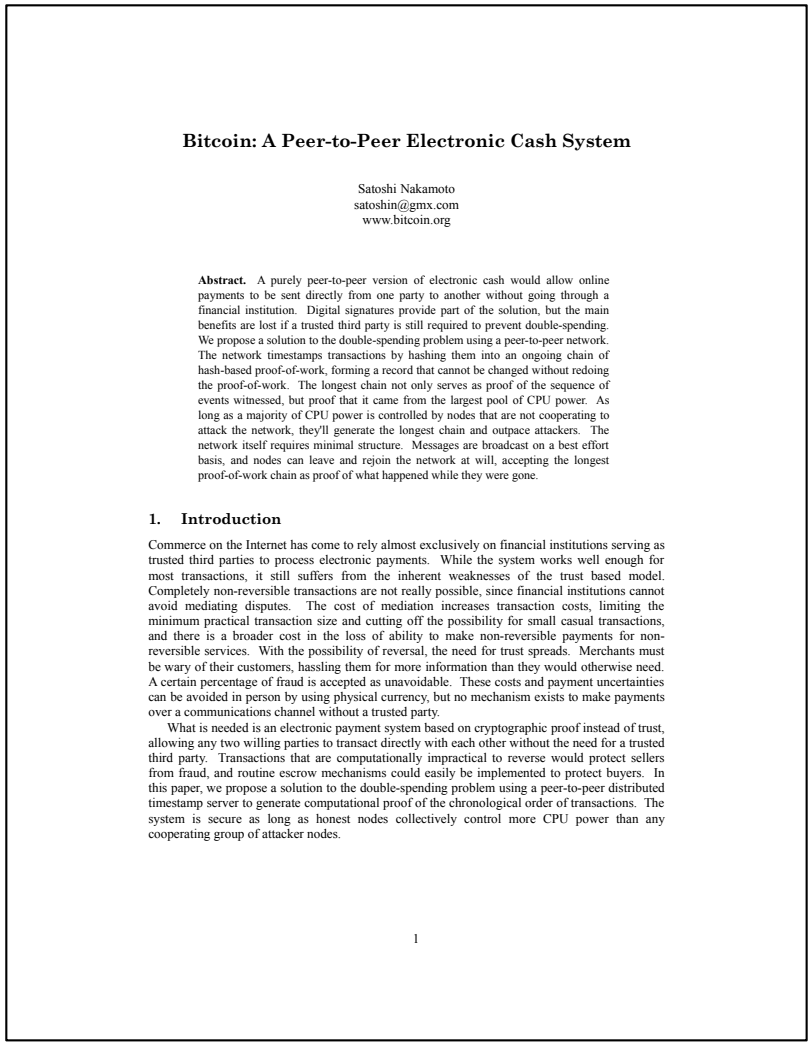
Primeri blokčejn tehnologija

Bitcoin

Bitcoin rad



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

https://bitcoin.org/bitcoin.pdf

Nakamoto o Bitcoinu

- Satoshi Nakamoto, 2008:
  - ”A **solution to the double-spending problem** using a **peer-to-peer network**”
  - “An **electronic payment system based on cryptographic proof instead of trust**, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”
  - “We propose a **solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions**. The system is **secure as long as honest nodes collectively control more CPU power** than any cooperating group of attacker nodes.”
  - “We define **an electronic coin as a chain of digital signatures**. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin.“

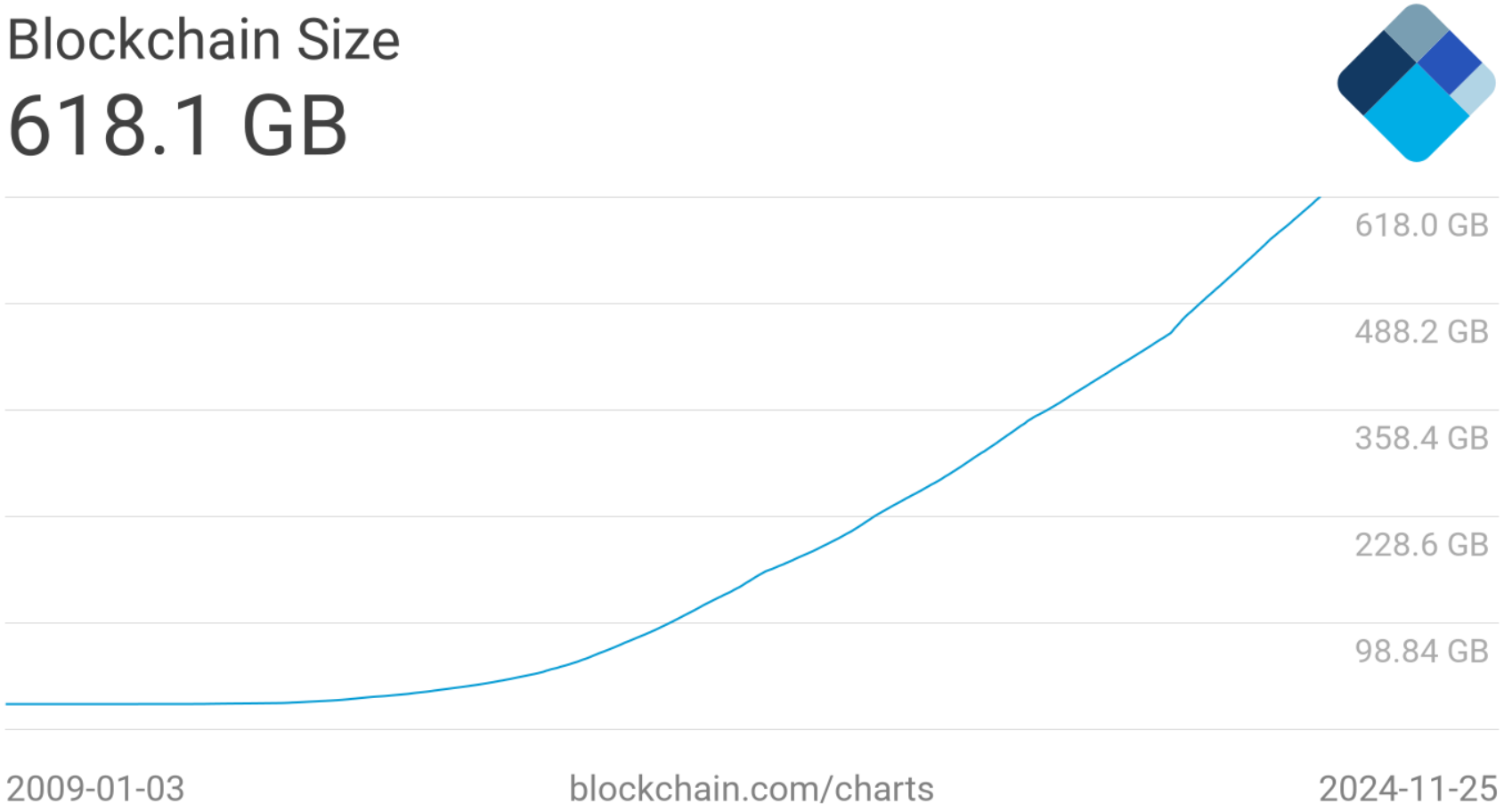
Nakamoto o Bitcoinu

- Satoshi Nakamoto, 2008:
  - ”We have proposed **a system for electronic transactions without relying on trust**. We started with the usual framework of **coins made from digital signatures**, which **provides strong control of ownership**, but is **incomplete without a way to prevent double-spending**. To solve this, we proposed a **peer-to-peer network using proof-of-work to record a public history of transactions** that **quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power**. The network is robust in its **unstructured simplicity**. Nodes work all at once with **little coordination**. They do not need to be identified, since **messages** are not routed to any particular place and only need to be delivered on a **best effort basis**. **Nodes** can **leave** and **rejoin** the network **at will**, **accepting the proof-of-work chain as proof of what happened while they were gone**. They **vote with their CPU power**, expressing their **acceptance of valid blocks by working on extending them** and **rejecting invalid blocks by refusing to work on them**. Any **needed rules and incentives can be enforced with this consensus mechanism**.“

Vrednost Bitcoina (BTC) 2013–2024

Izvor: https://coinranking.com/coin/bitcoin-btc

Veličina Bitcoin blokčejna



Izvor: https://www.blockchain.com/charts/blocks-size?timespan=all

Osnovi Bitcoina

Izvor: https://www.youtube.com/watch?v=l9jOJk30eQs

Osnovi Bitcoina

- "P2P elektronski keš sistem", pokrenut januara 2009. – Bitcoin Core implementacija (C++), verziju 0.1 objavio Satoshi Nakamoto 9.1.2009.
- Nova vrsta valute (engl. *currency*) – **kriptovaluta** (engl. ***cryptocurrency***)
- Sve virtuelne valute moraju odgovoriti na sledeće izazove:
  - **stvaranje virtuelnog novčića** (engl. *coin*), tj. novčanice (engl. *note*)
    - Kako se uopšte stvara novčić?
    - Kako se sprečava inflacija? (Šta sprečava bilo kog da stvori mnoštvo novčića?)
  - **validacija**
    - Da li je novčić ispravan? (proof-of-work)
    - Kako sprečiti dvostruku potrošnju novčića?
- Bitcoin je zasnovan na pristupu sa minimumom infrastrukture
  - zasniva se na **dokazu** umesto **poverenja**, nema centralne banke ili kliring kuće (engl. *clearing house*)
  - mreža danas podržava do 10 transakcija u sekundi
  - generisaće se ukupno 21 milion bitcoina (BTC) do 2140.

Onlajn transakcije i Bitcoin

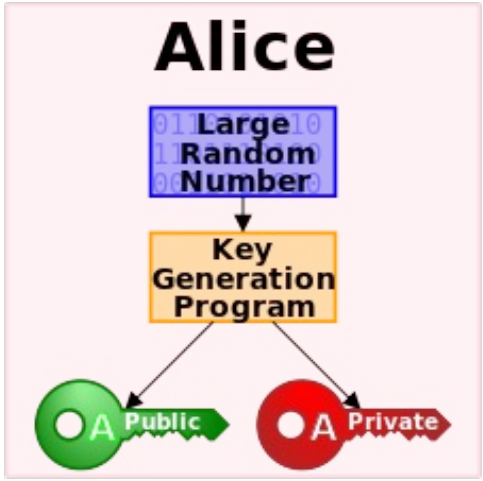
- **Bitcoin** se zasniva se na **dokazu umesto poverenja**
  - danas se onlajn transakcije dominantno zasnivaju na **stranama od poverenja** (engl. *trusted parties*), kao što su npr. VISA ili MasterCard, koje preuzimaju određeni rizik, rešavaju prevare i zbog toga dobijaju određenu proviziju na transakcije
- Kupac (engl. *buyer*) i prodavac (engl. *seller*) imaju zaštitu prilikom realizacije onlajn transakcija
  - situacija kada kupac plati, ali prodavac ne isporuči rešava se primenom escrow-a (zaštita kupca)
  - situacija kada prodavac isporuči, kupac plati, ali kupac potom podnese prigovor rešava se tako što VISA/MasterCard izvrše refundaciju; plaćanje se poništava. Ili se plaćaju penali od strane prodavca i/ili VISA/MasterCard naplaćuju veću proviziju kako bi se nosili sa ovakvim slučajevima
  - **Bitcoin eliminiše potrebu za posrednikom od poverenja** (engl. *trusted middleman*) **tako što može direktno pokazati kriptografski dokaz da je novac prenesen**

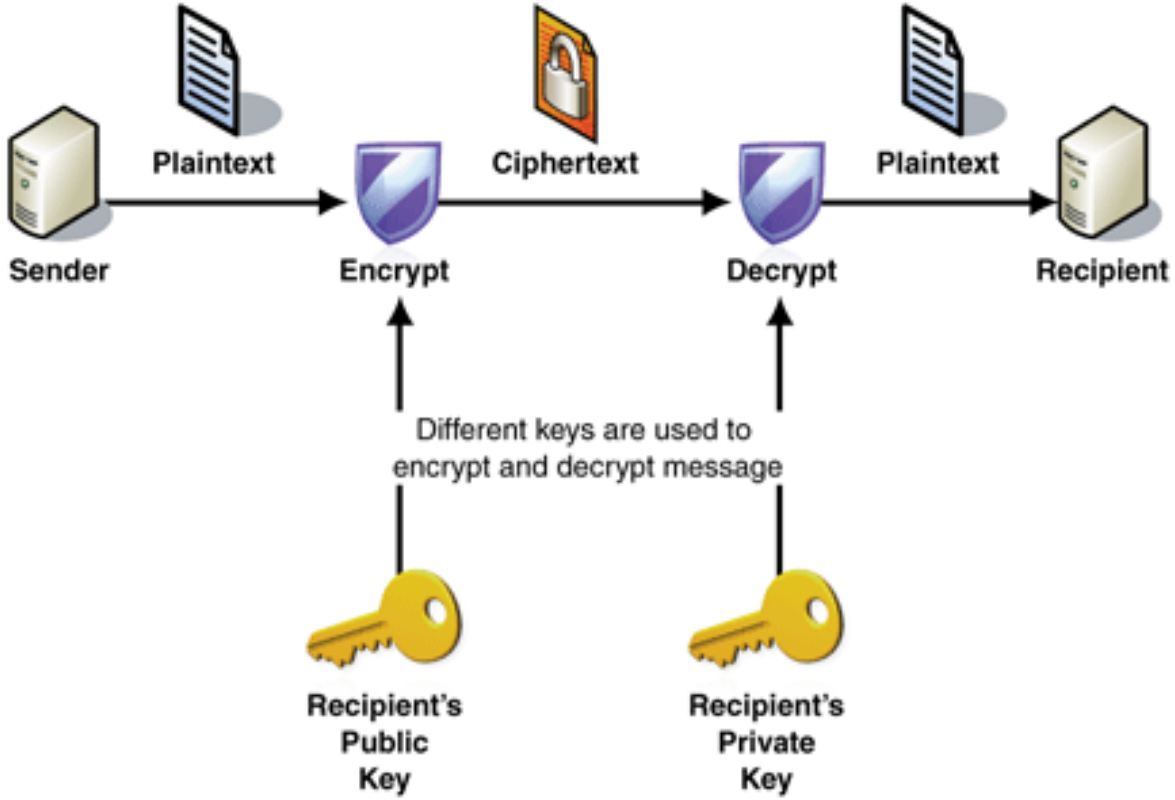
Bitcoin rešenje za bezbednu komunikaciju

- **Autentifikacija** se rešava **kriptosistemom sa javnim ključem putem digitalnih potpisa** (engl. *digital signatures*)
  - Da li plaćam pravoj osobi? Da li se neko ne predstavlja lažno?
- **Integritet** se rešava putem **digitalnih potpisa** i **kriptografskih heševa**
  - Da li je novčić dva puta potrošen?
  - Da li napadač može poništiti ili izmeniti transakcije?
- **Dostupnost** (engl. *availability*) kroz **broadcast poruke P2P mreži**
  - Da li mogu izvršiti transakcije kad god želim?
- **Poverljivost** (engl. *confidentiality*) ne postoji, već samo **pseudonimnost** (engl. *pseudonymity*)
  - Da li su transakcije poverljive ili samo anonimne?
  - U kontekstu Bitcoina prava poverljivost nije preterano relevantna, ali je privatnost (engl. *privacy*) uvek važna

Asimetrični kriptosistem za šifrovanje

- **Asimetrični kriptosistem** (sistem sa javnim ključem)
  - Jedinstveni par ključeva: **javni i privatni ključ** – služe za šifrovanje, odnosno dešifrovanje





Izvor: http://ina.kaist.ac.kr/ee324/F13/lectures/24-bitcoin.pptx

Primer: RSA asimetrični kriptosistem

- **Rivest-Shamir-Adelman kriptosistem** razvijen je 1977.
  - Rivest, R., Shamir, A., Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM*. 21 (2): 120–126, (http://people.csail.mit.edu/rivest/Rsapaper.pdf)
- **RSA generator ključeva** (engl. *keygen*)
  - biraju se dva različita prosta broja p i q (neka je $n = pq$)
  - računa se $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$, gde je ϕ Ojlerova totijent funkcija
    - $\phi(n)$: broj celih brojeva k u opsegu $1 \leq k \leq n$ za koje je $\gcd(n, k) = 1$, tj. koji su uzajamno prosti (nemaju zajedničkih faktora)
  - bira se uzajmno prosti broj sa $\phi(n)$, e, tako da je $1 < e < \phi(n)$, tj. $\gcd(e, \phi(n)) = 1$
  - traži se d gde je $d \cdot e \equiv 1 \pmod{\phi(n)}$
- **Javni ključ** je (n, e)
- **Privatni ključ** je (n, d)

Primer: RSA asimetrični kriptosistem

- **Javni ključ** (*n*, e) i **privatni ključ** (*n*, *d*)
  - **šifrovanje**: izračunava se šifrat C = m^e (**mod** *N*) (javni ključ)
  - **dešifrovanje**: rekonstruiše se m = C^d (**mod** *N*) (privatni ključ)

$$m^{ed} = m^{(ed-1)}m = m^{h(p-1)(q-1)}m = (m^{p-1})^{h(q-1)}m \equiv 1^{h(q-1)}m \equiv m \pmod{p},$$

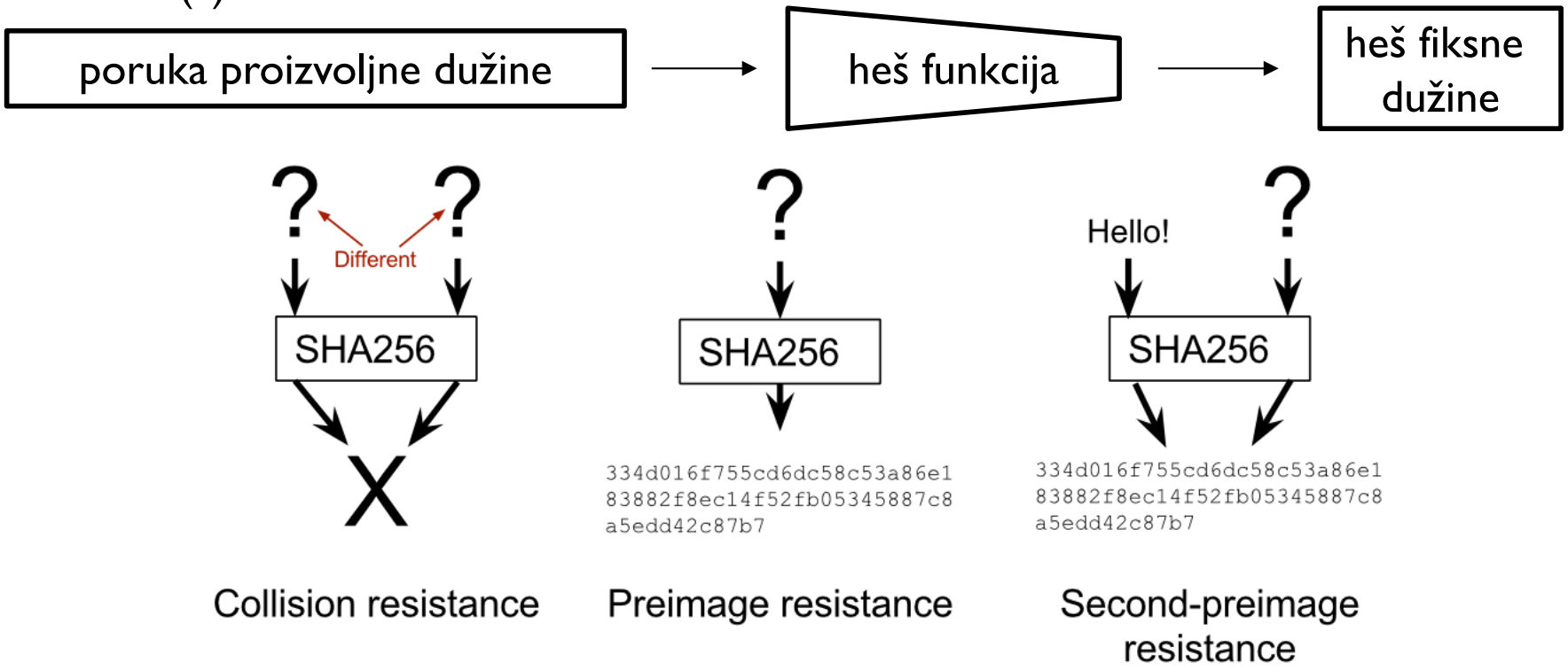
$ed \equiv 1 \pmod{(p-1)(q-1)}$.

Fermaova mala teorema

- **Princip rada**:
  - problem faktorizacije je složen za izračunavanje (nalazi se u klasi NP), ako je dato *n* teško je izračunati vrednosti za *p* i *q*
  - izračunavanje *m* je teško ako je poznat javni ključ (*n*, e) i šifrat $C \equiv m^e$ (**mod** *N*)

Kriptografske heš funkcije

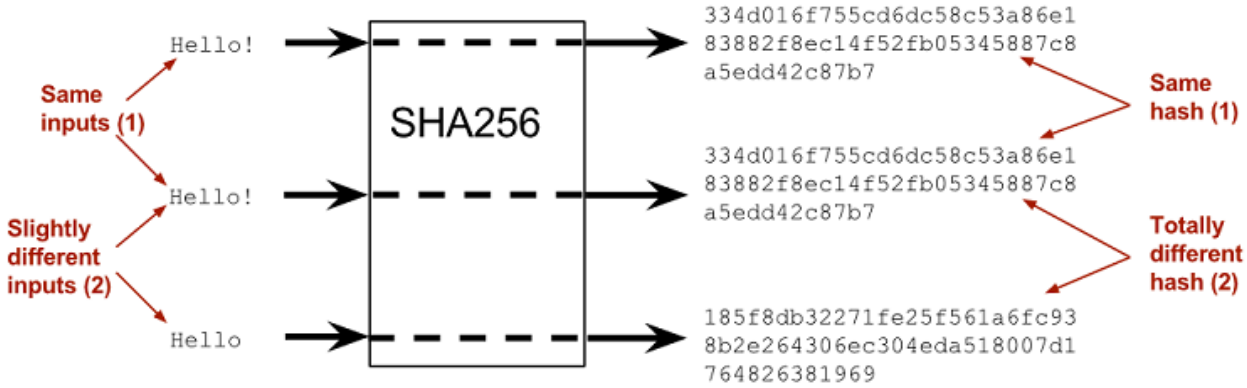
- **Osobine kriptografskih heš funkcija**:
  - **Konzistentnost**: $h = H(x)$ uvek daje isti rezultat
  - **Jednosmernost**: ako je dato y, teško je pronaći x tako da je $H(x) = y$
  - **Otpornost na kolizije**: ako je dat $H(w) = z$, teško je pronaći x tako da je $H(x) = z$



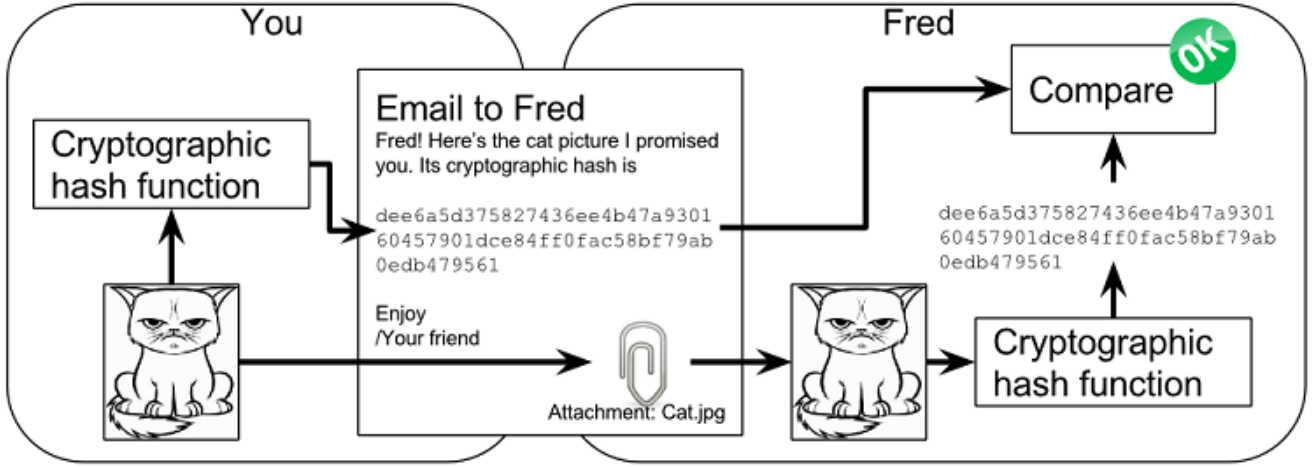
Izvor: https://freecontent.manning.com/cryptographic-hashes-and-bitcoin/

Kriptografske heš funkcije

- Najmanja promena na ulazu dovodi do velike promene u vrednosti heša:



- Primena kriptografskih heš funkcija za proveru **integriteta podataka:**



Izvor: https://freecontent.manning.com/cryptographic-hashes-and-bitcoin/

Bitcoin adrese

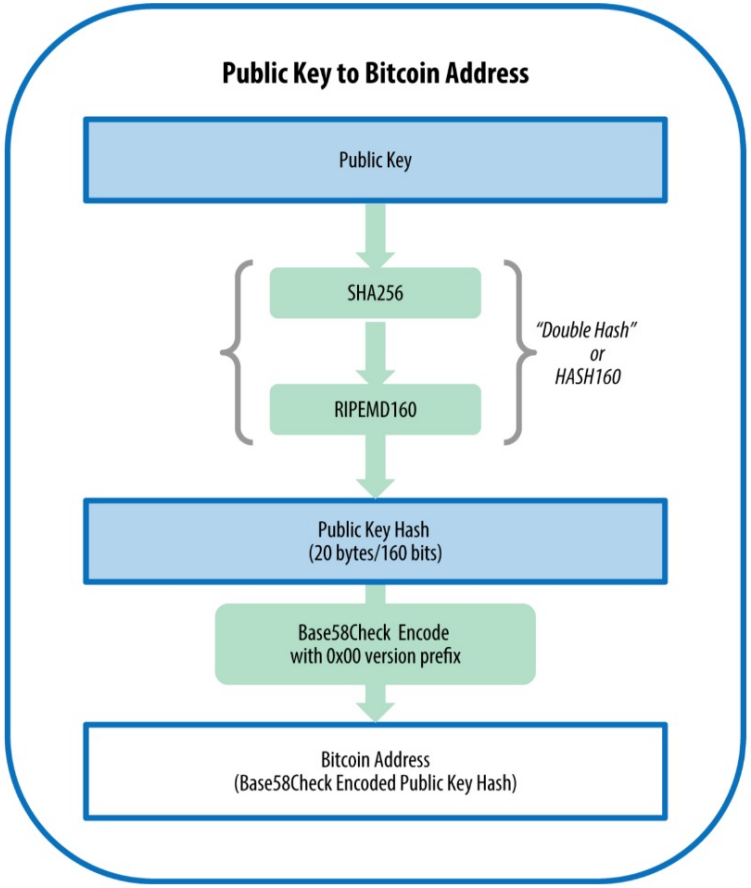
- **Bitcoin adresa** je string sastavljen od cifara i karaktera koji se može podeliti sa bilo kim ko želi da izvrši transakciju
- Bitcoin adresa se **izvodi iz javnog ključa** primenom **jednosmernog kriptografskog heširanja** putem **SHA** (engl. *Secure Hash Algorithm*) **algoritma** – SHA256, kao i RACE Integirty Primitives Evaluation Message Digest (**RIPEMD**) algoritma – RIPEMD160
- Kreće se od javnog ključa *K*, računa se njegov SHA256 heš i potom se traži RIPEMD160 heš rezultata, čime se dobija 160-bitni (20-bajtni) broj:

$$A = RIPEMD160(SHA256(K))$$

- Bitcoin adrese se predstavljaju u **brojnom sistemu sa osnovom 58 - Base58** i **Base58Check**
- Base64: 26 malih slova, 26 velikih slova, 10 cifara, kao i karakteri '+' i '/'
- Base58 je Base64 bez simbola 0 (nula), O (veliko o), l (malo L), I (veliko i), kao i simbola '+' i '/'

Bitcoin adrese

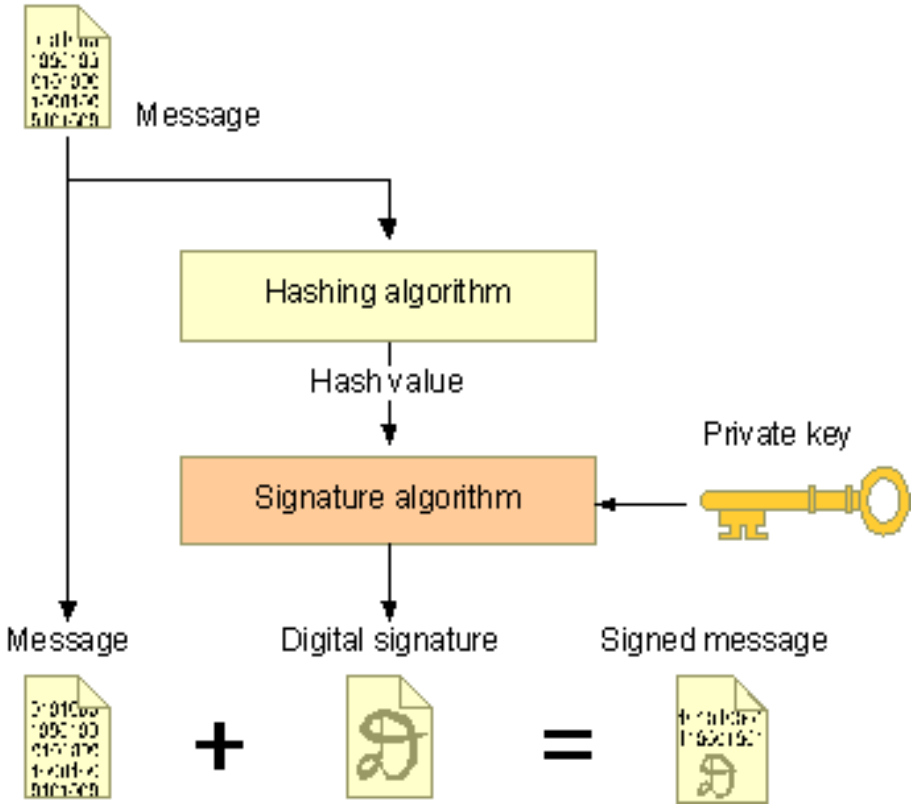
- Kreće se od javnog ključa *K*, računa se njegov SHA256 heš i potom se traži RIPEMD160 heš rezultata, čime se dobija 160-bitni (20-bajtni) broj:



Izvor: Antanopoulos, A., "Mastering Bitcoin", 2nd edition

Digitalni potpis

- **Bitcoin** koristi **ECDSA** (engl. *Elliptic Curve Digital Signature Algorithm*) potpise
- Prvo se kreira sažetak poruke primenom kriptografskog heša
- Potom se sažetak poruke šifruje primenom privatnog ključa



autentifikacija

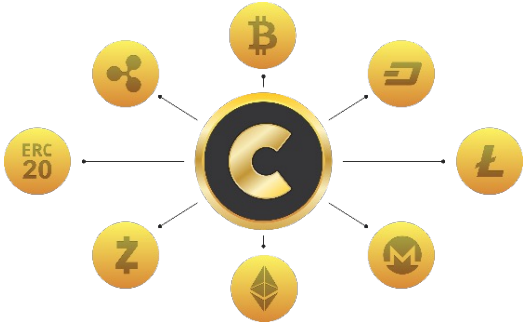
integritet

neoborivost
(engl. *non-repudiation*)

Izvor: http://ina.kaist.ac.kr/ee324/F13/lectures/24-bitcoin.pptx

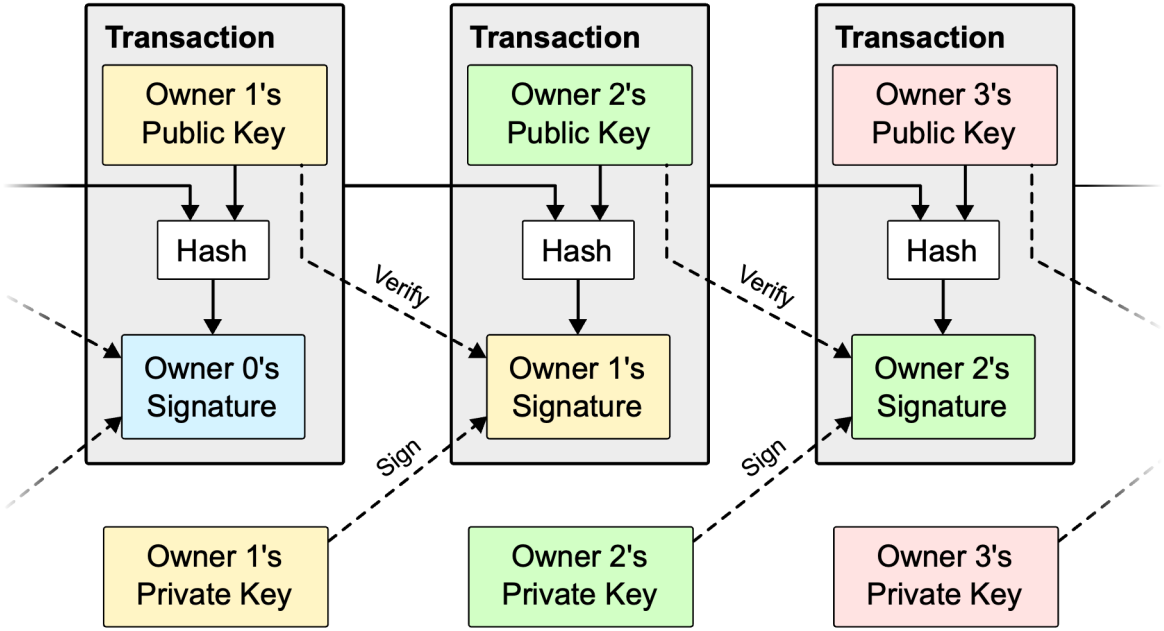
Bitcoin kao kriptovaluta

- Bitcoin rešenje za **validaciju**
  - Da li je novčić ispravan? (proof-of-work)
    - Rešenje: upotreba kriptografskih heševa
  - Kako sprečiti dvostruku potrošnju novčića?
    - Rešenje: broadcast transakcija svim čvorovima u P2P mreži
- Bitcoin rešenje za **stvaranje virtuelnog novčića**
  - Kako se uopšte stvara novčić?
    - Rešenje: pružiti podsticaj (engl. *incentive*) za majnere
  - Kako se sprečava inflacija? (Šta sprečava bilo kog da stvori mnoštvo novčića?)
    - Rešenje: ograničiti brzinu stvaranja bitcoina



Bitcoin

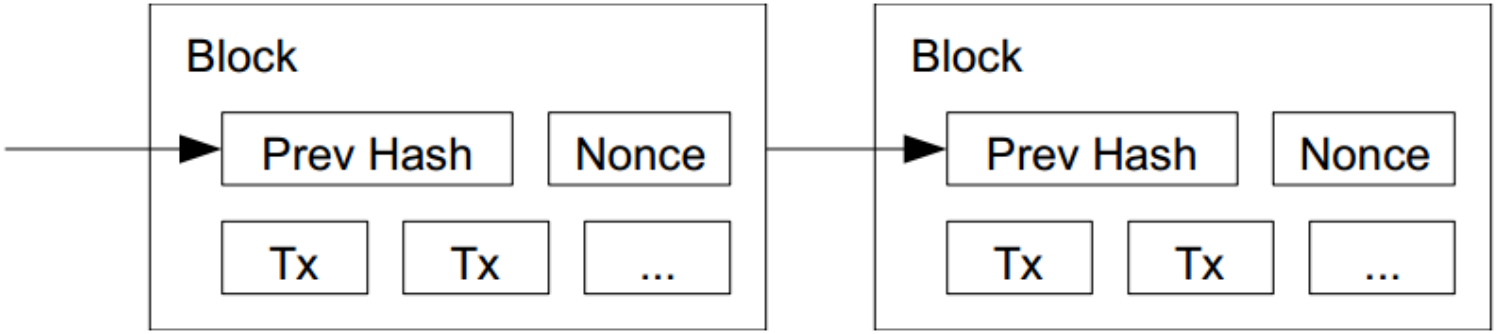
- **Elektronski novčić = lanac digitalnih potpisa**
- Bitcoin transakcija: *potpis*(*prethodna transakcija* + *javni ključ novog vlasnika*)
- Svako može verifikovati da je (*n* - 1) vlasnik izvršio prenos *n*-tom vlasniku
- Svako može ispratiti kompletnu istoriju transakcija



Izvor: https://nakamotoinstitute.org/bitcoin/

Bitcoin konsenzus algoritam

- Konsenzus algoritam **dokaz posla** (engl. **proof of work**)
  - **blok** sadrži **transakcije** koje trebaju biti **validirane** i **prethodnu heš vrednost**
  - bira se **nons** tako da je $H(prethodni\_heš, nons, Tx) < E$, gde je E promenljiva specificirana od strane sistema
  - kod **Hashcash algoritma u Bitcoin**-u prethodni korak se svodi na **pronalaženje heš vrednosti sa određenim brojem nula na početku**
  - neophodan posao **eksponencijalno raste sa zahtevanim brojem nula**
  - **verifikacija je laka, ali je dokaz posla težak**



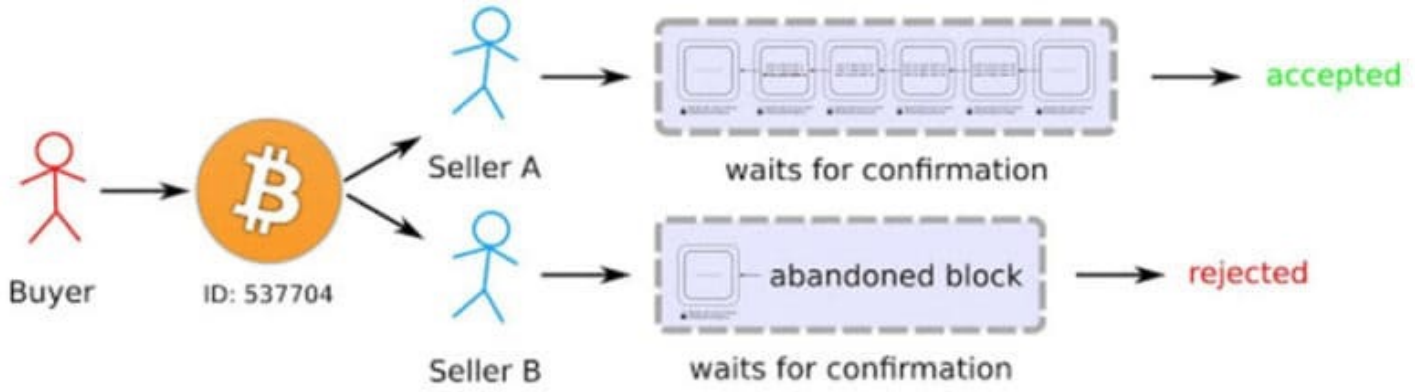
Izvor: http://ina.kaist.ac.kr/ee324/F13/lectures/24-bitcoin.pptx

Bitcoin mreža i algoritam

- Svaki od **čvorova u Bitcoin P2P mreži** izvršava sledeći **algoritam**:
  1. **Nove transakcije** se **broadcast**-uju svim čvorovima
  2. Svaki od čvorova prikuplja **nove transakcije u blok**
  3. Svaki od čvorova radi na **pronalaženju dokaza posla za njegov blok** (zadatak složen za izračunavanje, probabilistički – algoritam zasnovan na lutriji, onaj čvor koji najranije završi će najverovatnije pobediti)
  4. Kada čvor **pronađe dokaz posla**, vrši **broadcast svim ostalim čvorovima** u P2P mreži
  5. **Čvorovi prihvataju blok** samo ako su sve u njemu sadržane **transakcije validne** (vrši se provera digitalnih potpisa) i ako **nisu već potrošene** (vrši se provera svih transakcija)
  6. Čvorovi izražavaju svoje **slaganje** tako što **rade na stvaranju sledećeg bloka** u lancu, koristeći heš prihvaćenog bloka kao vrednost prethodnog heša

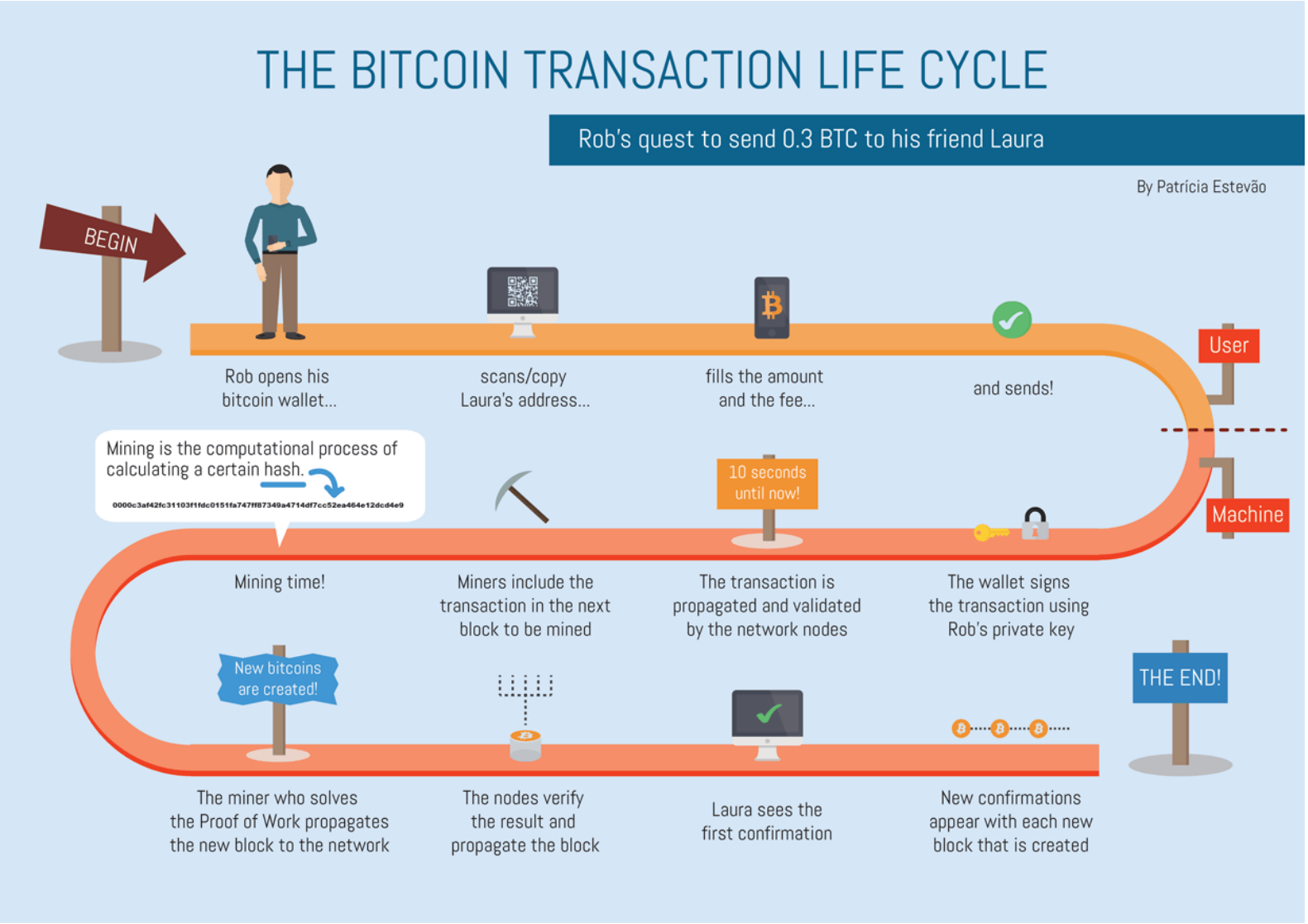
Sprečavanje dvostruke potrošnje

- **Dvostruka potrošnja** u Bitcoin-u se **sprečava** tako što su **svi čvorovi u P2P mreži budu upoznati sa svim transakcijama u mreži**
- **Svaki čvor** (tj. majner) **verifikuje** da je u pitanju **prva potrošnja datog bitcoina od strane platioca**
- Tek **nakon verifikacije, generiše se dokaz posla** i dodaje se u trenutni lanac



Izvor: https://coinsutra.com/bitcoin-double-spending/

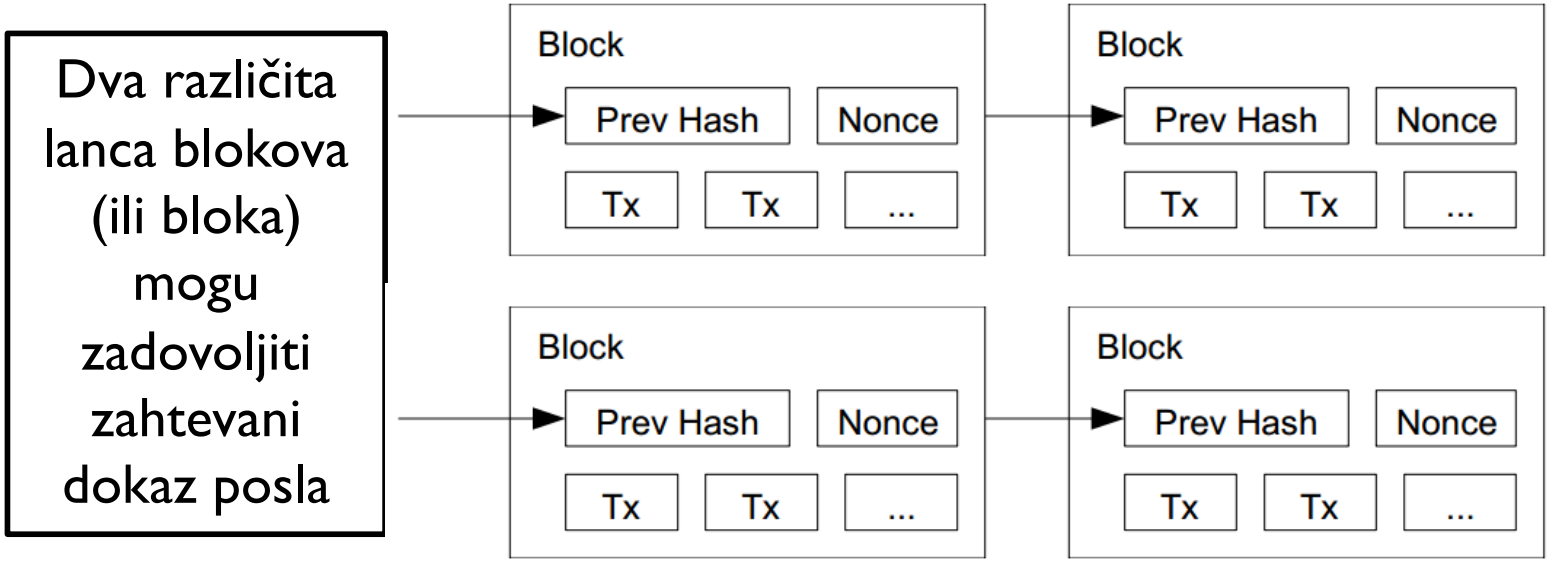
Mehanizam izvršavanja transakcije



Izvor: https://newsandstory.com/story/2312231838062017505 80/how-does-a-bitcoin-transaction-work/

Istovremeno kreiranje blokova

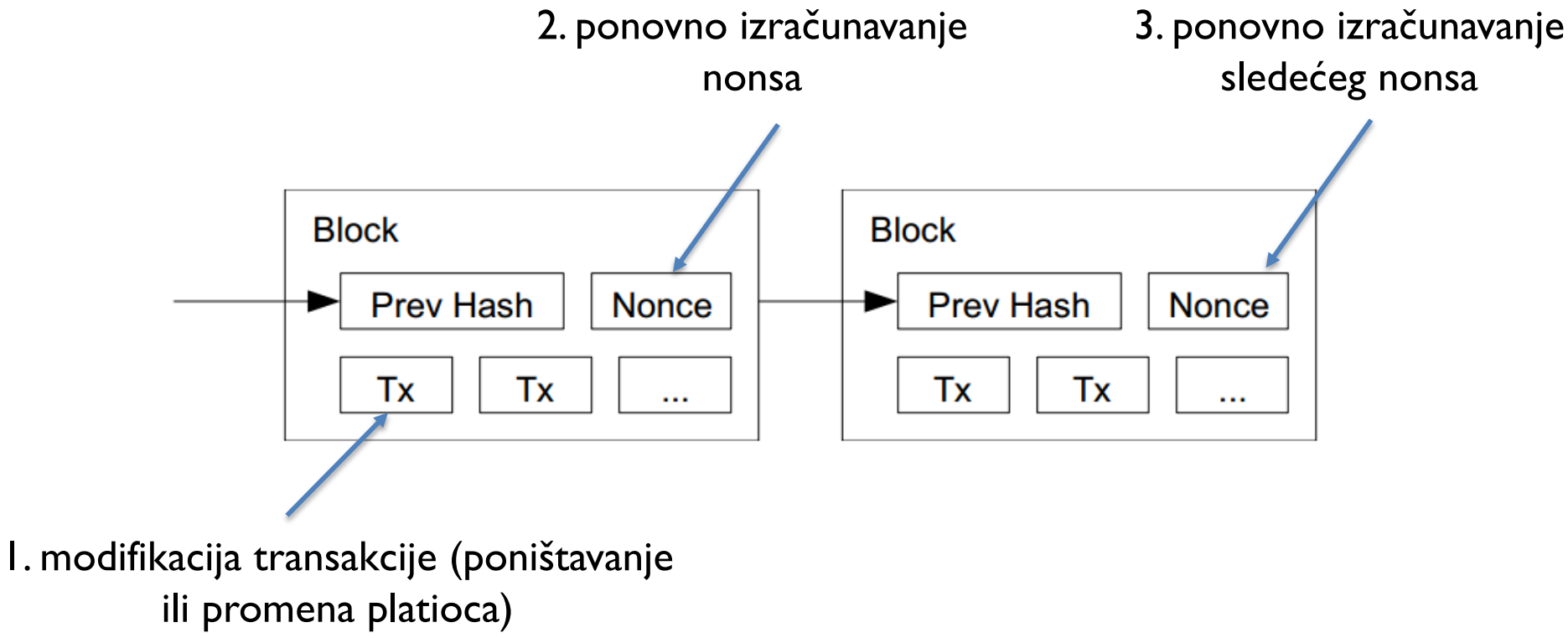
- Može se desiti da **dva čvora kreiraju istovremeno ispravne blokove** koji **zadovoljavaju dokaz posla**
  - oba se čuvaju, ali se dalje računa koristeći samo jedan od njih kao prethodni
  - ako **jedan od lanaca postane duži od drugog**, on se uzima kao **osnova za dalje**



Izvor: http://ina.kaist.ac.kr/ee324/F13/lectures/24-bitcoin.pptx

Poništavanje transakcija

- **Težina poništavanja transakcija eksponencijalno raste** sa **povećanjem dužine lanca u blokčejnu**

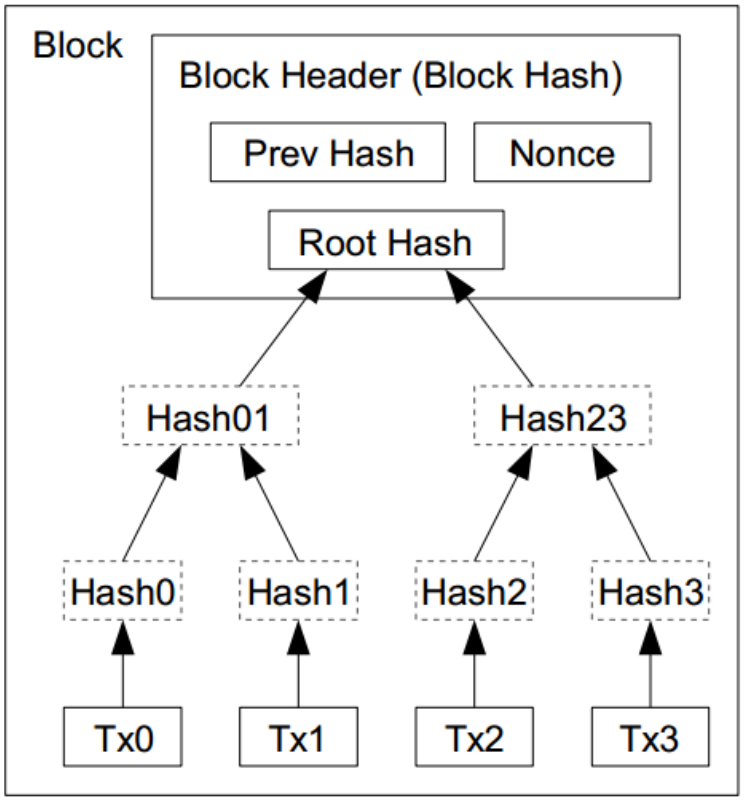


Izvor: http://ina.kaist.ac.kr/ee324/F13/lectures/24-bitcoin.pptx

Bitcoin optimizacije

- Bitcoin koristi i **Merkleovo stablo**
  - čuva se samo **heš korena** Merkleovog stabla u zaglavlju bloka
    - brišu se unutrašnje heš vrednosti kako bi se sačuvao memorijski prostor
    - zaglavlje bloka je veličine 80 bajtova
    - 80 B × 6 po h × 24 h * 365 = 4.2 MB/godini

Ralph Merkle (1952 –)

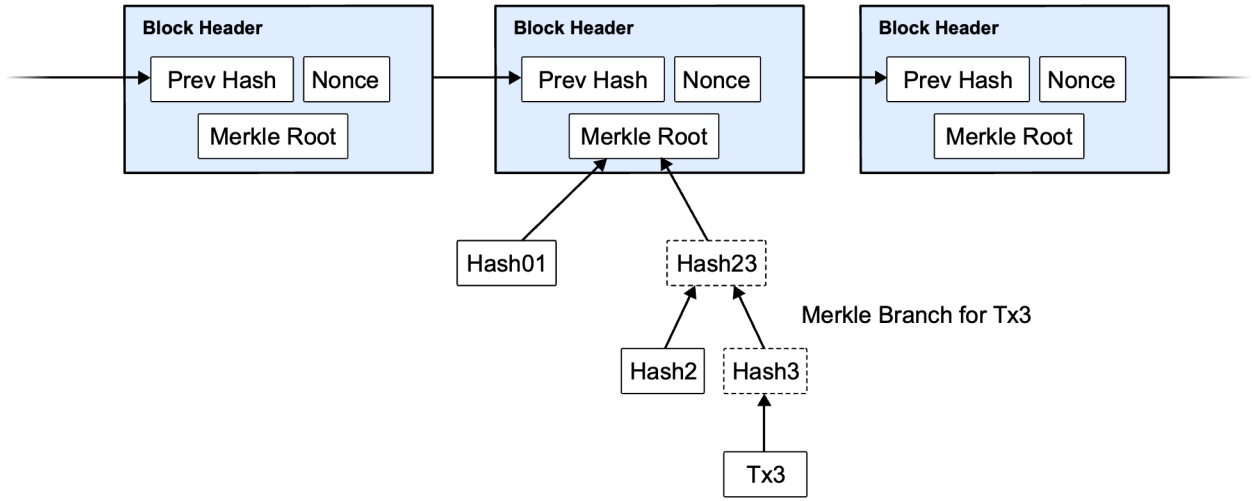


Transactions Hashed in a Merkle Tree

Izvor: http://ina.kaist.ac.kr/ee324/F13/lectures/24-bitcoin.pptx

Pojednostavljena verifikacija plaćanja

- Sistem **pojednostavljene verifikacije plaćanja** (engl. *simplified payment verification* – SPV)
- Svaki korisnik može lako verifikovati transakciju slanjem upita čvoru
- Prvo se pribavi najduži lanac dokaza posla
- Vrši se upit nad blokom u kome se nalazi transakcija koja se verifikuje (Tx3)
- Potrebni su samo Hash01 i Hash2 za verifikaciju, ne i heševi svih ostalih transakcija



Izvor: https://nakamotoinstitute.org/bitcoin/

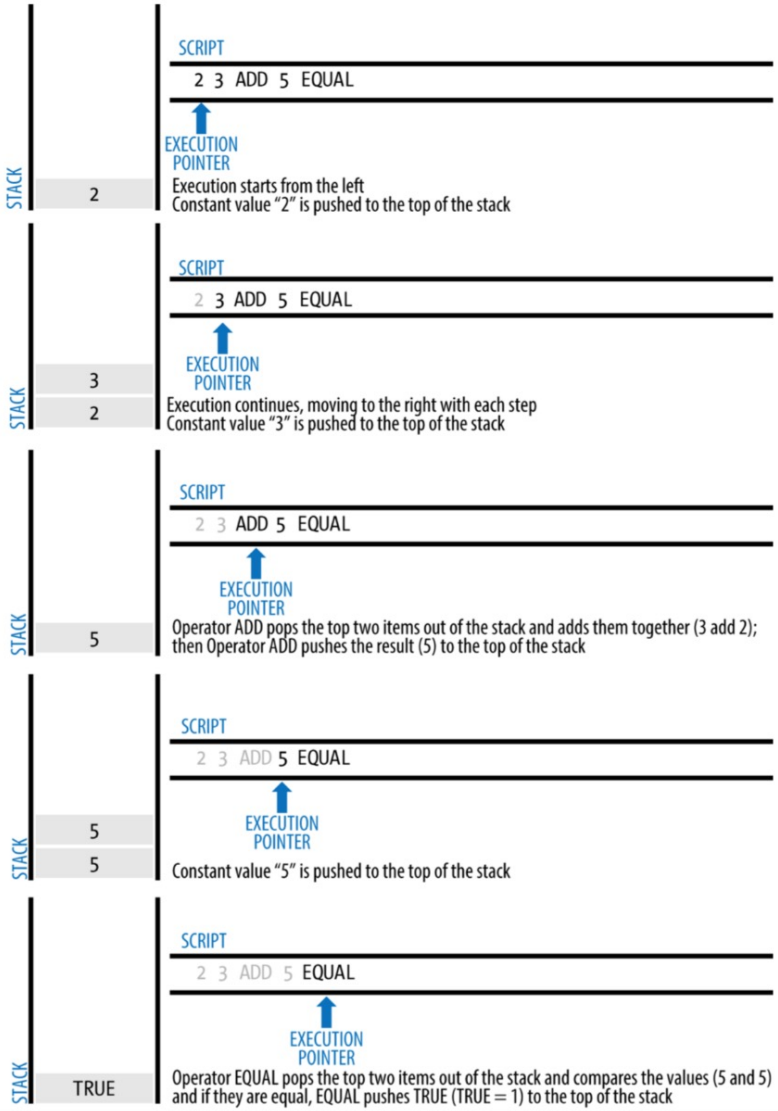
Bitcoin skripting jezik – Script

- Bitcoin **skripting jezik za opis transakcija Script** je programski jezik **zasnovan na steku** i koristi **inverznu poljsku notaciju** (engl. reverse-polish notation), inspirisan jezikom Forth koji je predstavio Chuck Moore 1970.
- Script sadrži širok skup operatora, ali je **namerno ograničen tako da ne podržava iteracije ili mogućnost složene kontrole toka**, već **samo prostu selekciju**
  - ovim se osigurava da jezik **nije Tjuring-kompletan,** što znači da **skripte** imaju **ograničenu kompleksnost** i **predvidljivo vreme izvršavanja**
  - ova ograničenja osiguravaju da jezik **ne može biti upotrebljen za kreiranje beskonačnih petlji** ili drugih oblika **„logičkih bombi“** koje mogu da se ugrade u transakcije na taj način da izazove napad tipa DoS (denial-of-service) protiv Bitcoin mreže
- Script jezik je **bez stanja** (engl. **stateless**), **ne pamti se stanje ni pre ni nakon izvršavanja skripte**
- **Sve informacije neophodne za izvršavanje skripte sadržane su u samoj skripti**
- **Skripte** će se **uvek predvidljivo izvršavati na isti način na svakom sistemu**

Bitcoin skripting jezik

- **Bitcoin sistem za validaciju transakcija** oslanja se na **dva tipa skripti** za validaciju transakcija:
  - **zaključavajuća skipta** (engl. ***locking script***) je uslov potrošnje (engl. *spending condition*) koji je postavljen na izlaz
  - **otključavajuća skripta** (engl. ***unlocking script***) je skripta koja rešava ili zadovoljava uslove postavljene na izlaz od strane zaključavajuće skripte i dozvoljava da izlazi budu potrošeni
  - zaključavajuća skripta, postavljena na UTXO (engl. *Unspent Transaction Output* – UTXO), i otključavajuća skipta pišu se u Script jeziku
- Primer:
  - **zaključavajuća skripta**: 3 OP_ADD 5 OP_EQUAL
  - **otključavajuća skipta**: 2
  - **rezultujuća skripta** dobijena konkatenacijom: 2 3 OP_ADD 5 OP_EQUAL
  - kada se **rezultujuća skripta** izvrši, dobija se rezultat OP_TRUE, što čini **transakciju validnom**

Primer: Bitcoin skripta



Izvor: Antanopoulos, A., "Mastering Bitcoin", 2nd edition

Praktična ograničenja Bitcoina

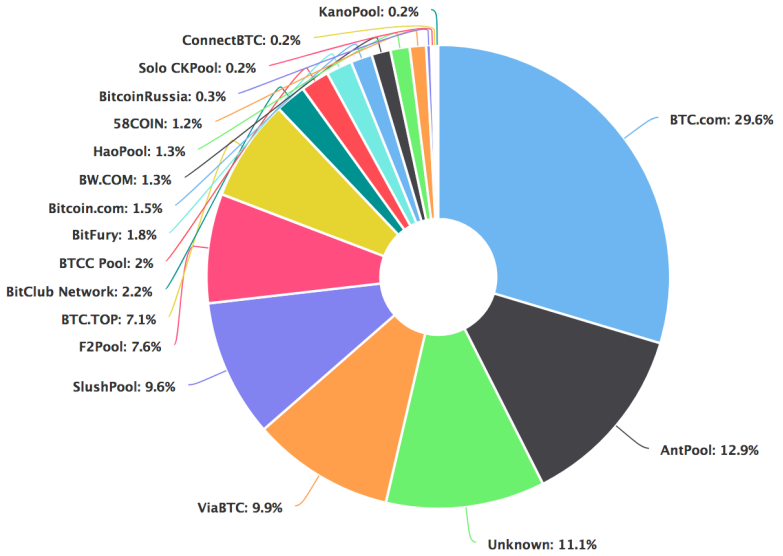
- Neophodno je **najmanje 10 minuta za verifikaciju transakcije**
  - saglasnost za plaćanje
  - čekanje na najmanje jedan blok (10 minuta) kako bi transakcija bila obrađena
  - za **veće transakcije** neophodno je **čekati duže** zato što na taj način **postaju bezbednije**. Tipično se u ovakvim situacijama **čeka na najmanje šest blokova** (1 sat)
- **Valuta** koja se **zasniva na poverenju** da će biti **prihvaćena kao sredstvo plaćanja** (engl. ***fiduciary currency***)
  - **nema intrinsičku vrednost**
- Implementaciona pitanja:
  - realizacija broadcast-a
  - vođenje evidencije o članstvu čvorova
  - kreiranje blokova
    - Kako se postiže dogovor o tome koje transakcije će biti uključene u blok?
    - Šta ako se razlikuju?
    - Šta ako neko vara tako što uključi mali broj transakcija u blok i počne brzo sa majningom?
  - prethodna pitanja nisu bila razmatrana u originalnom radu, ali su nužno rešavana prilikom implementacije, tj. razvoja Bitcoin Core

Bitcoin ekonomija

- **Ograničenje brzine** prilikom **kreiranja novih blokova**
  - stalno prilagođavanje na trenutni kapacitet mreže
  - blok se kreira svakih 10 minuta (6 blokova na sat)
    - težina se podešava svake dve nedelje kako bi se održao fiksnim odnos između kapaciteta i moći izračunavanja
  - *N* novih bitcoina za svaki novokreirani blok, dobija ih majner kao podsticaj
    - *N* je inicijalno bilo 50. 2020. je *N* = 6.25, sledeće polovljenje 2024.
    - polovljenje svakih 210000 blokova (svake četiri godine)
    - ukupan broj bitcoina doći će do 21 milliona
    - nakon 2140. majneri će imati podsticaj isključivo u vidu provizije od transakcija

Bitcoin – rezime

- **Bitcoin** kombinuje tehnike iz **kriptografije** sa pravim **podsticajem**
  - elegantan dizajn kao glavna osnova za veliku popularnost sistema
- U Bitcoin ekosistemu dešava se proces **industrijalizacije**
  - majneri formiraju **pulove** (engl. *pool*)
  - majning hardver je postao sofisticiran – prvobitno korišćeni CPU, potom GPU, a danas je majning isplativ isključivo korišćenjem ASIC
  - Bitcoin **menjačnice** (engl. *exchanges*)
    - tržište derivata (engl. *derivative market*)
    - problem **centralizacije**
  - važno pitanje **regulacije kriptovaluta**



Izvor: https://www.buybitcoinworldwide.com/mining/pools/