Ethereum

- Sajt: https://www.ethereum.org
- Vitalik Buterin, 2013. – Ethereum White Paper (https://github.com/ethereum/wiki/wiki/White-Paper), razvoj sistema krenuo 2014, mreža počela sa radom 30.7.2015.
- "Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments (colored coins), the ownership of an underlying physical device (smart property), non-fungible assets such as domain names (Namecoin), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules (smart contracts) or even blockchain-based decentralized autonomous organizations (DAOs). What **Ethereum intends to provide** is a **blockchain with a built-in fully fledged Turing-complete programming language** that can be **used to create "contracts"** that can be **used to encode arbitrary state transition functions**, **allowing users to create any of the systems described above**, as well as many others that we have not yet imagined, **simply by writing up the logic in a few lines of code**."

- Zamišljen kao "**The World Computer**" – blokčejn sistem koncipiran kako bi podržao rad decentralizovanih aplikacija (engl. *decentralized applications – dapps*)
- Dokumentacija: https://ethereum.org/en/developers/docs/
- Nativna valuta – **etar** (engl. *ether*) ETH (Ξ), najmanja jedinica 1 Wei – 10^{-18} ETH
- Koristi virtuelnu mašinu kao okruženje za izvršavanje (engl. *runtime environment*) programa napisanih u **Tjuring-kompletnom programskom jeziku** – **Ethereum Virtual Machine** (EVM), bajtkod u jeziku niskog nivoa zasnovan na radu sa 256-bitnim registarskim stekom u režimu izolovanom od ostatka fajlova i procesa na datom čvoru (engl. *sandbox*)
- **Tjuring-kompletan programski jezik za opis transakcija**
  - Solidity, LLC, Serpent, Vyper, …
  - u suštini namenski jezici (engl. *domain specific languages* – DSLs)

- Dva tipa **naloga** – korisnički nalozi (engl. *user* accounts) i ugovori (engl. *contracts*), oba imaju odgovarajući ETH balans, mogu da šalju ETH, da pozivaju javne funkcije ugovora, da kreiraju nove ugovore, identifikuju se putem **adresa**
  - samo korisnički nalozi mogu da kreiraju transakcije, potpisivanje se bazira na ECDSA
  - samo ugovori imaju pridruženi kod (skup funkcija i deklaracija promenljivih) i memoriju (vrednosti promenljivih u bilo kom trenutku)
- **Ethereum adresa** – prefiks 0x praćen sa 20 bajtova najmanje težine Keccak-256 heša ECDSA javnog ključa tj. 40 heksadecimalnih cifara (npr. 0x5994f5ea0ba39484ce839613fffba742795792af)
- Koncept **gasa** – količina ETH koju pošiljalac transakcije plaća rudaru koji uključuje odgovarajuću transakciju u blok, obično se izražava u Gwei (10^{-9} ETH)
  - svaki tip operacije ima tačno definisanu cenu u gasu, odgovara količini resursa (izračunavanja i memorije) neophodnih za njenu realizaciju
  - prilikom kreiranja transakcije specificiraju se gas limit i cena gasa, pošiljalac odmah na početku kupuje gas limit, eventualni "kusur" se vraća nakon izvršenja transakcije
- **Ethereum 2.0** (Eth2) 2022. – „The Beacon Chain" zasnovan na PoS pokrenut 1.12.2020.
- Prelazak na **proof-of-stake** konsenzus algoritam septembra 2022.

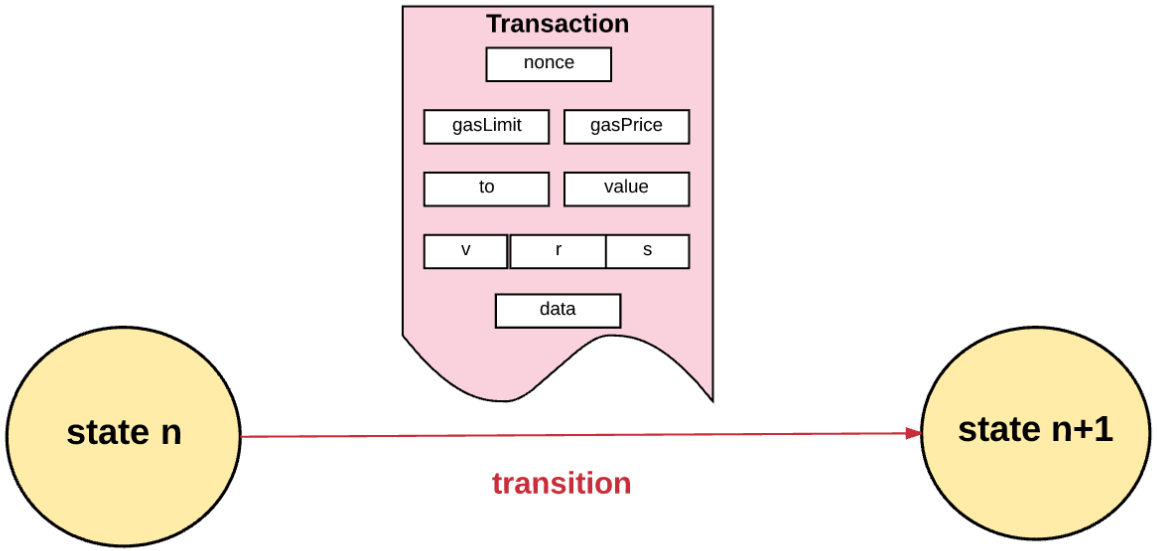
	Bitcoin	Ethereum
Creator(s)	Satoshi Nakamoto	Vitalik Buterin, Charles Hoskinson, Gavin Wood, Joseph Lubin, and Anthony Di Iorio
Launch Date	January 2009	July 2015
Currency vs. Platform	A credible alternative to traditional fiat currencies (medium of exchange, potential store of value)	A platform to run programmatic contracts and applications via Ether
Consensus Algorithm	Proof-of-Work (PoW)	Proof-of-Stake (PoS)
Block Time	10 minutes on average	12 seconds on average
Transaction Throughput	7 transactions per second (TPS)	14 transactions per second (TPS)
Supply	Finite supply-capped at 21 million BTC	Infinite supply
Scalability Solutions	SegWit, Lightning Network	Ethereum 2.0, Sharding, Plasma

Izvor: https://www.vaneck.com/us/en/blogs/digital-assets/bitcoin-vs-ethereum/

ethereum

- **Principi** projektovanja **Ethereum blokčejna**:
  - **jednostavnost**, **univerzalnost**, **modularnost**, **agilnost**
- **Nedostaci Ethereum blokčejna:**
  - **mali propusni opseg mreže**, **pametni ugovori** pisani u **DSL-u**, **koncept gasa** – L2 rešenja

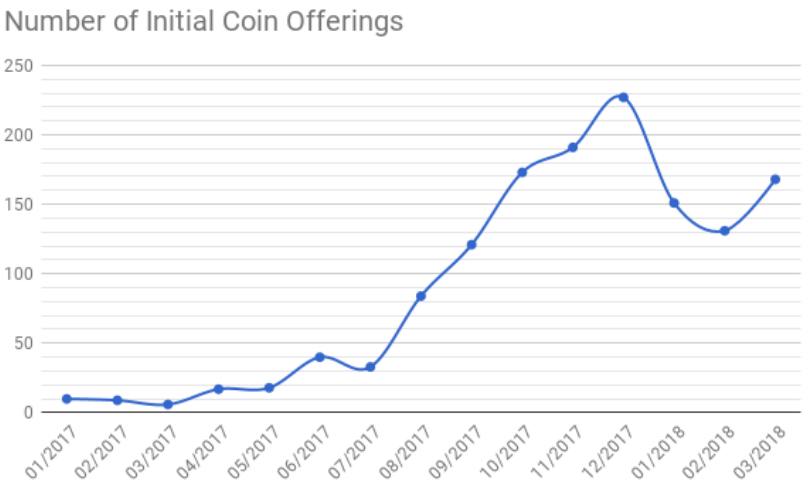
Vitalik Buterin (r. 1994)

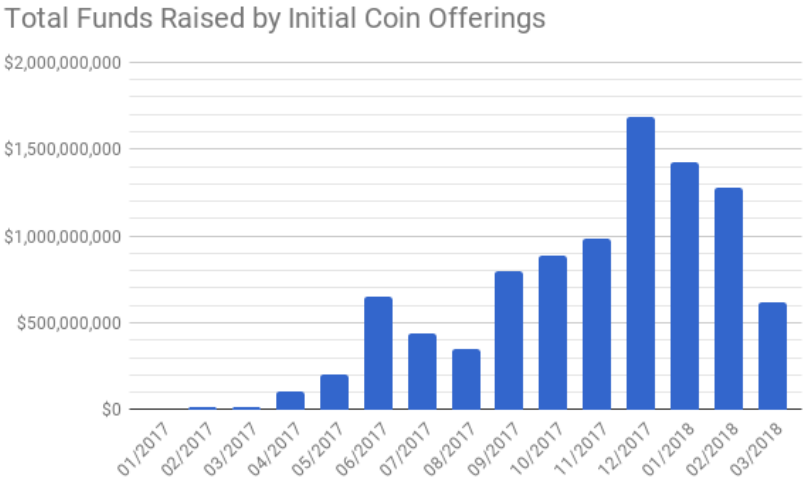


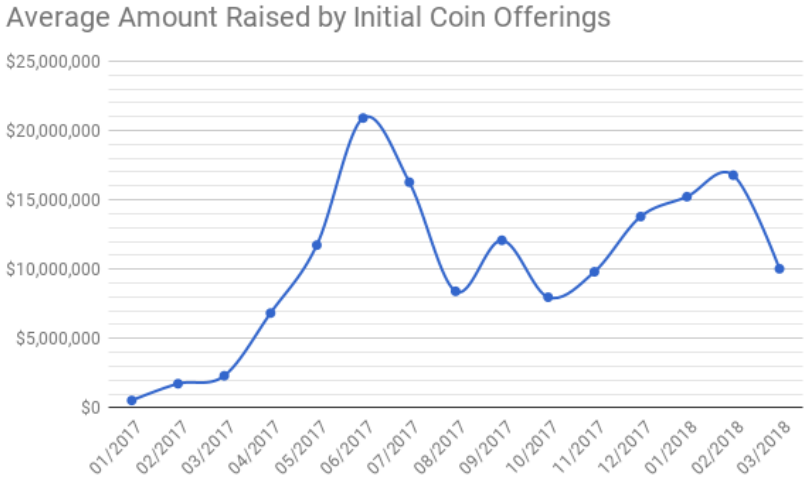
Izvor: https://medium.com/@reyesale/ethereum-the-world-computer-fb7b58948280

- Koncept **pametnih ugovora** (engl. *smart contracts*) – potiče od radova Nika Saboa (Nick Szabo) iz 1994. "Smart Contracts: Building Blocks for Digital Markets"
  (https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html)
  - **programski kod** koji **dovodi do promene stanja sistema** kada se **određeni uslovi ispune**, primer aparat za slatkiše (engl. *vending machine*): https://ethereum.org/en/developers/docs/smart-contracts/
- Koncept **tokena**
  - **razmenljivi** (engl. *fungible*) – **ERC20** (Ethereum Request for Comments 20)
  - **nerazmenljivi** (engl. *non-fungible*) **(NFT) – ERC721** – jedinstveni i nedeljivi
- Koncept **inicijalne ponude novčića** (engl. *initial coin offering – ICO*)
  - pametni ugovori koji se izvršavaju na Ethereum blokčejnu, jedna realizacija koncepta grupnog investiranja (engl. *crowdfunding*)
  - novija varijanta je STO (engl. *Security Token Offering*) koja uzima u obzir regulatorne zahteve, inicijalno tokeni dostupni samo akreditovanim investitorima

ICO statistika 2017-2018



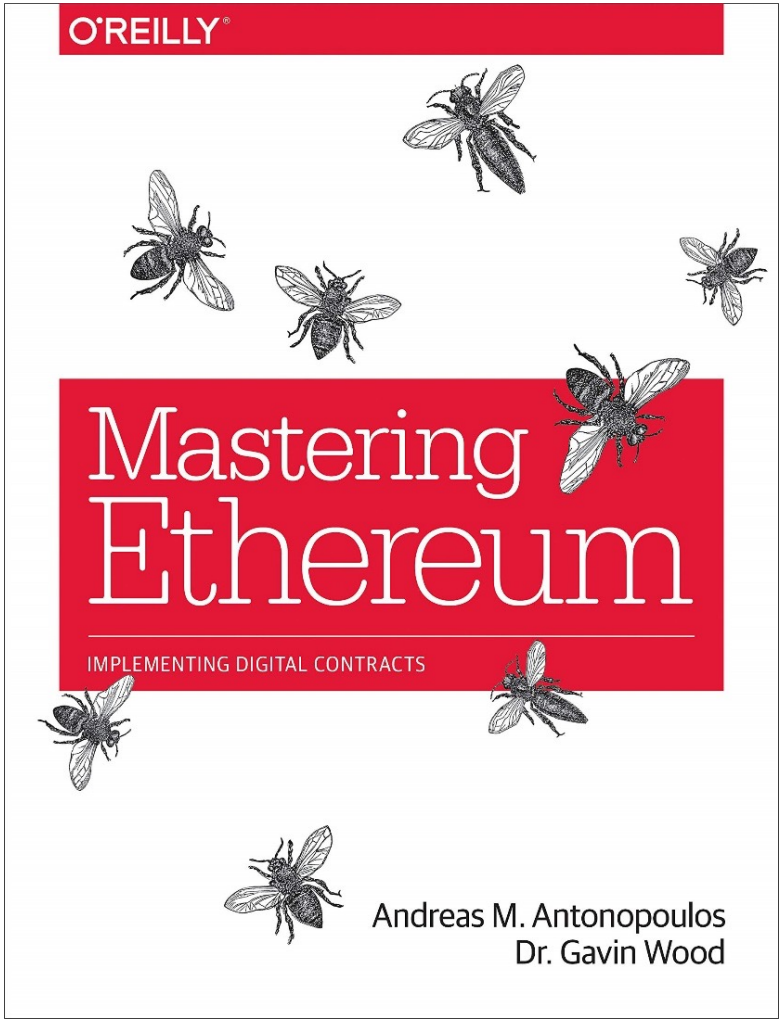




Izvor: https://medium.com/@argongroup/ico-market-report-april-2018-3857cbe729c3

- **Decentralizovane aplikacije** (Dapps)
  - Primeri: CryptoKitties, EtherTweet, Etheria, domaći LemonMail
- **Decentralizovane autonomne organizacije** (DAO) – koncept nastao 2016, inicijalno dobio 150 miliona USD, od čega je 50 milina USD potom ukradeno
- **Decentralizovane finansije** (engl. *Decentralized Finance – DeFi*) – zamena za tradicionalne banke, berze i brokerske kuće,
  - obično se DeFi aplikacijama pristupa preko Web3.0 proširenja pretraživača ili aplikacija, kao što je MetaMask (https://metamask.io/), koji omogućavaju korisnicima interakciju sa Ethereum blokčejnom direktno iz pretraživača
  - Primeri: Uniswap (https://uniswap.org/), MakerDAO (https://makerdao.com/en/), Compound (https://compound.finance/) , …

Literatura – Ethereum



https://github.com/ethereumbook/ethereumbook