuo svoj blockchain projekt pod imenom Polkadot⁹, Hoskinson je jedan od suosnivača projekta Cardano¹⁰ koji je direktna konkurencija Ethereumu, dok je Lubin pokrenuto ConsenSys¹¹, tvrtku koja nudi kompanijama korporativne usluge vezane za blockchain. Glavno lice Ethereum do danas ostaje Buterin, koji je projektu značajno pridonio prijedlozima rješenja za mnoge probleme koje Ethereum ima, ponajprije problem slabe skalabilnosti¹².

Ethereum je strukturiran kao neprofitna zaklada s bazom u švicarskom kantonu Zug, a ne kao klasična kompanija. Projekt se financirao 2014. putem inicijalne ponude tokena (eng. Initial Coin Offering (ICO)), gdje se sakupilo 17.3 milijuna dolara¹³. Unatoč padu

⁵ <http://yellowpaper.io/>

⁶ Prema podacima sa <http://gavwood.com/>,

⁷ Wilkeovi doprinosi mogu se vidjeti na Ethereumovom github repositoriju, dostupnom na: <https://github.com/ethereum/go-ethereum/graphs/contributors>

⁸ Prema podacima sa <https://bravenewcoin.com/insights/after-three-years-of-ethereum-how-close-are-we-to-web-3-0>

⁹ <https://polkadot.network/>

¹⁰ <https://www.cardano.org/en/home/>

¹¹ <https://consensys.net/>

¹² Neki od Buterinovih prijedloga su dostupni na njegovom Medium profilu, <https://medium.com/@VitalikButerin>

¹³ Prema podacima sa <https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview/>

vrijednosti bitcoina koji je uslijedio i financijski ugrozio zakladu, Ethereum je opstao te je projekt pokrenut u srpnju 2015. godine.

Jedan od ključnih momenata nakon pokretanja bilo je definiranje ERC-20 standarda¹⁴ za digitalne tokene na Ethereumovom blockchainu u studenom 2015. godine. Tim se standardom svima omogućila relativno jednostavna izrada novih blockchain projekata sa svojim vlastitim digitalnim tokenima, koji imaju gotovo sve karakteristike samog Ethereumovog tokena -- ethera.

Prednost tokena zasnovanih na Ethereumu za razliku od, primjerice, bitcoina, je u tome što se u same tokene može ugraditi dodatna funkcionalnost. Na taj način tokeni nisu samo puka jedinica vrijednosti već svaki od njih predstavlja pametni ugovor (vidi poglavlje 4) koji vlasniku može dati gotovo vrlo raznovrsne mogućnosti, primjerice vlasništvo ili postotak vlasništva nad nekim dobrom ili mogućnost sudjelovanja u glasanju oko nekog pitanja.

Ova revolucionarna ideja, u kombinaciji sa relativno jednostavnim procesom izrade nove kriptovalute na Ethereumovoj platformi, je pokrenula pravu lavinu novih kriptovaluta zasnovanih na ERC-20 standardu -- u ovom trenutku široko korištenih tokena ima preko 850¹⁵.

¹⁴ Tehnički opis ERC-20 standarda nalazi se ovdje:

<https://github.com/ethereum/eips/issues/20>

¹⁵ Prema podacima sa <https://eidoo.io/erc20-tokens-list/>

4. Pametni ugovori

U kontekstu blockchaina, pametni ugovori su postojali i prije Etheruma. Američki programer Nick Szabo definirao je koncept još 1996., u knjizi *Smart Contracts: Building Blocks for Digital Markets*. "Osnovna ideja pametnih ugovora jest da puno vrsta ugovornih klauzula (...) može biti ugrađeno u hardver i softver s kojim imamo interakcije, na način da se povreda ugovora napravi skupom (...) za onoga tko ga povrijedi." (Szabo, 1996)¹⁶.

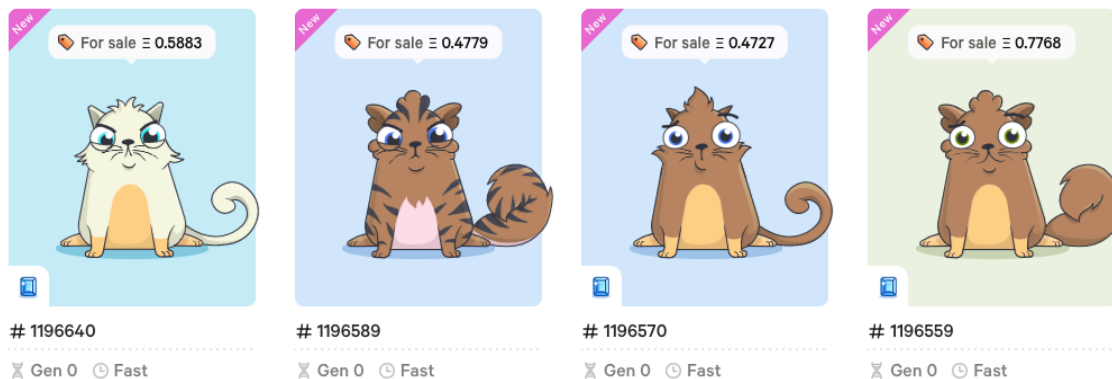
Bitcoin je jedan od prvih široko poznatih projekata koji je ovaj koncept proveo u djelo. Bitcoin ima svoj Script¹⁷ programski jezik koji omogućuje izradu jednostavnih pametnih ugovora, što se primjerice može koristiti za tzv. multi-signature (multisig) transakcije, gdje je potrebno više potpisnika da bi se poslala sredstva s neke adrese. No, Script ne dopušta korištenje programskih petlji te stoga na njemu nije moguće graditi kompleksne pametne ugovore.

Ethereumov Solidity ima puno manje ograničenja te je zato na Ethereumovoj platformi moguće napraviti vrlo kompleksne aplikacije. Primjeri aplikacija na Ethereumu variraju od relativno jednostavnih ugovora tipa riznica: "A može podići do X jedinica valute na dan, B može podići do Y po danu, A i B zajedno mogu podići koliko god žele, a A može spriječiti B da podiže valutu." (Buterin, 2013). S druge strane imamo znatno kompleksnije aplikacije tipa Cryptokitties¹⁸, igre u kojoj igrači skupljaju, uzgajaju i razmjenjuju digitalne mačke.

¹⁶ Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*
http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

¹⁷ Script je tehnički opisan ovdje <https://en.bitcoin.it/wiki/Script>

¹⁸ <https://www.cryptokitties.co/>



Slika 2 - Cryptokitties, jedinstvene digitalne reprezentacije mačaka na Ethereumovom blockchainu, kupuju se pomoću ethera i često dosežu cijenu od nekoliko stotina dolara po komadu. Izvor: <https://www.cryptokitties.co/>

Ključna inovacija kod implementacije pametnih ugovora na Ethereumu je koncept goriva (eng. gas). Riječ je zapravo o naplaćivanju izvršavanja pametnog ugovora putem Ethereumove digitalne valute, ethera. Svako izvršavanje ugovora košta neku malu količinu ethera koji se u ovom kontekstu zove gas. Na taj način se istovremeno nagrađuje rudare (eng. miners) koji odrađuju izvršavanje pametnih ugovora, te sprečava zlorabu u smislu izrade prohibitivno skupih pametnih ugovora koji bi trošili previše resursa na mreži.

Već spomenuti tokeni također su vrlo bitan dio Ethereumovog ekosustava. Većina tokena udovoljava standardu ERC-20, što znači da moraju poštovati određena pravila koja sprečavaju prevare i omogućuju zamjenu jednih tokena za druge. Iako ERC-20 tokeni nemaju vlastiti blockchain već se nalaze na Ethereum blockchainu, korištenje tokena (primjerice, slanje i primanje) je za korisnika gotovo identično kao i korištenje ethera. No, ponašanje i dodatne mogućnosti svakog tokena definirani su pametnim ugovorom koji ga je stvorio. Ovo čini tokene izrazito raznovrsnom i moćnom reprezentacijom digitalnog vlasništva uz zadržavanje interoperabilnosti unutar sustava.

5. Rast Ethereumu

Ethereum je vrlo brzo nakon pokretanja stekao veliku popularnost, koja se dobro ogleda u broju transakcija na mreži. Već krajem 2015. godine taj je broj povremeno prelazio 20,000 dnevno; u 2016. je prvi put prešao 50,000 dnevno, da bi krajem 2017. godine prešao brojku od milijun transakcija dnevno¹⁹.

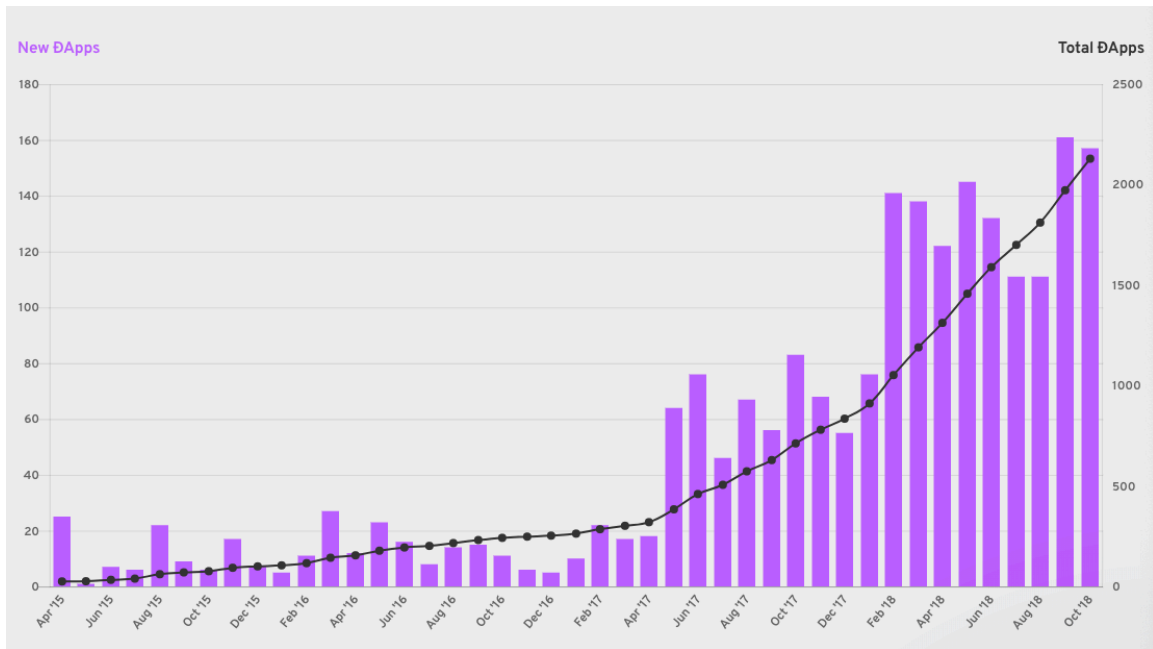


Slika 3 - Broj transakcija na Ethereumovoj platformi. Izvor: <https://bitinfocharts.com>

Pri tom valja imati na umu da su neke od ovih transakcija jednostavno prebacivanje ethera sa jedne adrese na drugu, dok druge izvršavaju neki kompleksniji pametni ugovor. No postoje i drugi pokazatelji stvarne aktivnosti na mreži. Jedan od njih je broj aktivnih decentraliziranih aplikacija, koji je od brojke 25 u travnju 2015. narastao na preko 2,200 u listaopadu 2018. godine²⁰.

¹⁹ Podaci preuzeti sa <https://bitinfocharts.com>

²⁰ Podaci preuzeti sa <https://www.stateofthedapps.com/>



Slika 4 - broj decentraliziranih aplikacija na Ethereumovoj platformi. Izvor: <https://www.stateofthedapps.com/>

Još jedan pokazatelj rasta popularnosti Ethereuma jest cijena ethera, koja je od oko \$0.48 u listopadu 2015. (najniža tržišna cijena te godine prema CoinMarketCap) narasla na \$1,416 u prosincu 2017. Nakon toga je cijena znatno pala te se u trenutku pisanja ovog teksta kreće oko \$150, što je još uvijek rast od preko 30,000% u tri godine²¹.

²¹ Podaci preuzeti sa <https://coinmarketcap.com/currencies/ethereum/>

Ethereum Charts



Slika 5 - Kretanje cijene Ethereum u posljednje tri godine. Izvor: <https://coinmarketcap.com/currencies/ethereum/>

Svi ovi pokazatelji upućuju na solidnu količinu interesa za razvoj i korištenje aplikacija na Ethereumu, koji bi možda bio i veći da neke od popularnijih aplikacija nisu zagušile mrežu i ukazale na problem skalabilnosti (vidi poglavlje 7.2). No, nagli pad cijene te nešto blaži pad broja transakcija na mreži u 2018. godini upućuju na potencijalno smanjivanje interesa za ovom platformom i decentraliziranim aplikacijama općenito.

6. Inicijalna ponuda tokena (ICO)

Ethereum je otvorio mogućnosti pokretanja raznovrsnih projekata zasnovanih na blockchainu, pa se ubrzo nametnulo pitanje: Koji će od tih projekata biti prvi koji će biti prihvaćen od šire publike, a ne samo od manjeg broja kripto entuzijasta? Na takvo što nije trebalo puno čekati; već godinu i pol nakon pokretanja Ethereuma postalo je jasno da je to inicijalna ponuda tokena (ICO) (Emin Gün Sirer, 2017)²².

Riječ je o novom načinu financiranja blockchain projekata, pri čemu se stvaraju novi digitalni tokeni koji najčešće imaju neku specifičnu mogućnost, definiranu pametnim ugovorom. Prije generiranja tokena javnosti se nudi kupovina određenog broja tokena, najčešće putem zamjene za ether²³. Sam proces razlikuje se od projekta do projekta, no najčešće bi potencijalni ulagači prvo iskazali interes za kupnju tokena, a potom bi u određenom vremenskom periodu slali ether, te bi zauzvrat dobili novonastale tokene.

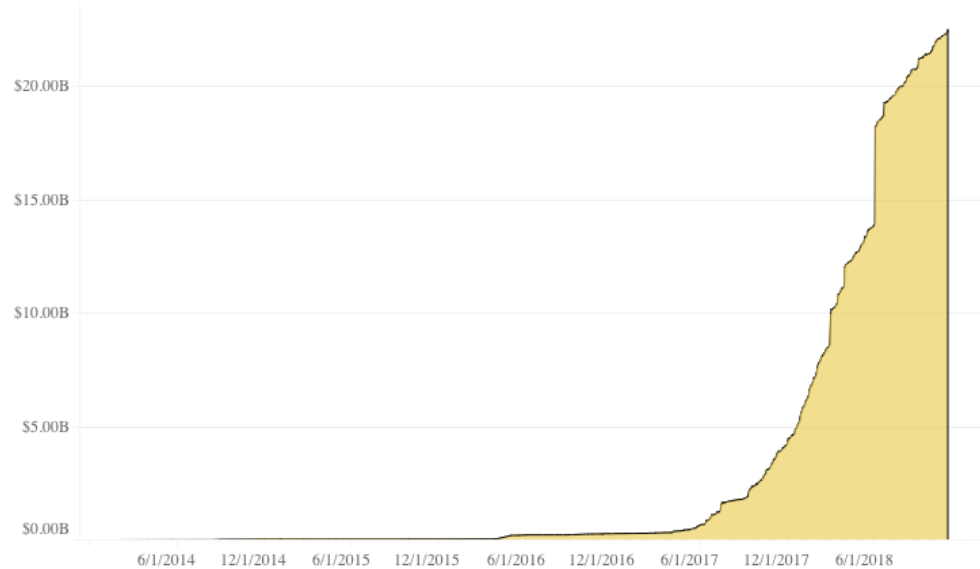
Obzirom da je ether nedugo nakon pokretanja Ethereuma imao relativno stabilnu vrijednost te ga je bilo moguće zamijeniti za fiat valute, novonastali startupi koji su se financirali putem ICO-a često su uspijevali skupiti ozbiljna financijska sredstva, ponekad i više desetaka milijuna dolara. U trenutku pisanja ovog teksta, putem ICO-ova skupilo se preko 22 milijarde dolara²⁴.

²² <https://twitter.com/el33th4xor/status/870327595434463232>

²³ Ether nije jedina kripto valuta koja se koristi u ICOovima; ponekad je to bio i bitcoin ili druge kriptovalute. Također, koncept ICOa postojao je prije Ethereum; sam Ethereum stvoren je jednim od najranijih uspješnih ICOova, pri čemu su korisnici ether tokene kupovali pomoću bitcoina. Izvor: <https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview/>.

²⁴ Podaci preuzeti sa <https://www.coindesk.com/ico-tracker>

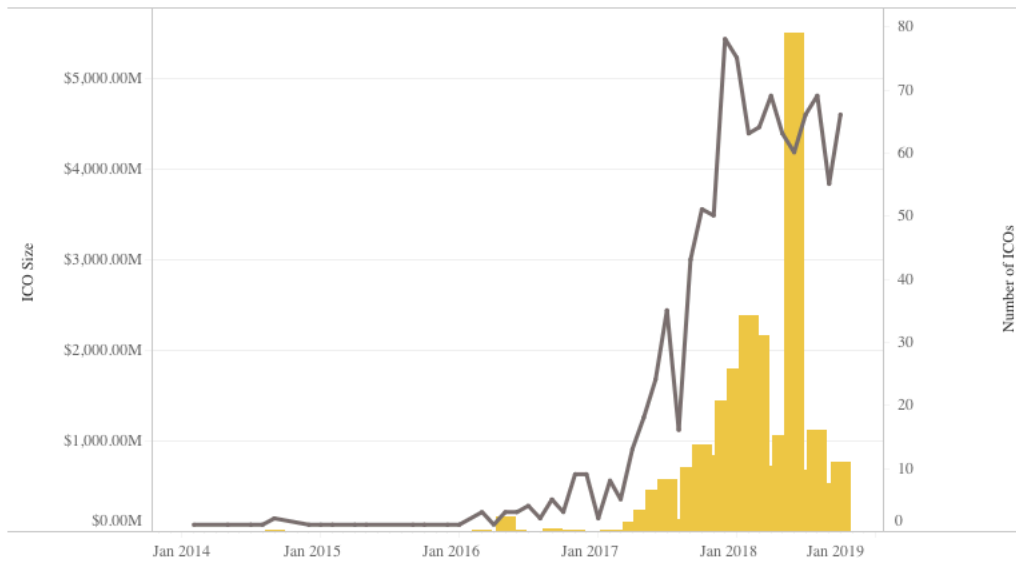
All-Time Cumulative ICO Funding



Slika 6 - Sredstva sakupljena putem ICO-ova. Izvor: <https://www.coindesk.com/ico-tracker>

ICO kao način financiranja ima nekoliko prednosti nad klasičnim načinima financiranja, među kojima se ističu znatno manje papirologije i mogućnost prikupljanja velike količine novca u vrlo kratkom vremenskom periodu. Također, ICO-ovi su za razliku od klasične inicijalne javne ponude dionica (eng. Initial Public Offer ili IPO) bili dostupni gotovo svim ulagačima, što je u skladu s principima decentralizacije na kojima je zasnovan Ethereum.

Monthly New ICO Funding



Slika 7 - Sredstva sakupljena putem ICO-ova na mjesečnoj bazi. <https://www.coindesk.com/ico-tracker>

No, ICO-ovi su privukli pozornost regulatornih tijela kao što su američki SEC (Securities and Exchange Commission) koji su krajem 2018. počeli globiti neke od tvrtki koje su pokrenule ICO a da ga prethodno nisu registrirali kod SEC-a²⁵. Pritom je ključno pitanje da li se tokeni distribuirani putem ICOa mogu klasificirati kao vrijednosni papiri, a stajalište SEC-a je da u određenom dijelu slučajeva mogu. Svaki takav ICO koji se nije registrirao je prema tumačenju SEC-a u prekršaju.

Usljed drastičnog pada cijene Ethereuma u 2018. godini te SEC-ovih globi, krajem 2018. količina novca prikupljena u ICO-ovima se znatno smanjuje, s preko 5.5 milijardi dolara u siječnju na 770 milijuna dolara u listopadu²⁶.

²⁵ <https://www.sec.gov/litigation/admin/2018/33-10575.pdf>

²⁶ Podaci preuzeti sa <https://www.coindesk.com/ico-tracker>

7. Problemi i nedostatci

7.1 Opasnosti pametnih ugovora

Ethereum kao platforma za pametne ugovore ima mnoge prednosti nad Bitcoinom, no ima i jedan veliki nedostatak. Solidity je Turing-kompletan programski jezik, i na njemu se mogu izvršavati programske petlje, što otvara mogućnost izrade vrlo kompleksnih aplikacija, no također i katastrofalnih grešaka u programu. Također, tu je mogućnost izrade malicioznih aplikacija koje bi mogle ugroziti čitav sustav.

Taj se problem najočitiije pokazao kod tzv. DAO hacka koji se dogodio u lipnju 2016. DAO (eng. decentralized autonomous organization -- decentralizirana autonomna organizacija) je tip organizacije koji djeluje autonomno, isključivo kroz pametne ugovore. Prva takva organizacija na Ethereumovoj platformi pokrenuta je u svibnju 2016. pod nazivom The DAO. Riječ je bio o nekoj vrsti investicijskog fonda koji je sakupio oko 12.7 milijuna ethera (tada vrijednih oko 150 milijuna dolara), gdje su članovi mogli glasati za projekte koji će dobiti sredstva za rad iz te riznice novca. No, u lipnju je nepoznati napadač je pronašao grešku u kodu koja mu je omogućila da neovlašteno povuče sredstva iz riznice, te je na svoju adresu prebacio 3.6 milijuna ethera, u to vrijeme vrijednih \$70 milijuna dolara. (Falkon, 2017)²⁷.

Ovaj je slučaj rezultirao prvim, velikim, neplaniranim račvanjem (eng. hard fork) Ethereuma koje se dogodilo u srpnju 2016. Zaklada koja upravlja projektom odlučila je promijeniti kôd projekta na način da se poništi šteta koju je napravio napadač na The DAO. Kod račvanja blockchain projekata zapravo nastaju dva nova blockchain projekta, s tim da sudionici mreže, prvenstveno rudari, nastave raditi na novom projekta, dok se stari napušta. No, neki članovi Ethereumove zajednice nisu se složili sa odlukom da se poništi napad na DAO, te su nastavili voditi staru verziju Ethereuma koja je od tog trenutka poznata kao Ethereum Classic (Pearson, 2016)²⁸.

²⁷ <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>

²⁸ https://motherboard.vice.com/en_us/article/z43qb4/the-ethereum-hard-fork-spawned-a-shaky-rebellion-ethereum-classic-etc-eth

Epizoda s napadom na The DAO značajna je jer je ukazala na još jedan potencijalni problem Etheruma²⁹, a to je problem upravljanja (eng. governance). Nemogućnost ključnih ljudi koji su u to vrijeme stajali iza Etheruma da se dogovore oko smjera u kojem bi projekt trebao krenuti ukazuje na mogućnost sličnih takvih problema u budućnosti. Ethereum osim ove izvanredne epizode nije imao većih problema sa nadogradnjama, koje su zbog arhitekture sustava gotovo uvijek u tehničkom smislu račvanja. No takva se račvanja događaju relativno često³⁰ i svako račvanje može biti potencijalni problem ako se ne dogodi konsenzus oko smjera u kojem treba ići.

²⁹ S ovim se problemom u nekoj mjeri susreću svi projekti zasnovani na blockchainu čiji je cilj neki stupanj decentralizacije.

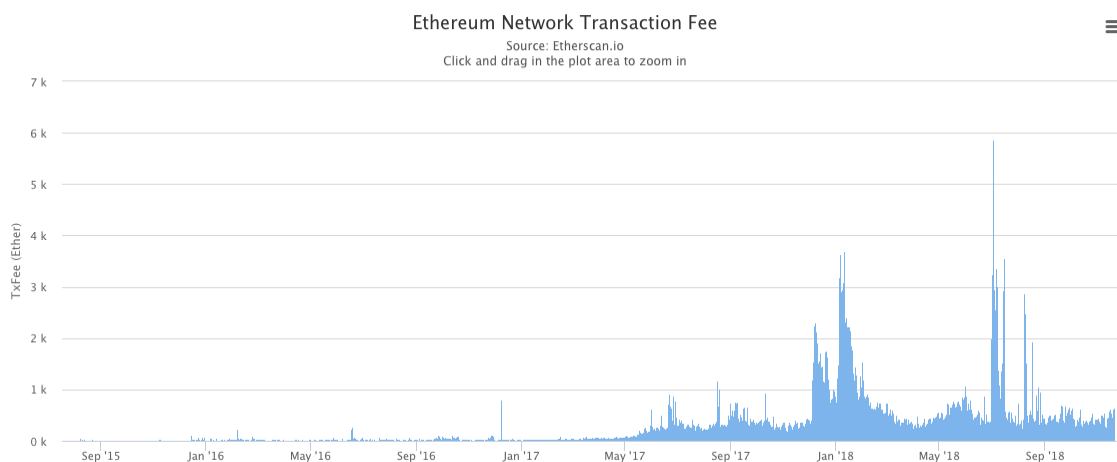
³⁰ Do sad ih je bilo pet, prema

<https://ethereum.stackexchange.com/questions/13014/please-provide-a-summary-of-the-ethereum-hard-forks>

7.2 Problemi skalabilnosti

Daleko najozbiljniji problem Ethereumu u ovom trenutku je skalabilnost. Ethereum u ovom trenutku podržava maksimum od 15 transakcija u sekundi (eng. transactions per second ili TPS), što je nedovoljno za, primjerice, neku ozbiljniju financijsku aplikaciju na globalnoj razini³¹.

Ovaj se problem prvi put ozbiljnije pojavio u praksi s porastom popularnosti inicijalnih ponuda tokena, kod kojih je često vladalo pravilo "tko prvi, njegova djevojka" (eng. first come, first serve). Radi toga bi se u kratko vrijeme dogodio velik broj transakcija od strane korisnika koji su željeli sudjelovati u ICO-u, pa bi mreža znatno usporila, a cijene transakcija bi porasle.

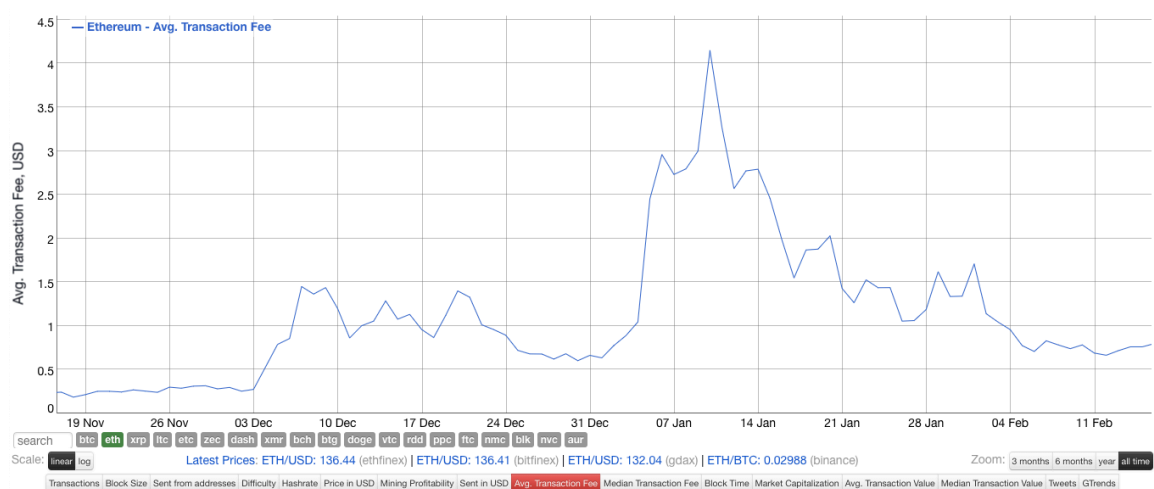


Slika 8 - Cijena transakcija na Ethereumovoj platformi u posljednje tri godine. Izvor: <https://etherscan.io/chart/transactionfee>

Puna ozbiljnost problema postala je jasna s naglim porastom popularnosti igre Cryptokitties, koja se oslanja na Ethereumov blockchain. U studenom 2017. godine zbog Cryptokittiesa su cijene transakcija na Ethereumu, kao i broj transakcija koje čekaju na

³¹ U ovom kontekstu se često spominje Visa, koja je krajem 2016 procesuirala oko 1,700 transakcija u sekundi s teoretikom od 56,000 transakcija u sekundi. (izvor: <https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html>)

izvršenje, dramatično porasle, dovevši u pitanje normalno funkcioniranje mreže³². Za razliku od problema s ICO-ovima, koji su najčešće trajali par sati ili pokoji dan, Cryptokitties je gušio mrežu Etheruma više tjedana.



Slika 9 - Cijena transakcija na Ethereumovoj platformi od sredine studenog 2017. do sredine veljače 2018. godine. Izvor: <https://bitinfocharts.com/comparison/ethereum-transactionfees.html>

Predloženo je više rješenja ovog problema. Jedno od njih je prelazak na proof-of-stake (PoS) algoritam postizanja konsenzusa, koji bi zamijenio proof-of-work (PoW) algoritam koji se trenutno koristi. Kod proof-of-stake algoritma nove transakcije ne potvrđuju rudari doniranjem svojeg procesorskog vremena, već vlasnici same valute ether koji su neku količinu ethera posvetili toj svri. Pritom se stvaratelj sljedećeg blocka u Ethereumovom blockchainu bira kombinacijom nasumičnog odabira i uzimanja u obzir nekih parametara kao što su količina ethera koju netko posjeduje te vrijeme posjedovanja³³.

Prelazak na proof-of-stake primarno rješava neke druge probleme, primjerice smanjuje se potrošnja električne energije potrebne za rad mreže. No njegova nuspojava teoretski je i povećanje mogućeg broja transakcija na mreži³⁴. U ovom trenutku nije jasno do koje

³² <https://www.bbc.com/news/technology-42237162>

³³ <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs>

³⁴ <https://ethereum.stackexchange.com/questions/5708/can-proof-of-stake-pos-improve-the-number-of-transactions-per-second>

mjere PoS može ubrzati broj tps-a na Ethereumu, ali ga je bitno spomenuti jer je on službeno u Ethereumovom dugoročnom planu razvitka (eng. roadmap).

Druga predložena rješenja problema skalabilnosti uključuju razlamanje (eng. sharding), bočne lance (eng. sidechains) i plazma (eng. plasma).

Razlamanje je termin koji dolazi iz klasičnih baza podataka. Trenutno, kod Ethereumovog blockchaina svaki čvor pohranjuje sva stanja (iznose na računima, kôd pametnih ugovora te pohranjene podatke) i procesira sve transakcije. Razlamanjem bi se napravio novi mehanizam kod kojeg bi samo mali dio čvorova na mreži verificirao određene transakcije. Na ovaj način se smanjuje sigurnost, ali ideja je da dovoljno mali broj čvorova verificira transakciju da sustav ostane siguran, a da se paralelno procesira velik broj transakcija, što bi znatno ubrzalo mrežu³⁵.

Bočni lanci su zapravo zasebni blockchainovi na kojima radi određena aplikacija ili skup aplikacija, koji su pak povezani s glavnim, Ethereumovim blockchainom. Premda to samo po sebi ne povećava potencijalni broj transakcija u sekundi na Ethereumu, na taj način neka aplikacija može raditi vrlo brzo a da pritom ne opterećuje glavnu mrežu. Glavni nedostatak ovog pristupa je određeni gubitak decentralizacije, dok je prednost relativno laka implementacija bez promjena na samom kodu Ethereumu (Konstantopolous, 2018)³⁶.

Plazma je rješenje koje je, u nekoliko iteracija, predložio sam Buterin u suradnji s Josephom Ponom, a radi se o prebacivanju određenih transakcija izvan glavnog Ethereumovog blockchaina (eng. off-chain), koji se onda koristi primarno za sigurnosnu verifikaciju da su transakcije validne (Buterin, Poon, 2017)³⁷. Plazma donosi nekoliko važnih prednosti, među kojima se ističu mogućnost provođenja puno većeg broja transakcija po sekundi, smanjivanje količine nepotrebnih podataka na Ethereumovom

³⁵ <https://github.com/ethereum/wiki/wiki/Sharding-FAQs>

³⁶ <https://medium.com/loom-network/million-user-dapps-on-ethereum-an-introduction-to-application-specific-sidechains-c0fdc288c5e5>

³⁷ <https://plasma.io/plasma.pdf>

blockchainu te potencijalno smanjenje cijene transakcija. Buterin i drugi autori su u 2018. godini predstavili i nekoliko novih, poboljšanih verzija Plasma protokola, primjerice Plasma Cash, Plasma Debit i More Viable Plasma (Zhang, 2018)³⁸.

Sva predložena rješenja su u relativno ranom stadiju razvoja; na njima se radi paralelno ali niti jedno još nije isprobano na velikom, produkcijskom (eng. production) blockchain projektu kao što je Ethereum.

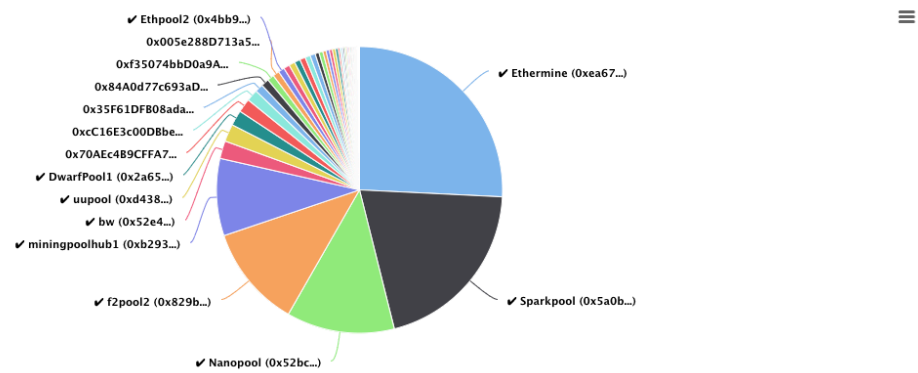
Također, svako od ovih rješenja dodatno povećava kompleksnost čitavog sustava te potencijalno donosi nove probleme koji bi pak mogli dodatno usporiti razvoj platforme.

³⁸ <https://media.consensys.net/the-state-of-plasma-1-6b48c1e4b295>

7.3 Problemi centralizacije

Ključna karakteristika Ethereuma je decentraliziranost, tj. nemogućnost jednog entiteta ili manjeg broja udruženih entiteta da zaustavi ili omete izvršavanje nekog pametnog ugovora na mreži. No, Ethereum trenutno sprečava napade na mrežu pomoću proof-of-work algoritma (sličnom onome koji koristi Bitcoin), što je pak stvorilo situaciju gdje nekoliko velikih rudarskih kompanija, primarno lociranih u Kini, kontrolira nesrazmjerno veliki hashrate³⁹ -- u trenutku pisanja teksta, 5 velikih poolova⁴⁰ kontrolira preko 75% Ethereumovog hashratea⁴¹. Pošto rudari odlučuju o nekim vrlo važnim karakteristikama mreže -- primjerice koju će verziju Ethereum softvera koristiti -- iz ovoga se vidi da je Ethereum u velikoj mjeri ovisan o svega nekoliko entiteta te se ne može smatrati značajno decentraliziranim.

Top Miners over the last 24h



Slika 10 - Najveći rudari u posljednjih 24 sata na dan 22. studenog, 2018. Izvor: <https://www.etherchain.org/charts/topMiners>

Ovaj problem mogao bi se riješiti planiranim prelaskom na proof-of-stake algoritam, no tada se otvaraju nove mogućnosti manipulacije mrežom jer bi se tada entiteti koji posjeduju veliku količinu Ethereuma mogli udružiti u raznorazne interesne grupe.

³⁹ Brzina kojom rudari provode računске operacije kojima se pronalazi novi ether.

⁴⁰ Udružena grupa rudara kriptovalute koja djeluje kao cjelina.

⁴¹ Podaci preuzeti sa <https://www.etherchain.org/charts/topMiners>

8. Budućnost Ethereumu

Uspješnost Ethereumu kao globalne platforme za decentralizirane aplikacije ovisi primarno o brzom i uspješnom rješenju gorespomenutih problema. Sljedeće račvanje pod nazivom Constantinople planirano je za početak 2019. godine ali ono po trenutnom planu neće donijeti implementaciju nijednog predloženog rješenja za problem skalabilnosti. Najranije se ta rješenja mogu očekivati sredinom 2019. godine⁴².

Kao što se vidi u konstantnom porastu broja novih decentraliziranih aplikacija na platformi, interes ne jenjava unatoč slaboj skalabilnosti i relativnoj centraliziranosti. Zanimljivo je pogledati i presjek prema vrsti aplikacija na platformi. Na prvom mjestu su burze i mjenjačnice, zatim sustavi za pohranu, nakon čega slijede financijske aplikacije, kockanje i igre⁴³.

Categories				
Category	Total DApps	Monthly active users ?	Transactions (30d) ?	# of contracts
<u>EXCHANGES</u>	181	51.45k	792.58k	442
<u>STORAGE</u>	55	41.55k	61.64k	19
<u>FINANCE</u>	229	25.28k	92.29k	2.02k
<u>GAMBLING</u>	490	20.71k	518.46k	1.31k
<u>GAMES</u>	451	11.52k	466.03k	955

Slika 11 - Vrste aplikacija na Ethereumu. Izvor: <https://www.stateofthedapps.com/stats>

Broj dnevnih aktivnih korisnika je negdje oko 26,000 prema <https://www.stateofthedapps.com/stats>, s oko 1.27 milijuna transakcija na dan. S jedne strane te brojke su još uvijek malene, tako da je prostor za rast ogroman. S druge strane, u

⁴² Podaci preuzeti sa <https://www.mangoresearch.co/ethereum-roadmap-update/>.

⁴³ Podaci preuzeti sa <https://www.stateofthedapps.com/stats>

ovom trenutku Ethereum ne bi mogao ni podnijeti znatno veće brojke zbog već spomenutih problema skalabilnosti.

Konkurencije ima mnogo, no zapravo je malo globalnih platformi za pametne ugovore široke primjene koje su u punom pogonu. Jedna koja se ističe je EOS, koji prema <https://www.stateofthedapps.com/stats> trenutno ima 94 aplikacije i oko 13,700 dnevno aktivnih korisnika. EOS u teoriji omogućuje dramatično veći broj transakcija po sekundi (milijuni), no, EOS je znatno manje decentraliziran od Ethereuma, obzirom da je cijela mreža⁴⁴ zasnovana na svega 21 čvorova⁴⁵. Tu je i kineski NEO, koji također ima manji broj čvorova koji mogu donositi odluke (tzv. consensus nodes) , od trenutnih 7 do maksimalnih 1,024⁴⁶.

Postoji još mnoštvo obećavajućih projekata u raznim stupnjevima razvoja, među kojima se ističu Cardano, Dfinity i Stellar. Valja spomenuti i sam Bitcoin koji se može koristiti kao podloga za pametne ugovore⁴⁷. No, u ovom trenutku Ethereum vodi po broju korisnika, aplikacija, aktivnosti i čvorova na mreži i ima dobre izgleda da ostane na prvom mjestu, pogotovo ako se riješe spomenuti problemi.

⁴⁴ Prema podacima sa

<https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md>

⁴⁵ Za usporedbu, Ethereum trenutno ima preko 12,400 čvorova prema <https://www.ethernodes.org/>

⁴⁶ Prema podacima sa <https://medium.com/neo-smart-economy/how-to-become-a-consensus-node-27e5317722e6>

⁴⁷ <https://bitcoinmagazine.com/articles/yes-bitcoin-can-do-smart-contracts-and-particl-demonstrates-how/>

8.1 Ethereum u širokoj primjeni

Prihvatanje Ethereuma kao platforme za razvoj decentraliziranih aplikacija od strane razvojnih programera je izuzetno važno, no jednako je bitno da se te aplikacije počnu koristiti u širokoj primjeni. Da bi se to dogodilo, potrebno je ukloniti ili barem smanjiti mnoge prepreke koje u ovom trenutku čine ove aplikacije nedovoljno atraktivnim ili prekompleksnim za prosječnog korisnika.

Ključni problemi su:

1. Kompleksnost uporabe, kako decentraliziranih aplikacija tako i samog Ethereuma tj. ethera čije je posjedovanje preduvjet za korištenje svih aplikacija na sustavu. Već i samo slanje ethera ili nekog tokena zahtijeva korištenje duge i nerazumljive adrese te upisivanje parametara kao što su "gas price" i "gas limit" što može biti teško razumljivo prosječnom korisniku⁴⁸.
2. Volatilnost cijene (kako ethera tako i tokena na Ethereumovom ekosustavu). Cijena ethera i tokena često pada ili raste više postotaka ili čak na desetke postotaka u danu, što može obeshrabriti krajnje korisnike⁴⁹.
3. Visoka cijena ulaska (eng. barrier to entry). Korisnik koji želi sudjelovati u sustavu mora na neki način kupiti ether te ga pohraniti na digitalnom novčaniku (eng. wallet) koji je prethodno konfigurirao. Također mora poznavati elementarne koncepte vezane uz blockchain te naučiti koristiti alate za praćenje transakcija na blockchainu kao što je Etherscan⁵⁰.
4. Nedostatak regulative i sigurnosni rizici. Korisnik je u većini slučajeva sam odgovoran za pohranu ethera i tokena te može radi pogreške ili sigurnosnog problema izgubiti sredstva, pri čemu ne postoji neko tijelo koje ga štiti i jamči povrat sredstava. Također, svijet kriptovaluta prepun je prevara, od lažnih ICOova preko lažnih kripto novčanika i mjenjačnica pa do hakerskih napada. U lipnju ove

⁴⁸ <https://ethereum.stackexchange.com/questions/3/what-is-meant-by-the-term-gas>

⁴⁹ Prema podacima sa: <https://coinmarketcap.com/currencies/ethereum/>

⁵⁰ <http://etherscan.io/>

godine je broj ukradenog ethera dosegao brojku od najmanje 38,179, što je u to vrijeme vrijedilo oko 23 milijuna dolara (Arvanaghi, 2018)⁵¹.

Premda su svi ovi nedostaci u određenoj mjeri prisutni, vide se pozitivni pomaci, pogotovo u posljednjih godinu dana.

Nabavka ethera, koji je preduvjet za sudjelovanje u sustavu, je danas razmjerno jednostavna putem relativno pouzdanih mjenjačnica kao što su američki Coinbase⁵² ili luksemburški Bitstamp⁵³. Same mjenjačnice ali i mnogi projekti izgrađeni na Ethereumu su danas znatno bolje regulirani, bilo od strane američkog SEC-a ili od regulatornih tijela u drugim zemljama. Mnogi od njih uveli su i dodatne sigurnosne mjere kako bi zaštitili korisnike od prevara.

Volatilnost cijene još uvijek je velik problem, no postoje naznake rješenja u vidu tzv. stablecoina, posebnih tokena (većinom izgrađenih na Ethereumu) čija je cijena vezana za neku fiat valutu ili drugu vrstu imovine iz stvarnog svijeta. Primjeri stablecoina su Dai⁵⁴ čija se vrijednost algoritamski održava bliskom dolaru, i TrueUSD⁵⁵, koji je također vezan uz dolar ali se njegova vrijednost održava na istoj razini putem rezerve u stvarnoj fiat valuti.

Što se tiče kompleksnosti i visoke cijene ulaska, ovi problemi su još uvijek prisutni ali i tu se događaju pozitivni pomaci. Jedan od primjera je MetaMask⁵⁶, kripto-novčanik koji funkcionira kao dodatak za popularne web preglednike tipa Chrome. On omogućuje jednostavnu integraciju sa decentraliziranim aplikacijama koje se izvršavaju u web pregledniku; nakon jednostavnog otključavanja korisničkog novčanika putem šifre može se odmah početi koristiti neki dApp, ili slati i primiti kriptovalute.

⁵¹ <https://blog.hellobloom.io/the-most-lucrative-eth-scams-top-to-bottom-5678bd056fe4>

⁵² <https://www.coinbase.com/>

⁵³ <https://www.bitstamp.com/>

⁵⁴ <https://makerdao.com/>

⁵⁵ <https://www.trusttoken.com/trueusd/>

⁵⁶ <https://metamask.io/>

9. Zaključak

Ethereum je izuzetno bitan projekt za razvoj kriptovaluta i blockchain tehnologije. Bitcoin je prvi projekt koji je popularizirao blockchain, no on je usko fokusiran na financijske transakcije. Ethereum je prva decentralizirana platforma zasnovana na blockchainu koja je omogućila izradu naprednih pametnih ugovora i aplikacija. Posebno je bitno da se na Ethereumu relativno brzo pojavilo i nekoliko vrlo popularnih primjena ove tehnologije, primarno ICOove koji su novi i revolucionarni način prikupljanja sredstava za pokretanje blockchain projekata. Osim ICOova, potencijalne primjene decentraliziranih aplikacija zasnovanih na blockchainu uključuju i druge financijske usluge, igre te online kockanje.

Unatoč snažnoj konkurenciji koja se razvila u 2017. i 2018., i uključuje 'žive' projekte kao što je EOS te neke nadolazeće kao što su Cardano i Dfinity, Ethereum je još uvijek daleko najaktivnija platforma za izradu decentraliziranih aplikacija.

Ipak, Ethereum u budućnosti čekaju mnogi izazovi. Mnoga predložena rješenja za probleme skalabilnosti i relativne centraliziranosti nedovoljno su testirana i mogu teoretski sa sobom donijeti nove, dosad neviđene probleme. Također, potreba za većom skalabilnošću je snažna već danas, a Ethereumu će trebati barem pola godine da počne implementirati potencijalna rješenja. Nije nezamislivo da neki od konkurenata, koji svi u određenoj mjeri pate od istih problema, rješenja implementira brže i/ili bolje i taj način Ethereumu uzme primat.

U svakom slučaju, Ethereum je pokazao da postoji stvarni interes za decentralizirane aplikacije zasnovane na blockchainu, zbog njihove transparentnosti, otpornosti na cenzuru te mogućnosti da se određeni kompleksni procesi iz stvarnog života pretoče u pametne ugovore koji teoretski ne dopuštaju pogreške. Projekt je star svega tri godine, i već se oko njega razvio čitav ekosustav programera, korisnika i startup kompanija. Budućnost će pokazati je li interes opravdan, no u ovom trenutku potencijal je velik.

10. Literatura

1. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. URL: <https://bitcoin.org/bitcoin.pdf> [12.10.2018].
2. Sedgwick, Kai. A brief History of Hidden Messages in the Bitcoin Blockchain, 2018. URL: <https://news.bitcoin.com/a-brief-history-of-hidden-messages-in-the-bitcoin-blockchain/> [14.11.2018].
3. Namecoin. URL: <https://namecoin.org/> [20.11.2018].
4. Buterin, Vitalik. Ethereum White Paper, 2013. Originalni dokument je uklonjen; kopija preuzeta sa <https://whitepaperdatabase.com/ethereum-eth-whitepaper/> [12.10.2018].
5. Wood, Gavin. Ethereum: A Secure Decentralised Generalised Transaction Ledger. URL: <https://gavwood.com/paper.pdf> [20.11.2018].
6. Wood, Gavin. Who I Am. URL: <http://gavwood.com/> [20.11.2018].
7. Go-Ethereum, Contributions to master, excluding merge commits. URL: <https://github.com/ethereum/go-ethereum/graphs/contributors> [20.11.2018].
8. Strajnar, Fran. After three years of Ethereum how close are we to Web 3.0? URL: <https://bravenewcoin.com/insights/after-three-years-of-ethereum-how-close-are-we-to-web-3-0> [20.11.2018].
9. Polkadot. URL: <https://polkadot.network/> [20.11.2018].
10. Cardano. URL: <https://www.cardano.org/en/home/> [20.11.2018].
11. ConsenSys. URL: <https://consensys.net/> [20.11.2018].
12. Buterin, Vitalik. Medium profil. URL: <https://medium.com/@VitalikButerin> [12.10.2018].
13. Buterin, Vitalik. Ether Sale: A Statistical Overview, 2014. URL: <https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview/>
14. ERC: Token standard #20. URL: <https://github.com/ethereum/eips/issues/20> [20.11.2018].

15. Eidoo, ERC20 Tokens list. URL: <https://eidoo.io/erc20-tokens-list/> [20.11.2018].
16. Szabo, Nick, Smart Contracts: Building Blocks for Digital Markets, 1996. URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
17. Bitcoin Wiki. Script. URL: <https://en.bitcoin.it/wiki/Script> [20.11.2018].
18. CryptoKitties. URL: <https://www.cryptokitties.co/> [20.11.2018].
19. BitInfoCharts. URL: <https://bitinfocharts.com> [20.11.2018].
20. State of the Dapps. URL: <https://www.stateofthedapps.com/> [20.11.2018].
21. CoinMarketCap. Ethereum. URL: <https://coinmarketcap.com/currencies/ethereum/> [20.11.2018].
22. Emin Gün Sirer. Twitter, 2017. URL: <https://twitter.com/el33th4xor/status/870327595434463232>
23. Coindesk ICO Tracker. URL: <https://www.coindesk.com/ico-tracker> [20.11.2018].
24. Fields, J. Brent. Order Instituting cease-and-desist proceedings pursuant to section 8A of the Securities Act of 1933, making findings, and imposing penalties and a cease-and-desist order. URL: <https://www.sec.gov/litigation/admin/2018/33-10575.pdf> [20.11.2018].
25. Falkon, Samuel. The Story of the DAO—Its History and Consequences, 2017. Medium. URL: <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>
26. Pearson, Jordan. The Ethereum Hard Fork Spawned a Shaky Rebellion, 2016. Motherboard. URL: https://motherboard.vice.com/en_us/article/z43qb4/the-ethereum-hard-fork-spawned-a-shaky-rebellion-ethereum-classic-etc-eth
27. Ethereum Stack Exchange. Please provide a summary of the Ethereum hard forks. URL: <https://ethereum.stackexchange.com/questions/13014/please-provide-a-summary-of-the-ethereum-hard-forks> [20.11.2018].
28. Vermuelen, Jan. VisaNet – handling 100,000 transactions per minute, 2016. MyBroadBand. URL: <https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html>

29. BBC. CryptoKitties craze slows down transactions on Ethereum, 2017. URL: <https://www.bbc.com/news/technology-42237162>
30. Github. Proof of Stake FAQs. URL: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs> [20.11.2018].
31. Ethereum Stack Exchange. Can Proof of Stake (PoS) improve the number of Transactions per Second? URL: <https://ethereum.stackexchange.com/questions/5708/can-proof-of-stake-pos-improve-the-number-of-transactions-per-second> [20.11.2018].
32. GitHub. Sharding FAQs. URL: <https://github.com/ethereum/wiki/wiki/Sharding-FAQs> [20.11.2018].
33. Konstantopoulos, Georgios. Million-User DApps on Ethereum: An Introduction to Application-Specific Sidechains, 2017. Medium. URL: <https://medium.com/loom-network/million-user-dapps-on-ethereum-an-introduction-to-application-specific-sidechains-c0fdc288c5e5>
34. Buterin, Vitalik. Poon, Joseph. Plasma: Scalable Autonomous Smart Contracts, 2017. URL: <https://plasma.io/plasma.pdf>
35. Etherchain. Top Miners over the last 24h. URL: <https://www.etherchain.org/charts/topMiners> [20.11.2018].
36. Decter, Shawn. Ethereum Roadmap Update [2018]: Casper & Sharding Release Date, 2018. URL: <https://www.mangoresearch.co/ethereum-roadmap-update/>
37. GitHub. EOS.IO Technical White Paper v2. URL: <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md> [20.11.2018].
38. Zhang, Kevin. The State of Plasma: #1. URL: <https://media.consensus.net/the-state-of-plasma-1-6b48c1e4b295> [18.12.2018].
39. Ethernodes. URL: <https://www.ethernodes.org/> [20.11.2018].
40. NEO. How To Become A NEO Consensus Node, 2018. Medium. URL: <https://medium.com/neo-smart-economy/how-to-become-a-consensus-node-27e5317722e6>
41. Particl. BTC Studios. Yes, Bitcoin Can Do Smart Contracts and Particl Demonstrates How. URL: <https://bitcoinmagazine.com/articles/yes-bitcoin-can-do-smart-contracts-and-particl-demonstrates-how/> [20.11.2018].

42. Ethereum Stack Exchange. What is meant by the term “gas”? URL: <https://ethereum.stackexchange.com/questions/3/what-is-meant-by-the-term-gas> [18.12.2018].
43. CoinMarketCap, Ethereum. URL: <https://coinmarketcap.com/currencies/ethereum/> [18.12.2018].
44. EtherScan. URL: <http://etherscan.io/> [18.12.2018].
45. Arvanaghi, Brandon. The most lucrative ETH scams, top-to-bottom. URL: <https://blog.hellobloom.io/the-most-lucrative-eth-scams-top-to-bottom-5678bd056fe4> [18.12.2018].
46. Coinbase. URL: <https://www.coinbase.com/> [18.12.2018].
47. BitStamp. URL: <https://www.bitstamp.com/> [18.12.2018].
48. MakerDAO. URL: <https://makerdao.com/> [18.12.2018].
49. TrueUSD. URL: <https://www.trusttoken.com/trueusd/> [18.12.2018].
50. MetaMask. URL: <https://metamask.io/> [18.12.2018].