Lanac blokova (Blockchain)

Primenjeni algoritmi

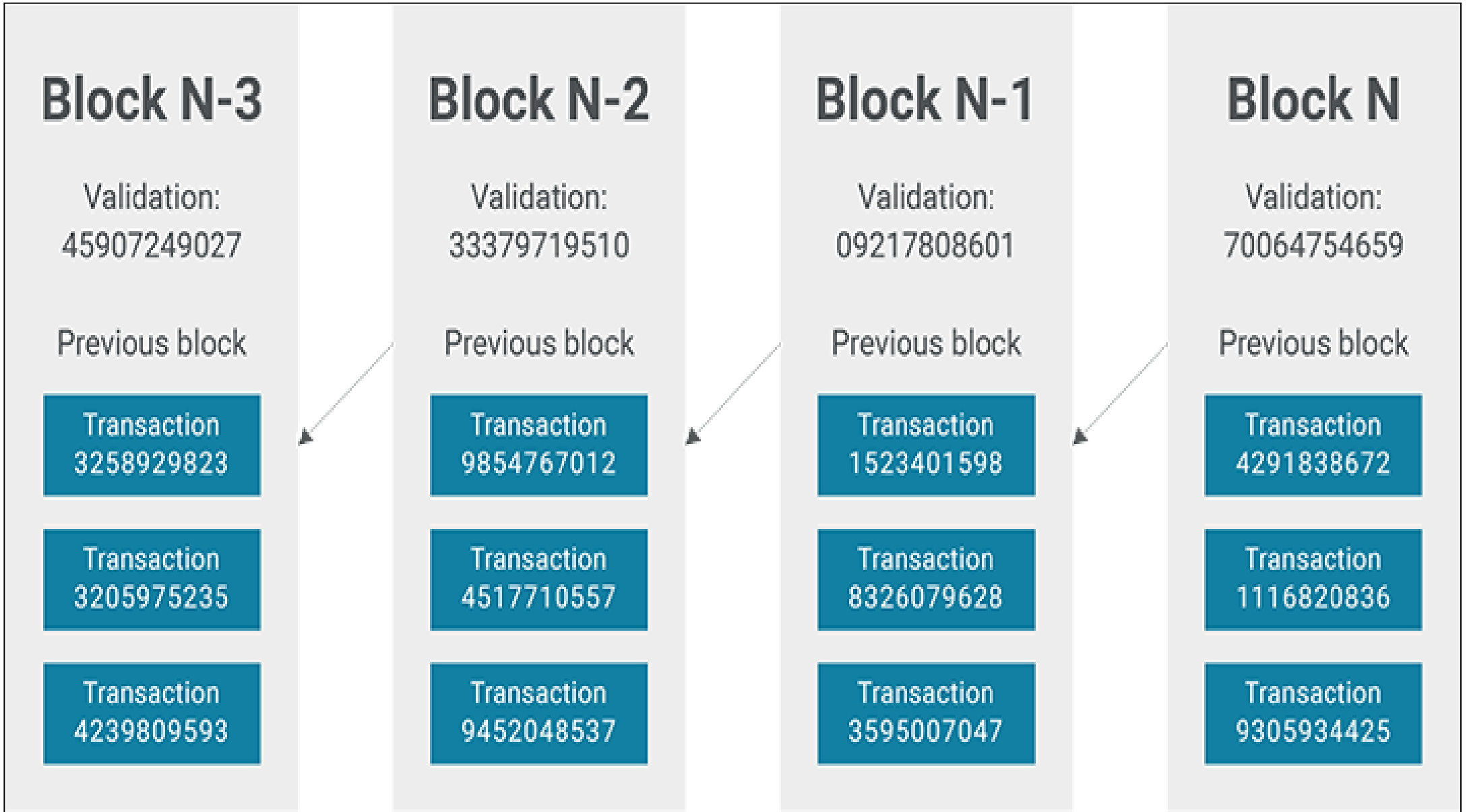
Uvod

- *Blockchain* - kolekciju podataka
  - decentralizovana,
  - distribuirana i
  - javna (uglavnom)

- Logička povezanost blokova
  - veza bloka sa prethodnikom - lanac (*chain*)
  - blok sadrži heš (engl. *Hash*) vrednost prethodnog bloka. Kriptografija!

- Podaci u bloku - skup korisničkih transakcija.

Logička predstava



Osnovni principi

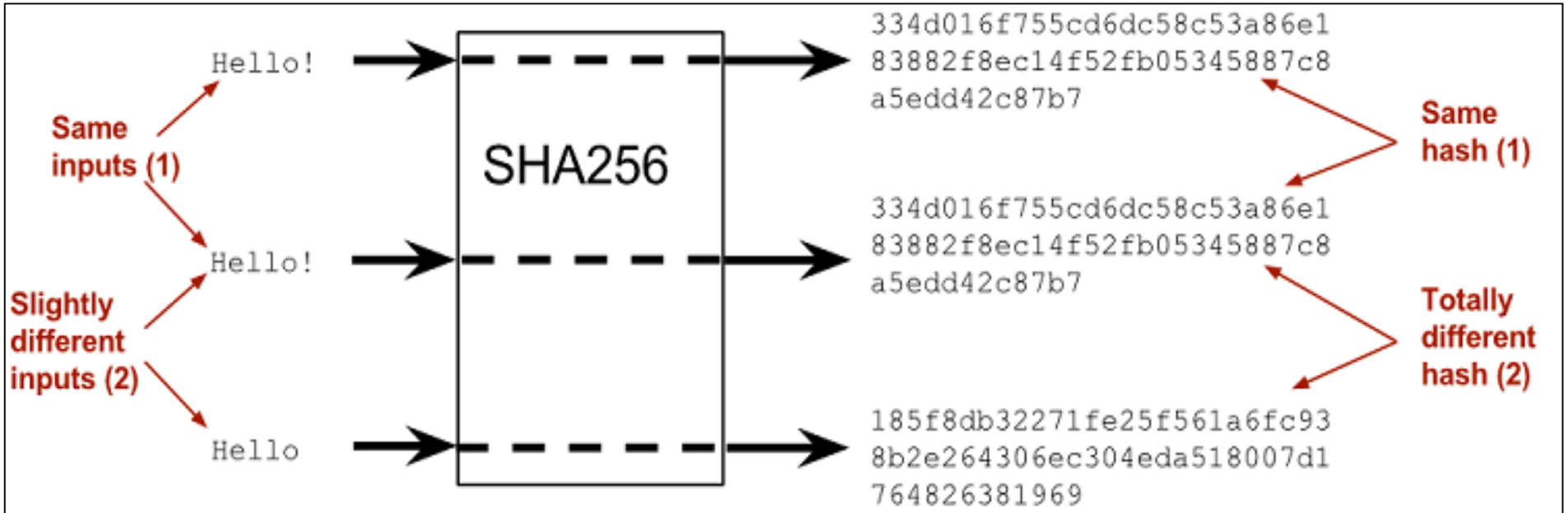
- *Blockchain* se može posmatrati kao distribuirana knjiga podataka (engl. *Distributed Ledger Techology*) koja nema centralno skladište.
- Podaci su dostupni svakom čvoru u mreži čime se postiže transparentnost.
- Svaka promena (dodavanje novog bloka) je javna i svaki čvor dobija najnovije stanje u mreži.
- Dodavanje novih blokova vrše „rudari” (engl. *Miners*), tj. povezani računari koji koriste veliku količinu električne energije prilikom rešavanja kriptografskih zadataka.
- *Blockchain* tehnologija se najviše primenjuje u oblasti kriptovaluta. Najpoznatije su *Bitcoin* i *Ethereum*.
- Takođe, može se koristiti za skladištenje medicinskih nalaza, kreiranje pametnih ugovora (engl. *Smart contract*), za analizu poslovnih procesa, itd.

Struktura

- Logička predstava *Blockhain* arhitekture se interpretira kao lanac blokova gde je svaki blok povezan sa svojim prethodnikom.
- Glavni elementi i karakteristike *Blockchain*-a su:
  - Heš
  - Lanac blokova
  - Direktna komunikacija (P2P)
  - Digitalni potpis (engl. *Signature*)
  - Algoritmi koncenzusa

Heš

- Heš vrednost se dobija pomoću heš funkcije.
- Ne postoji inverzna heš funkcija.
- Ulazne vrednosti - bilo koji tip podataka, izlazne – najčešće u heksadecimalnom zapisu
- SHA256 algoritam – jedna od najčešće korišćenih heš funkcija

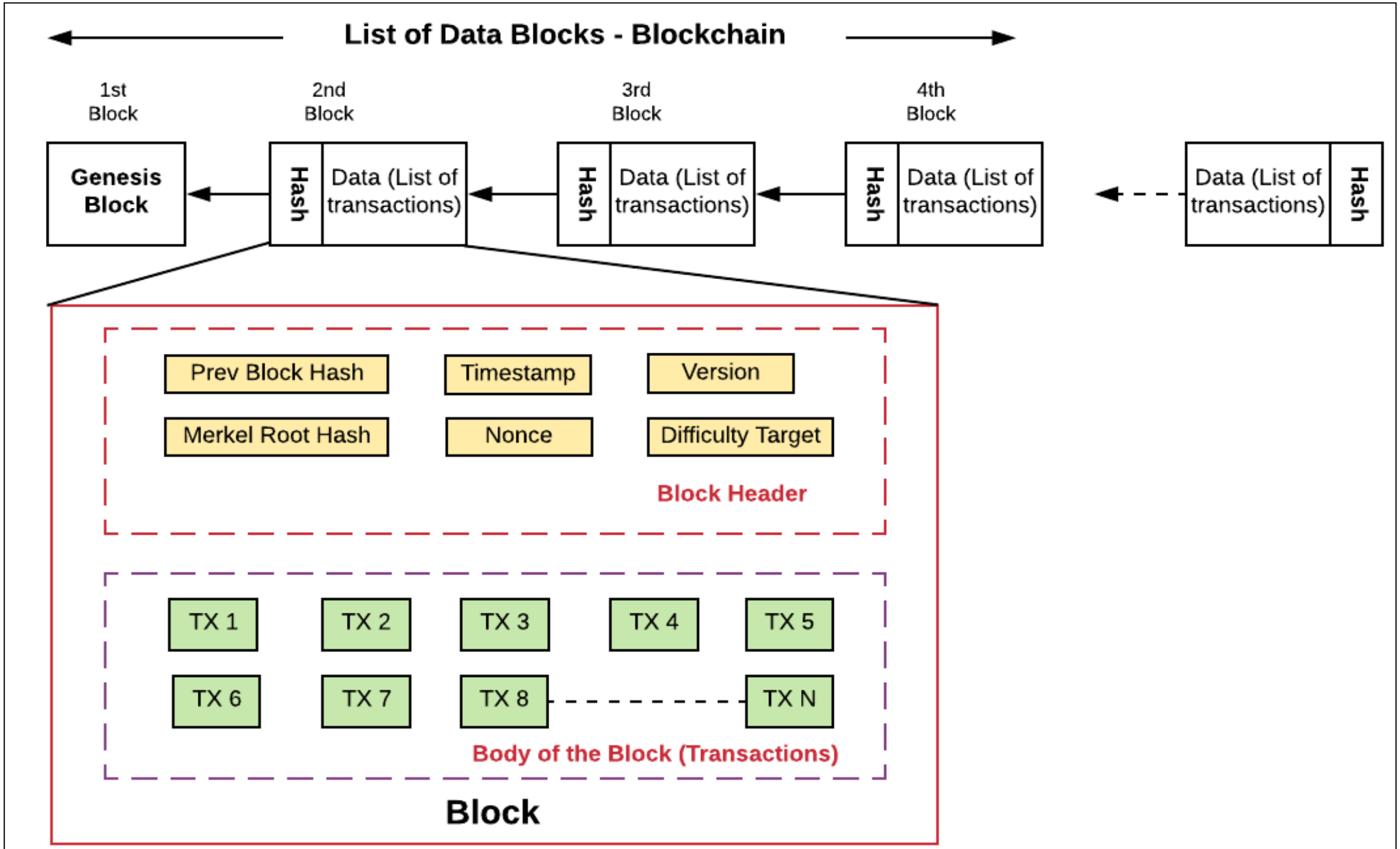


Lanac blokova

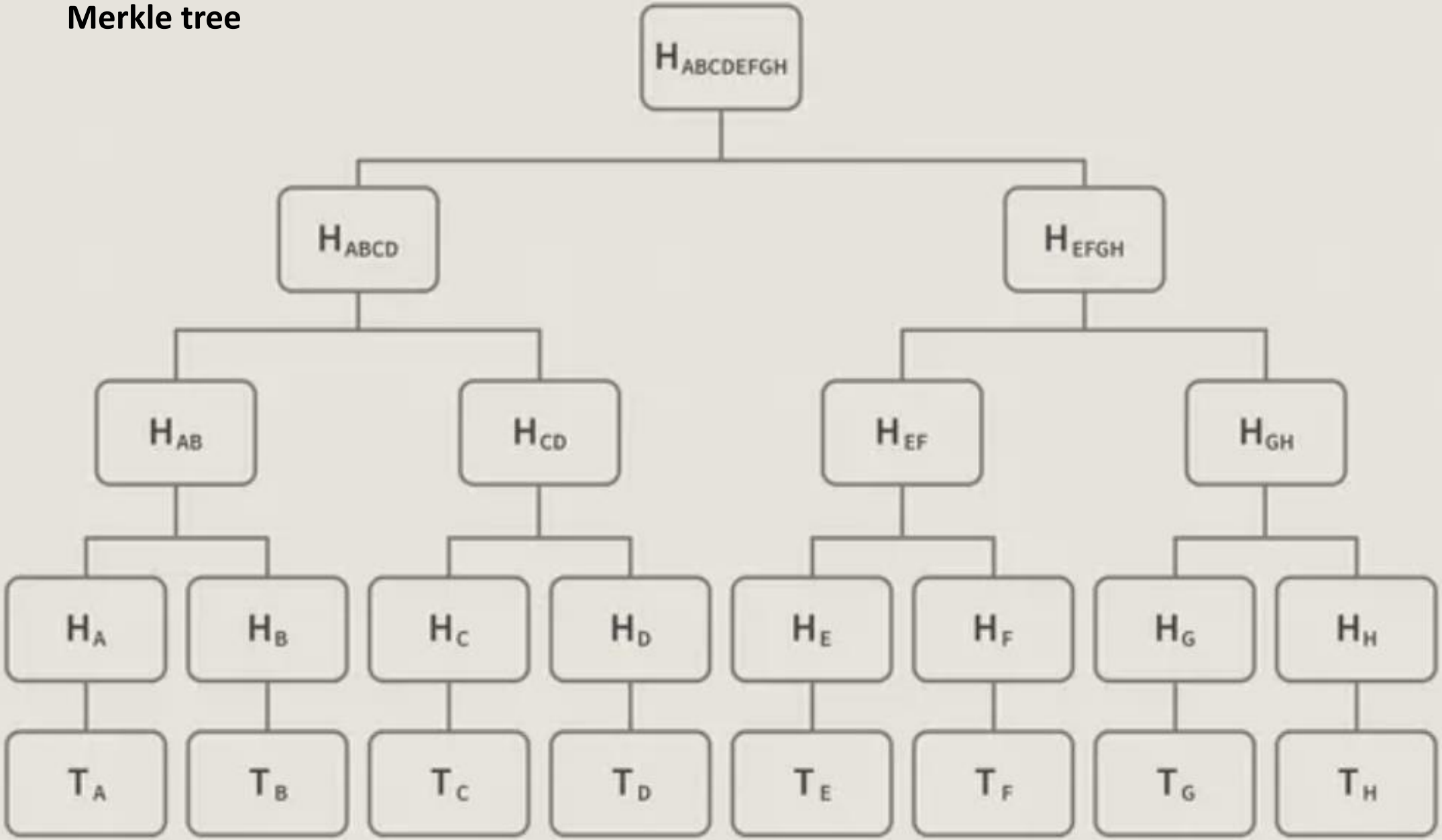
- Transakcije između korisnika u mreži se skladište u blokove koji su međusobno povezani, čime se kreira lanac.
- Blok sadrži:
  - **Veličinu** (engl. *Block Size*) – izražava se u bajtima (4 bajta).
  - **Broj transakcija** (engl. *Transaction counter*) – broj transakcija smeštenih u blok.
  - **Transakcije** – podaci smešteni u blok.
  - **Zaglavlje** (engl. *Block Header*) – sadrži polja koja definišu blok.

Sadržaj zaglavlja bloka

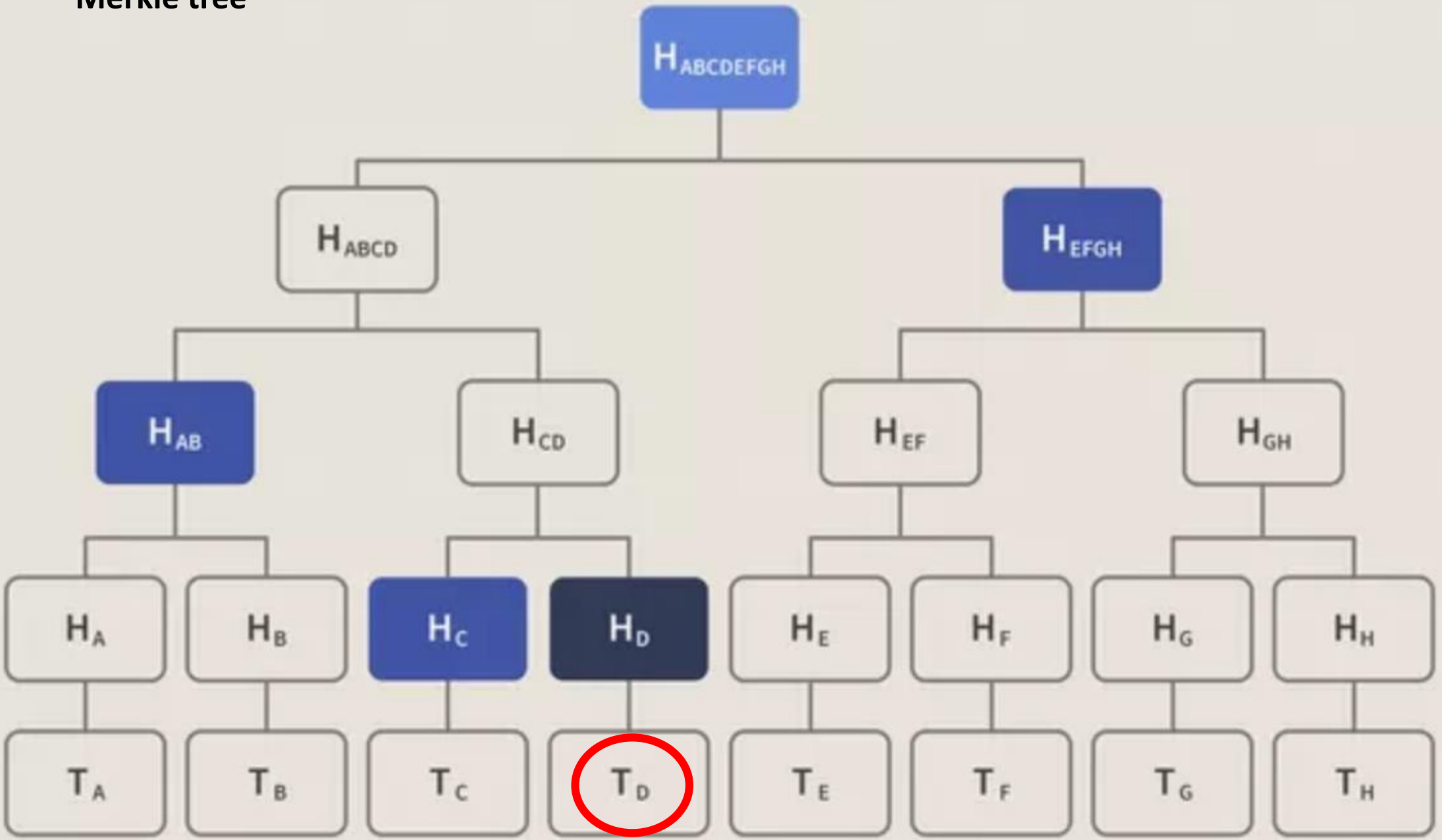
- **Pokazivač na prethodni blok** – sadrži heš vrednost prethodnog bloka.
- **Korensku heš vrednost** (engl. *Merkle Root Hash*) – predstavlja heš vrednost svih transakcija u bloku koja se dobija pomoću *Merkle Tree* strukture.
- **Težinu** (engl. *Difficulty Target*) – parametar koji određuje koliko je vremena i električne energije potrebno da bi se kreirao novi blok.
- **Brojač** (engl. *Nonce*) – jedinstvena, nasumična vrednost koja se može samo jednom iskoristiti za kreiranje bloka. Povećava se ukoliko generisana heš vrednost nije validna za kreiranje novog bloka.
- **Vreme** (engl. *Timestamp*) – trenutak kreiranja bloka.
- **Verziju** (engl. *Version*) – određuje validaciona pravila.


List of Data Blocks - Blockchain
1st Block
2nd Block
3rd Block
4th Block
Genesis Block
Hash
Data (List of transactions)
Hash
Data (List of transactions)
Hash
Data (List of transactions)
Data (List of transactions)
Hash
Prev Block Hash
Timestamp
Version
Merkel Root Hash
Nonce
Difficulty Target
Block Header
TX 1
TX 2
TX 3
TX 4
TX 5
TX 6
TX 7
TX 8
TX N
Body of the Block (Transactions)
Block

Merkle tree

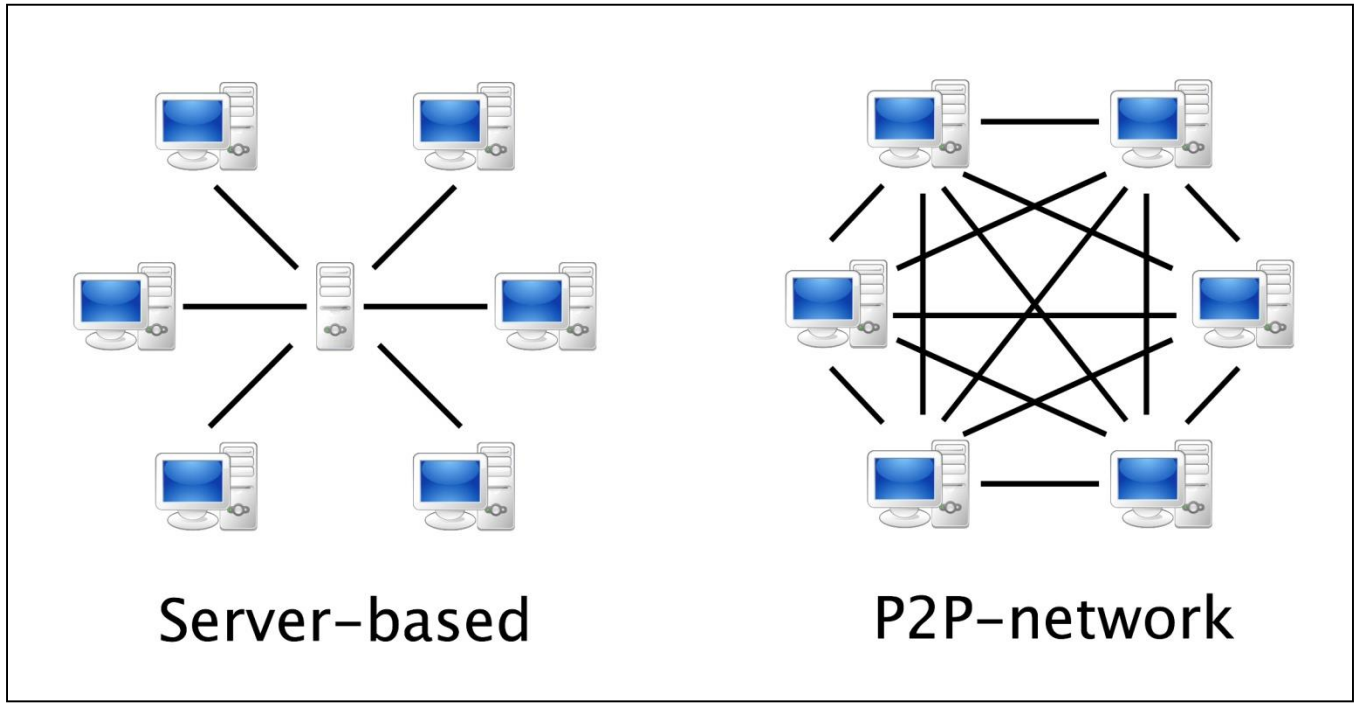

$H_{ABCDEFGH}$
H_{ABCD}
H_{EFGH}
H_{AB}
H_{CD}
H_{EF}
H_{GH}
H_A
H_B
H_C
H_D
H_E
H_F
H_G
H_H
T_A
T_B
T_C
T_D
T_E
T_F
T_G
T_H

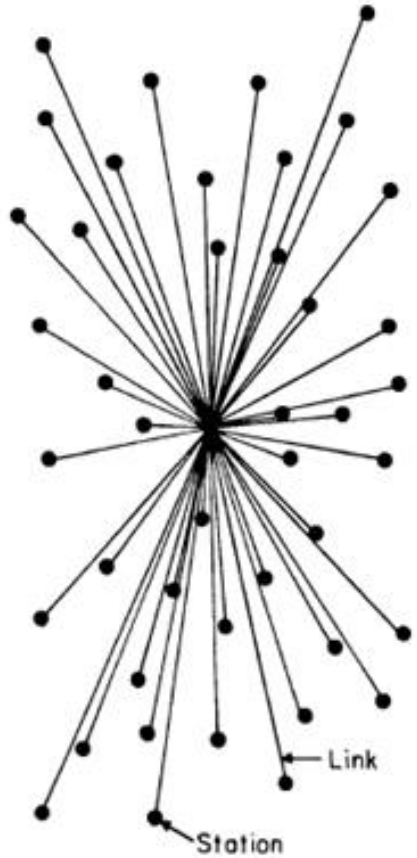
Merkle tree


$H_{ABCDEFGH}$
H_{ABCD}
H_{EFGH}
H_{AB}
H_{CD}
H_{EF}
H_{GH}
H_A
H_B
H_C
H_D
H_E
H_F
H_G
H_H
T_A
T_B
T_C
T_D
T_E
T_F
T_G
T_H

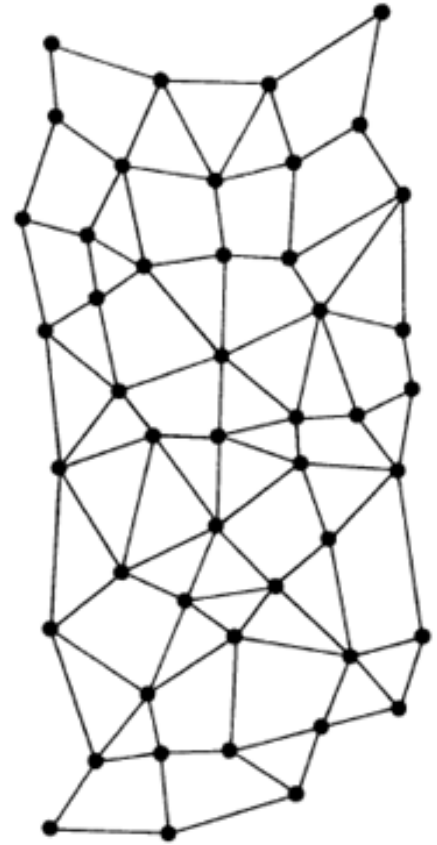
Direktna komunikacija (P2P)

- Blockchain arhitektura je bazirana P2P komunikaciji

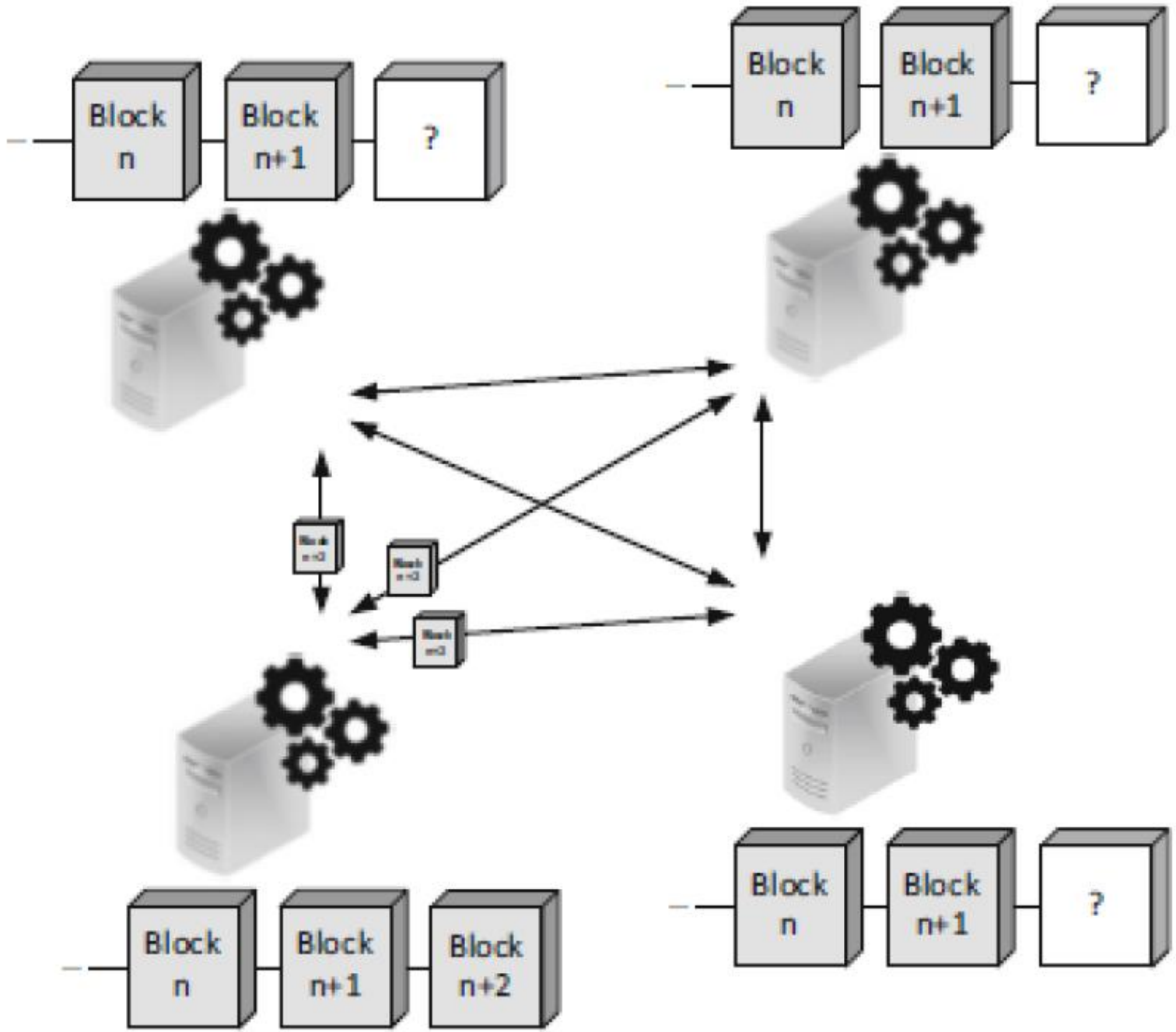




CENTRALIZED



DISTRIBUTED


Block n
Block n+1
?
Block n
Block n+1
?
Block n
Block n+1
Block n+2
Block n
Block n+1
?

Digitalni potpis

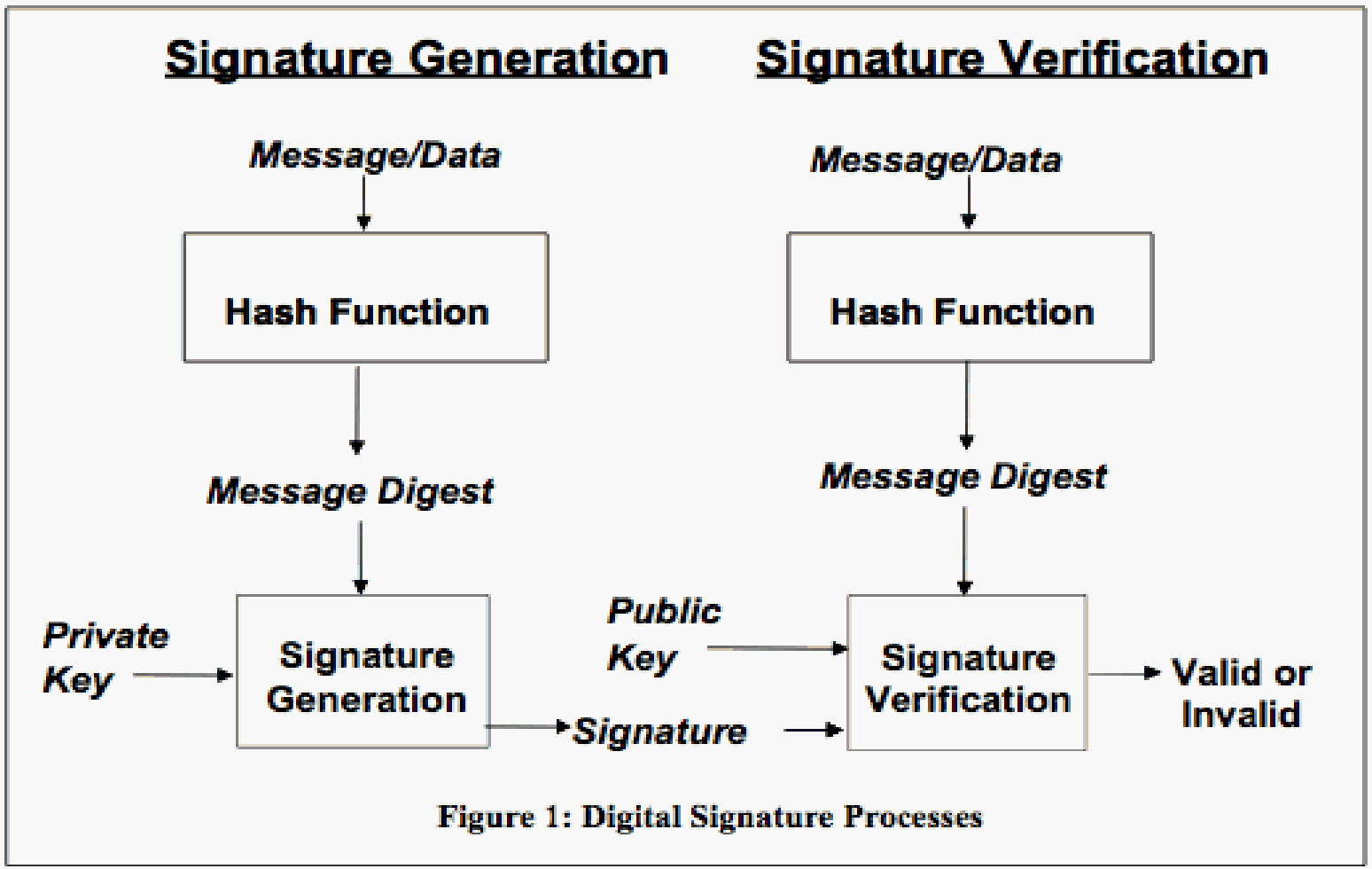


Figure 1: Digital Signature Processes

Algoritmi koncenzusa

- Najpoznatiji algoritmi koncenzusa su:
  - *Proof of Work* (PoW)
  - *Proof of Stake* (PoS)
  - *Proof of Authority*
  - *Practical Byzantine Fault Tolerance* (PBFT)
  - *Proof of Burn* (PoB)
  - *Proof of Capacity*
  - *Proof of Elapsed Time*

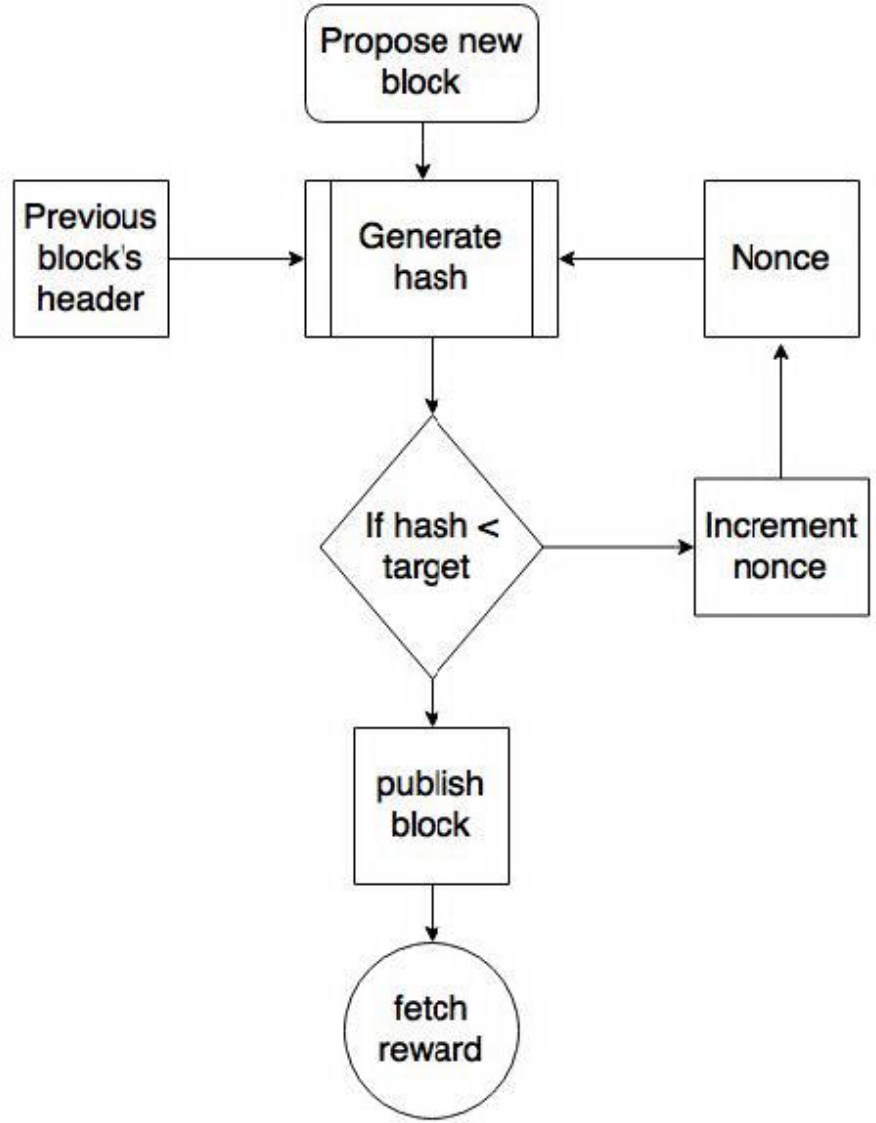
Proof of Work

- *Proof of Work* je najpoznatiji algoritam koncenzusa.
- Radi po principu: „Rešenje je teško pronaći, ali ga je lako potvrditi”.
- Čvorovi u mreži koji vrše dodavanje novih blokova se popularno nazivaju rudari.
- Međusobno se takmiče rešavajući kriptografske zadatke – heš vrednosti sa određenim uslovima
- Rešenje u vidu heš vrednosti predstavlja dokaz o radu, s obzirom da je utrošena značajna količina električne energije.
- Dodavanje novog bloka se u proseku izvršava na svakih deset minuta.
- Rudari se često udružuju (engl. *Mining pools*) kako bi imali veće šanse prilikom pronalaženja heš vrednosti. Kada je pronađu, nagrada se deli između svih čvorova na osnovu njihove priložene računarske moći.

Algoritam kopanja

Koraci:

1. Uzima se zaglavlje prethodnog bloka iz mreže.
2. Sakuplja se skup transakcija koje se difuzno emituje na mrežu kao predloženi blok
3. Računa se dupli heš zaglavlja prethodnog bloka koji se kombinuje sa nonce-om i novim predloženim blokom koristeći SHA-256 algoritam
4. Proverava se da li je rezultujući heš manji od trenutnog cilja (nivoa težine).
   - **Uspešno**: šalje se blok u novi i kopači traže nagradu.
   - **Neuspešno**: proces se ponavlja posle inkrementiranja nonce-a.



Proof of Stake

- Radi po principu ulaganja kriptovaluta (engl. *Stake*) u mrežu
- Validatori su zaduženi za kreiranje blokova:
  - Svaki validator ulaže u mrežu određen iznos u kriptovaluti.
  - Mreža nasumično bira validatora koji će da kreira naredni blok.
  - Validator sa najvećim ulogom ima najveće šanse da bude izabran.
  - Za kreiranje bloka se dobija nagrada u određenom iznosu kriptovalute.
- Prednosti PoS mehanizma u odnosu na PoW su:
  - Energetska efikasnost – nije neophodno trošiti resurse i električnu energiju.
  - Ušteda u opremi – nije neophodno koristiti moćne računare za kreiranje novog bloka.
  - Jača otpornost ka centralizaciji – moguće je povećati broj čvorova u mreži.
  - Podrška za sporedne lance (engl. *Shard chains*) – utiče na skalabilnost *Ethereum* mreže.

Proof of Authority

- Obično za odobrene knjige identiteti korisnika moraju biti poznati i verifikovani.
- Mogućnost objavljivanja novih blokova je diktirana korisničkim dozvolama (isto kao kod tradicionalnih baza podataka).
- Nema problema u vezi sa procesorskom snagom ili strujom.

Primena Blockchain-a

- Finansijske organizacije
- Osiguravajuća društva
- Zdravstvene organizacije
- Sajber bezbednost

Pametni ugovori (*Smart Contracts*)

- Korisnički definisan program koji se pokreće na blockchain-u i omogućuje izvršavanje transakcija bez trećeg lica.
- Omogućuju dodatnu sigurnost uz smanjanje transakcionih troškova
- Pametni ugovori imaju sledeće karakteristike:
  - isključivo elektronske prirode;
  - implementacija softvera;
  - povećana sigurnost;
  - uslovne prirode;
  - nezavisnost

Primena pametnih ugovora

- Automobilska industrija
- Nekretnine
- Zdravstvena zaštita
- Elektronska trgovina