



Conf.dr.Cristian KEVORCHIAN

Facultatea de Matematica si  
Informatica

# Distributed Ledger, Blockchain, Bitcoin

# Istoric

- Conceptul de monedă digitală descentralizată, precum și aplicații alternative, cum ar fi registrele de proprietate, au existat de zeci de ani.
- Protocoalele anonime cum ar fi **e-cash** din anii 1980 și 1990, bazate în cea mai mare parte pe primitive criptografice cunoscute sub numele de Chaumian blind, au fundamentat o monedă cu un grad înalt de confidențialitate, dar protocoalele nu au reușit să câștige popularitate la tranzacționare datorită dependenței lor de un nod central.
- În 1998, **B-money** ai lui **Wei Dai** au devenit prima propunere de introducere a ideii de a crea bani prin rezolvarea **puzzle-urilor computationale**, precum și a consensului descentralizat, însă propunerea nu era suficient de detaliată cu privire la modul în care consensul descentralizat ar putea fi pus în aplicare.
- În 2005, **Hal Finney** a introdus un concept de „**reuseble proofs of work**”, un sistem care utilizează idei de la B-money împreună cu puzzle-urile Hashcash compuse de **Adam Back** pentru a crea un concept pentru o criptomonedă, dar, din nou, bazându-se pe trustworcy computing ca backend.
- În 2009, o monedă descentralizată a fost pusă în aplicare pentru prima dată în practică de **Satoshi Nakamoto**(**Bitcoin: A Peer-to-Peer Electronic Cash System**”, combinând primitivele stabilite pentru gestionarea proprietăților criptografie cu chei publice cu un algoritm de consens pentru a urmări cine deține monede, cunoscut ca „proove of work”.

# Registrul distribuit(ledger)

- Un registru distribuit(ledger) este un tip de bază de date care este partajat, reprodus și sincronizat între membrii unei rețele. Registrul distribuit înregistrează tranzacții, cum ar fi schimbul de mijloace fixe sau date, între utilizatorii rețelei.
- Utilizatorii rețelei iau decizii prin consens de actualizare a înregistrărilor din "ledger". Nu există implicarea niciunui mediator central sau terț, cum ar fi o instituție financiară sau un centru de compensare.
- Fiecare înregistrare din registrul distribuit include o amprentă de timp și o semnătură unică, astfel făcând registrul auditabil pentru toate tranzacțiile din rețea.
- Un framework pentru dezvoltarea de aplicații în zona consensului sau a serviciilor de "membership" de tip open source Hyperledger Fabric

# DLT(Distributed Ledger Technology)

- În 2016 termenul de DLT a fost utilizat pentru a descrie tehnologia care nu se baza în mod specific pe blockchain
- Tehnologia non-blockchain a generat suport pentru volume mari de transacții și date asociate micro-transacțiilor, DAG(Direct Acyclic Graph)
- Proiecte din categoria HashGraph în care este creată o nouă alternativă de consens la blockchain. Folosește un protocol gossip care funcționează în felul următor: Fiecare nod din Hashgraph poate răspândi informații semnate (numite evenimente) pentru noile tranzacții create și pe tranzacțiile primite de la alții către vecinii aleși aleatoriu.
- Fluree – o bază de date blockchain ordonată în funcție de timp

# Blockchain

- Reprezintă baza de date distribuită(nu exista un server central)
- Publică, neavând un deținător.
- Continu actualizată de orice utilizator.
- Securizată criptografic de fiecare utilizator
- Datele în blockchain sunt imutabile
- Fiecare înregistrare a bazei de date distribuite se numește **bloc**
- Fiecare nou **bloc** constă dintr-o familie de transacții care este adăugata la sfârșitul blockchain-ului.

# Monede digitale decentralizate

- 2009-Satoshi Nakamoto, dezvoltă Bitcoin , un "asset" digital fără "valoare intrinsecă" și fără un emitent sau gestionar central.
- Mai important decât aceasta este tehnologia care fundamentează acest produs financiar, Blockchain, drept un instrument de distribuire a consensului(proof-of-work).
- Ether este o criptomonedă al cărui blockchain este generat de platforma ETHEREUM
- ETHEREUM este o stivă de tehnologii open source compatibilă web 3.0(server less architecture), care poate fi configurată drept un sistem de operare. OS este una din numeroasele posibilități în care poate fi configurat Ethereum. Poate fi configurat ca o criptomonedă asociată unui blockchain, o platformă destinată execuției de contracte smart etc.
- O oarecare confuzie se produce când se pune semnul egal între blockchain și DLT(Distributed Ledger Technology)

Cele două diferă prin:

- Blockchain utilizează o criptomonedă. DLT nu
- Blockchain lucrează cu proof of work. DLT nu
- Blockchain, datele sunt vizibile din fiecare nod DLT nu.
- Blockchain este fara-permisiuni, DLT nu.

1

Cele două au în comun:

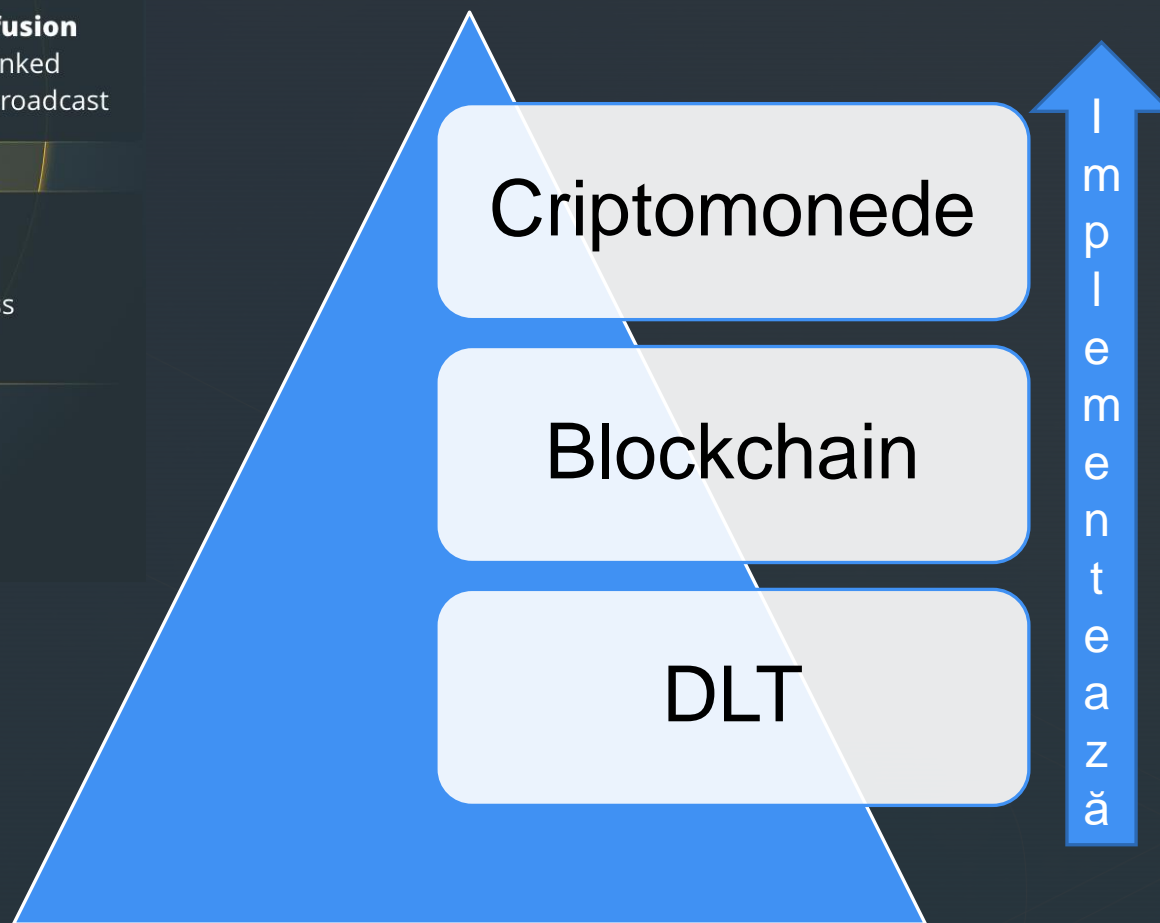
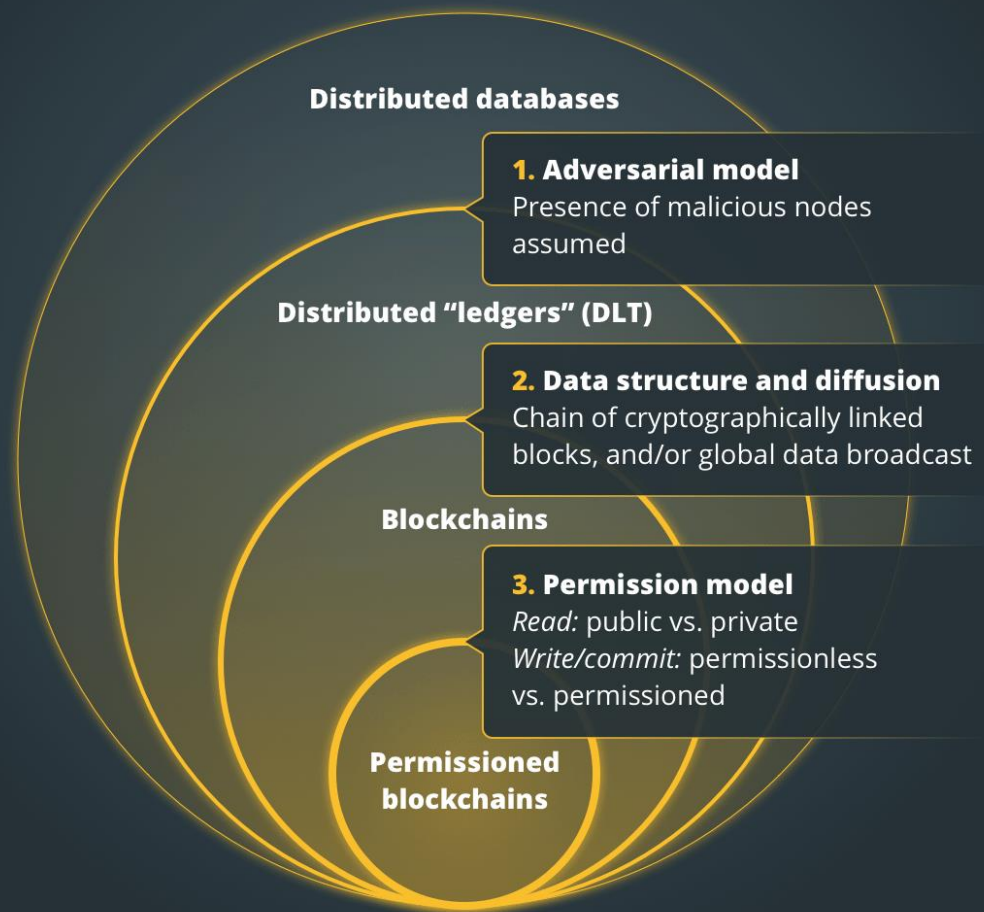
- Utilizează chei criptografice publice/private
- Utilizează hashing
- Utilizează modele de comunicare P2P.

DLT vs. BLOCKCHAIN

Blockchain este un caz particular de DLT




# Ierarhia Conceptuală





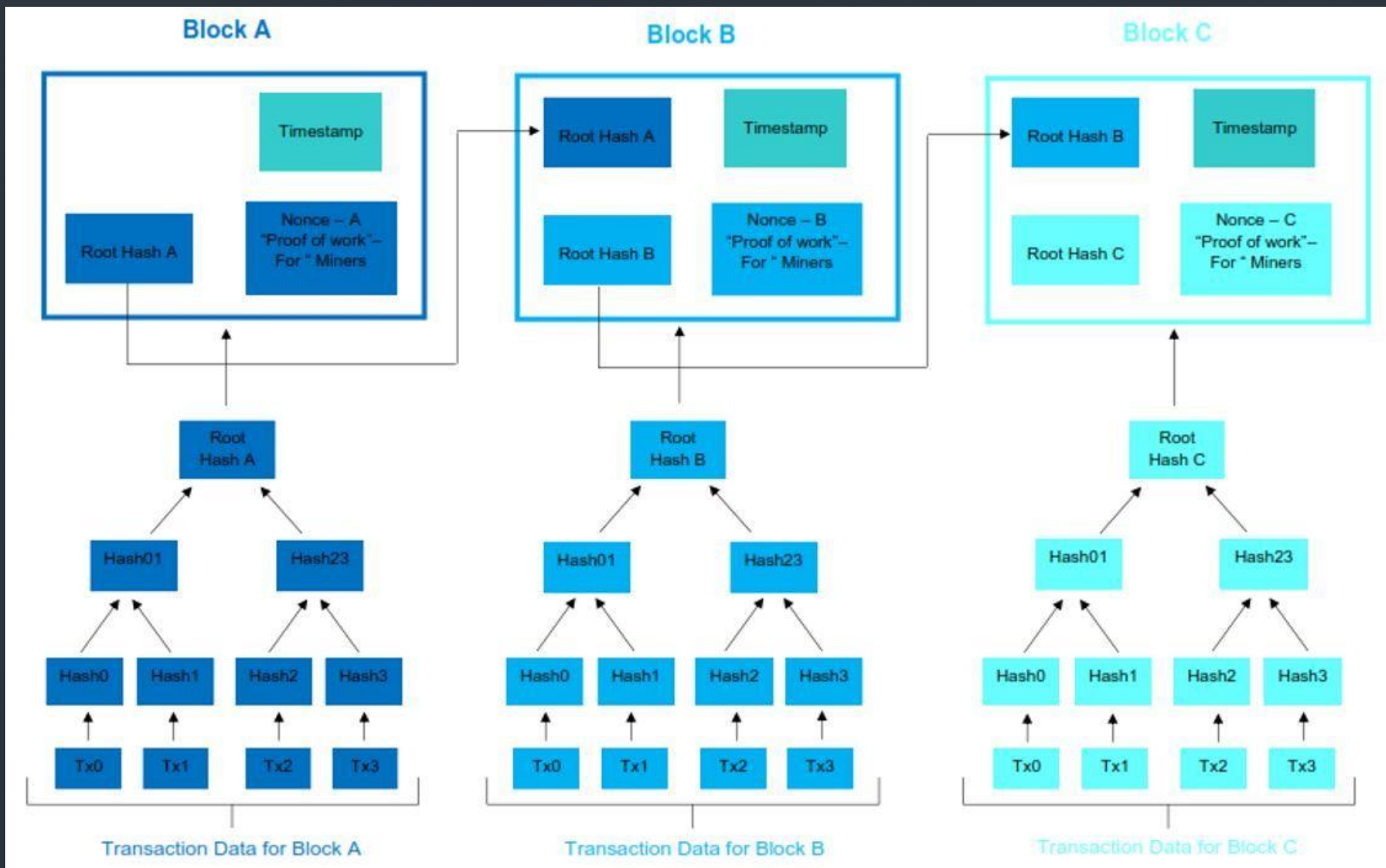
# Bitcoin ca masină cu stări finite

- **Sistemul clasic de tranzactionare**
- Functia de tranzitie:  $APLIC(S, TX) \rightarrow S'$  sau EROARE
- Exemplu:  $APLIC(\{Ion:Ron50, Maria:Ron50\}, \{TRIMITE\ Ron20\ de\ la\ Ion\ la\ Maria\}) = \{Ion:Ron30, Maria:Ron70\}$
- **BITCOIN**
- Starea Bitcoin este data de o colectie de monede:
- $S_{BTC} = UTXO$ (Unspend Transaction Output) care au fost minate si nededtinute.
- O tranzactie contine unul sau mai multe input-uri. Fiecare input conține o referinta la UTXO si o semnatura criptografica generate de o cheie private.

- 
- Blockchain poate fi văzută drept un registru public în care toate tranzacțiile sunt stocate sub forma unei secvențe lineare temporal înlănțuită de fișiere numite block-uri.
  - Lista de block-uri este nelimitată prin faptul că noi blocuri pot fi atașate în coada ei.
  - Tranzacțiile noi sunt în mod constant procesate de "miner-i" în blocuri noi care sunt adăugate la sfârșitul secvenței și nu pot fi niciodată modificate sau eliminate după ce au fost acceptate în rețea.
  - Implementarea criptografiei asimetrice și a algoritmului de consens asigură securitatea și consistența

# Anatomia unui block

- Un block este format dintr-un:
  - Header(80 bytes), care include:
    - Versiunea blocului
    - Rădăcina arborelui Hash
    - Amprenta-de-Timp – timpul curent in timp-universal(1-lanuarie-1970).
    - nBiți- pragul țintă pentru un block hash valid
    - **Nonce**: un câmp de 4 octeți, care de obicei începe cu 0 și crește pentru fiecare calcul hash
    - Block-ul hash părinte-o valoare hash de 256 de biți care indică blocul anterior.
  - Corpul block-ului - este compus dintr - un contor de tranzacții și tranzacțiile propriu-zise.
    - Numărul maxim de tranzacții pe care un bloc le poate conține depinde de dimensiunea blocului și dimensiunea fiecare tranzacție.
    - Acestea sunt distribuite indirect prin rădăcina arborelui hash. Deoarece tranzacțiile nu sunt rulate direct, hashing-ul unui bloc cu 1 tranzacție expune același efort ca și hashing-ul unui bloc cu 10.000 de tranzacții.



# Semnătura Digitală

- Fiecare utilizator deține o pereche de chei una privată și una publică. Se folosește cheia privată care va fi păstrată în confidențialitate pentru a semna tranzacțiile. Tranzacțiile semnate digital sunt difstribuite peste întreaga rețea.
- Semnătura este utilizată în două faze: faza de semnare și faza de verificare.
- De exemplu, o utilizatoare Maria dorește să îl trimită un mesaj unui utilizator Ion. În faza de semnare, Maria criptează datele ei cu cheia privată și îi trimite lui Ion rezultatul criptat și datele originale. În faza de verificare, Ion validează valoarea cu cheia publică a lui Maria. De această manieră, Ion a putut verifica cu ușurință dacă datele au fost sau nu schimbate.
- Algoritmul tipic de semnătură digitală folosit în block-uri este cel de semnătură digitală al curbei eliptice (ECDSA)



# Principale caracteristici ale Blockchain-**Decentralizarea**

- **Descentralizarea**-în contextul clasic al tranzacționării centralizate, fiecare tranzacție trebuie să fie validată de o structură centrală (cum ar fi Banca Centrală) fapt ce conduce inevitabil la costuri ridicate pe tranzacție precum și probleme legate de performanța serverelor centrale.
- În opoziție cu abordarea centralizată a tranzacționării existența unei terțe autorități nu mai este necesară în cazul blockchain.
- Algoritmii de consens în blockchain rezolvă problema consistenței datelor la nivelul rețelei distribuite.



# Principale caracteristici ale Blockchain-Persistența

- Tranzacțiile pot fi validate rapid, iar cele respinse în procesul de validare nu ar trebui acceptate de "miner-ii" onești.
- Practic este foarte dificil să ștergem sau să facem rollback la tranzacții incluse în blockchain.
- Block-urile care includ tranzacții invalide pot fi identificate imediat.

## Principale caracteristici ale Blockchain- **Anonimitatea și Auditibilitatea**

- Fiecare utilizator poate interacționa cu blockchain-ul prin intermediul unei adrese generate, care nu poate revela reala identitate a utilizatorului.
- Datorită unor restricții interne blockchain nu poate garanta păstrarea intimității utilizatorului
- Blockchain-ul Bitcoin-stochează date despre utiliztor, balanțe bazate pe modelul Unspent Transaction Output. Orice tranzacție trebuie să refere orice tranzacție trecută și "necheltuită". Tranzacția poate fi ușor monitorizată .



# Taxonomia sistemelor Blockchain



# Clasificarea sistemelor Blockchain

- Sistemele actuale de blockchain se clasifică astfel:
  - Blockchain public – toate înregistrările au caracter public și toți utilizatorii participă la procesul de stabilire al consensului.
  - Blockchain privat – numai acele noduri care provin de la o anumită organizație le este permisă participarea la procesul de stabilire a consensului.
  - Blockchain asociat unui consorțiu – numai un grup de noduri preselecțate participă la stabilirea consensului.

# Determinarea consensului

- Sistemele centralizate impun controlul accesului, fapt ce conduce la stabilirea unui nivel de încredere asupra celor care operează sistemul.
- Un blockchain este operat de persoane necunoscute și de părți pentru care nu putem realiza un nivel minim de încredere(nu stim dacă este o persoană, organizație sau un robot care operează automat, sau orice altceva similar)
- Lipsa încrederii în modul de operare al utilizatorilor blockchain este deosebit de importantă în utilizarea "consensului". Deoarece orice entitate, poate trimite informații către blockchain(adică poate să adauge informații în baza de date), este necesar ca operatorii distribuiți ai acestuia să evalueze și să cadă de acord asupra tuturor addendelor înainte de a fi permanent încorporate în blockchain. Deoarece încrederea în autor este minimă, este vital ca toate informațiile noi să fie revizuite și confirmate înainte de a fi acceptate. Această revizuire are drept rezultat "consensul,,.

# Permisele Citirii

- Tranzacțiile într-un Blockchain sunt vizibile utilizatorilor, în timp ce pentru un Blockchain Privat sau de un Blockchain al Consorțiului depinde de un nivel de control al accesului integrat în protocol. Există platforme dedicate pentru Private Blockchain scalabile pentru organizații mari cum ar fi MultiChain, Hyperledger și Chain.
- Pentru un Blockchain complet privat permisiunile de scriere sunt păstrate centralizat de către o singură organizație. Opțiunile de citire pot fi publice sau limitate într-o măsură arbitrară. Aplicațiile probabile includ gestionarea bazelor de date, auditul etc. intern al unei singure companii, astfel încât citirea în public poate să nu fie necesară în multe cazuri, deși în alte cazuri este dorită audibilitatea publică.



# Imutabilitate

- Deoarece înregistrările sunt stocate pe un număr mare mare de echipamente, este aproape imposibil să se poată fi manipulate tranzacțiile într-un Blockchain Public.
- Nu același lucru se poate spune dacă ne referim la Blockchain-ul Privat sau de Consorțiu, care pot fi manipulate datorită faptului că există doar un număr limitat de participanți.

# Eficiența

- Este nevoie de mult timp pentru a propaga tranzacțiile și blocurile datorită, în principal, numărului mare de noduri ale Blockchain-ului public. Drept urmare debitul de tranzacționare este limitat, iar latența este ridicată.
- Cu mai puține validări, Blockchain-ul de consorții și privat poate fi mai eficient.

# Analiză comparativă

Proprietate	Blockchain		
	Public	Privat	Consortiu
Determinarea consensului	Toate nodurile	Mulțime de noduri selectate	Organizație
Permiuni de citire	Public	Poate fi public sau restricționat	Poate fi public sau restricționat
Imutabilitate	Aproape imposibil de falsificat	Posibilitate de falsificare	Posibilitate de falsificare
Eficiență	Scăzută	Mare	Mare
Centralizat	Nu	Parțial	Da
Procesul de realizare a Consensului	Nepermis	Permis	Permis

# Algoritmi de consens in Blockchain

- Există patru metode importante pentru stabilirea consensului
  - Practical Byzantine Fault Tolerance Algorithm(PBFTA)
  - Proof-of-Work Algorithm(PoW)
  - Proof-of-Stake Algorithm(PoS)
  - Delegated-Proof-of-State(DPoS)

# Proof-of-Work(PoW)

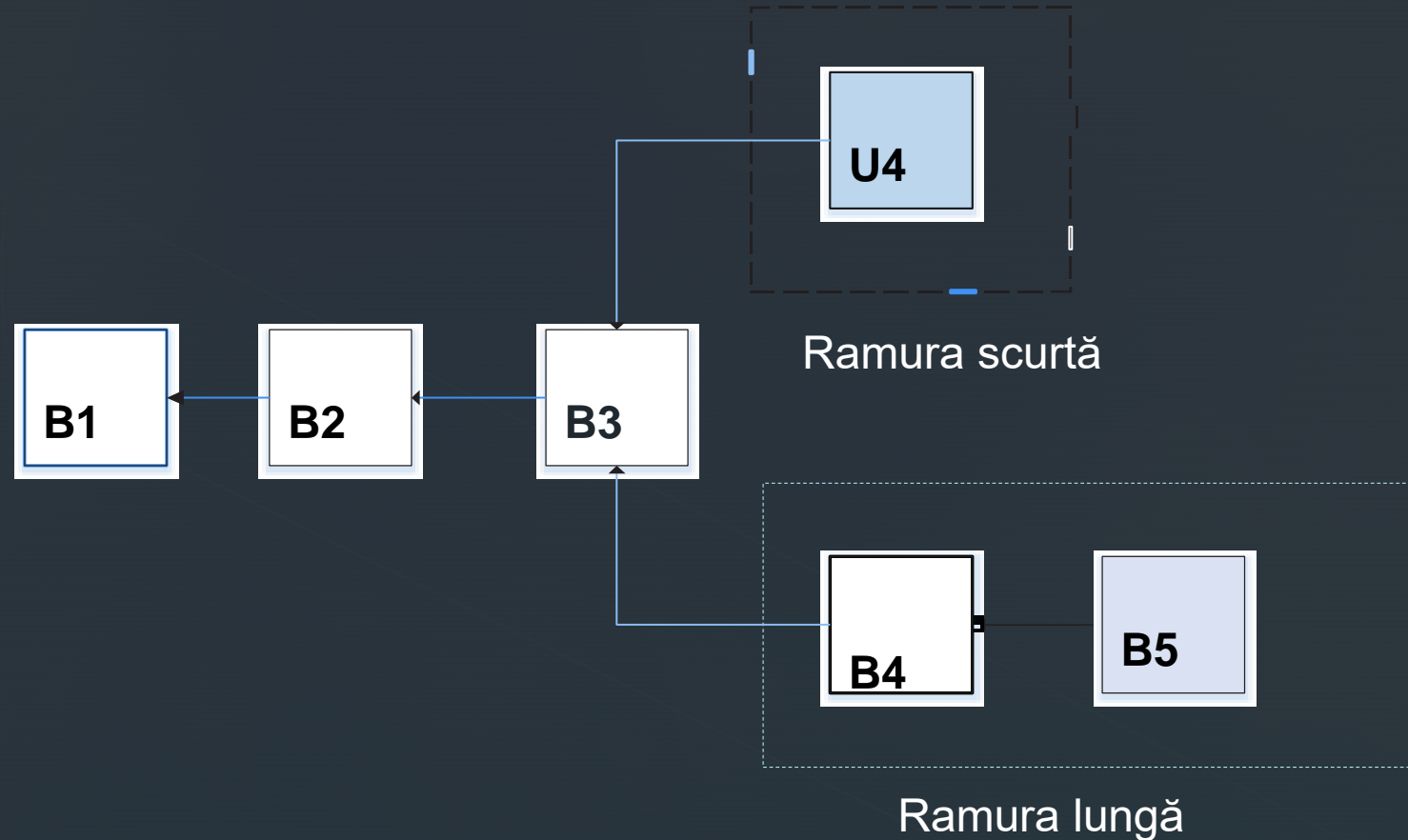
- Este o strategie de consens utilizată în rețeaua Bitcoin.
- Într-o rețea descentralizată, o "autoritate virtual" trebuie selectată pentru a înregistra tranzacțiile.
- Cea mai ușoară este selecția aleatorie.
- Selecția aleatoare este vulnerabilă la atacuri. Dacă un nod dorește să publice un bloc de tranzacții, trebuie un volum mare de analiză(efort de calcul) pentru a dovedi că nodul nu este malițios.
- PoW – implică faptul că fiecare nod al rețelei calculează o valoare hash a antetului blocului. Antetul blocului conține un "nonce" și minerii ar schimba frecvent "nonce" pentru a obține valori hash diferite. Consensul presupune ca valoarea calculată să fie egală sau mai mică decât o anumită valoare dată.

# Proof-of-Work(PoW) [cont]

- Când un nod atinge valoarea țintă, acesta va transmite blocul către alte noduri iar toate celelalte noduri trebuie să confirme reciproc corectitudinea valorii hash. Dacă blocul este validat, atunci alți miner-i vor adăuga acest nou bloc propriilor blocuri.
- Nodurile care calculează valorile hash sunt numite “miner-i”, iar procedura PoW este numită “minerit” în Bitcoin.
- În rețele descentralizate, este posibil ca blocurile valide să poată fi generate simultan atunci când mai multe noduri găsesc în același timp un ”nonce” potrivit. Ca urmare, pot fi generate ramificații.
- Este puțin probabil ca două ramificații concurente să genereze simultan același bloc.
- În protocolul PoW, un lanț care devine mai lung este considerat drept unul autentic.



# Scenariu pentru distribuția pe ramuri pentru blockchain



Ex. Considerăm ramificațiile care generează U4 și B4 validate simultan. Minerii își păstrează blocurile până când se găsește o ramură mai lungă. B4, B5 formează un lanț mai lung, astfel că minerii de pe U4 ar trece la ramura mai lungă.