

Blockchain –същност

проф. д-р инж. Венета Алексиева

ОСНОВНИ МОМЕНТИ

- Идеята за блокчейн
- Възникване на технологиите
- Абстрактни модели
- Структура на блок
- Дърво на Меркъл
- Хеш
- Токени
- Bitcoin – началото
- Копаене на криптовалута (mining) – цел, използвани алгоритми, хардуер, сайтове.

Преди идеята за Blockchain (1/2)

- Информация с времеви печат
 - Цифров подпис, включващ времеви печат (1991)
 - Използване на техники за хеширане
- Дърво на Меркъл (1979)
 - Съхраняване на хеширана информация
 - Организация на двоично дърво
 - Сливането на блокове включва изчисляване на нов хеш, свързан с „бащиния възел“
- Силна криптографска основа, но
 - Как може да се съхранява дървото на Меркъл
 - Как да се защити от атаки

Преди идеята за Blockchain (2/2)

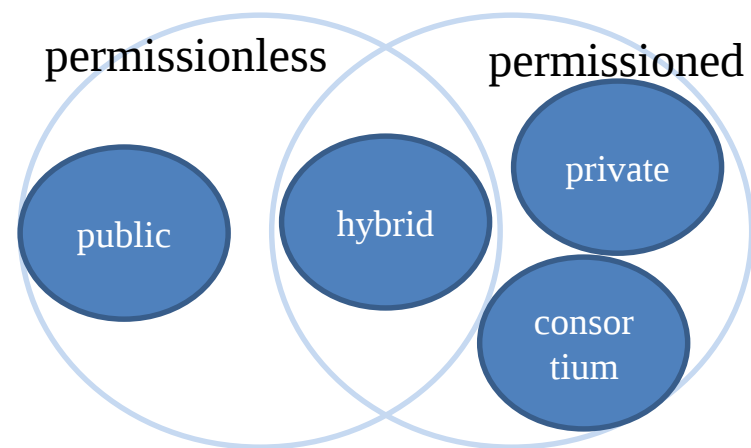
- От транзакция до блокчейн
 - Блокът съхранява данни за транзакции и Хеш на предишния блок
- Дърво на Меркъл съхранява блоковете
 - Всеки блок е подписан с хеш
- Децентрализирано съхранение на дървото на Меркъл
 - Разпределени регистри за по-безопасно съхранение
 - Общо правило за управление – доверие в процеса на валидиране на блокове

Консенсусни механизми

- Proof of Work (PoW)
 - Хешът на блока се изчислява чрез математическо предизвикателство - намиране на „nonce“ чрез bruteforce метод
 - Изисква значителни изчислителни ресурси и енергия
 - Доверието зависи от инвестицията в хардуер и от „консумираните“ изчислителни ресурси
- Proof of Stake
 - Валидаторът се избира на случаен принцип според инвестираната валута
 - Избягва се тежко изчисление
 - Включва по-малко спекулации
- Proof of Authority
 - Списък с потенциални сертифицирани валидатори
 - Марка за репутация

Контрол на достъпа

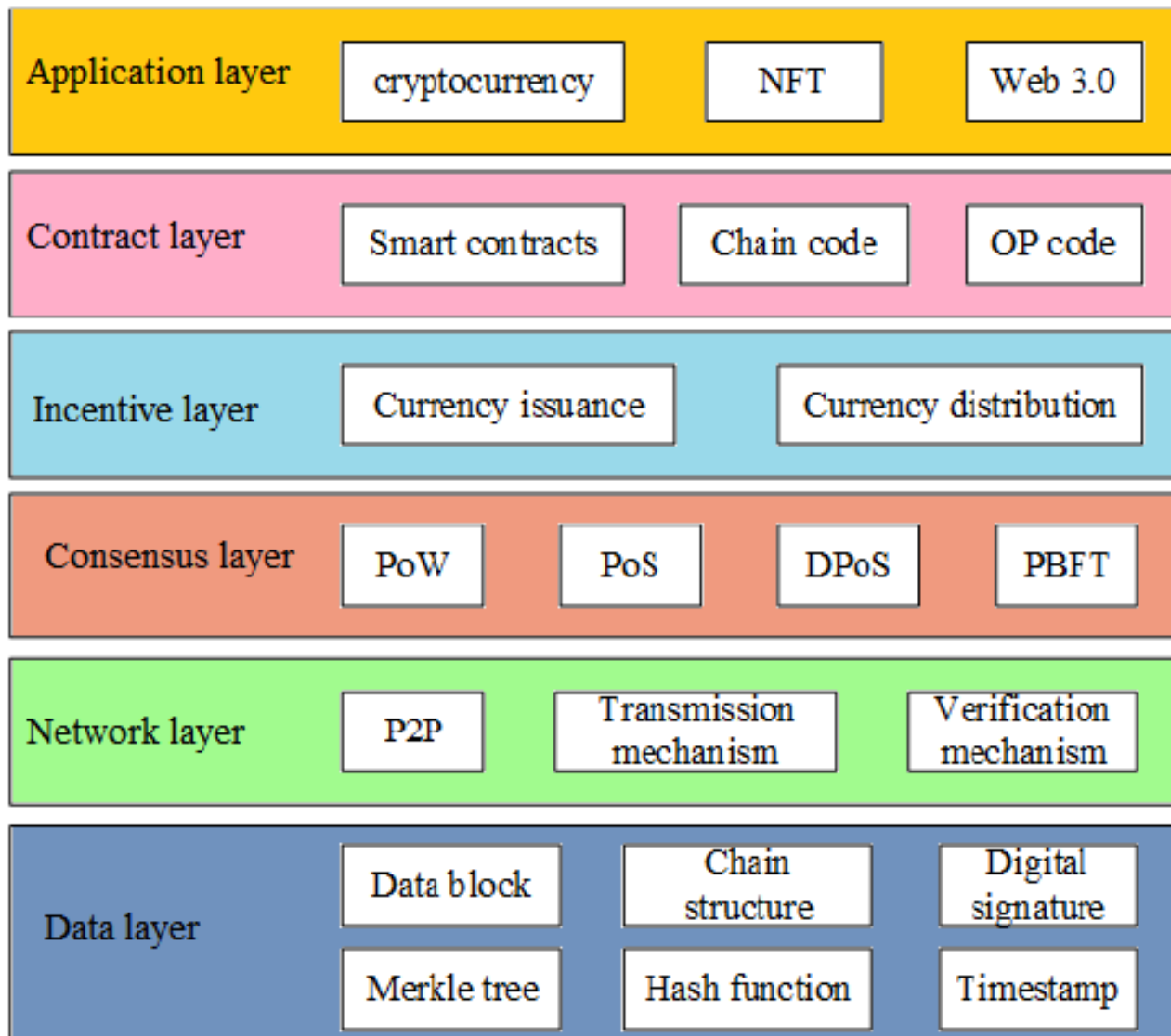
- Permissionless blockchain
 - Отворени и споделени регистри
 - Безплатен достъп за валидатори
 - Потребителите се идентифицират по аватара си
 - Публичен блокчейн
- Permissioned blockchain
 - Упълномощени валидатори
 - Ограничен достъп до регистри
 - Потребителите са свързани с добре познати самоличности
 - Използва се за частен блокчейн / консорциумен блокчейн



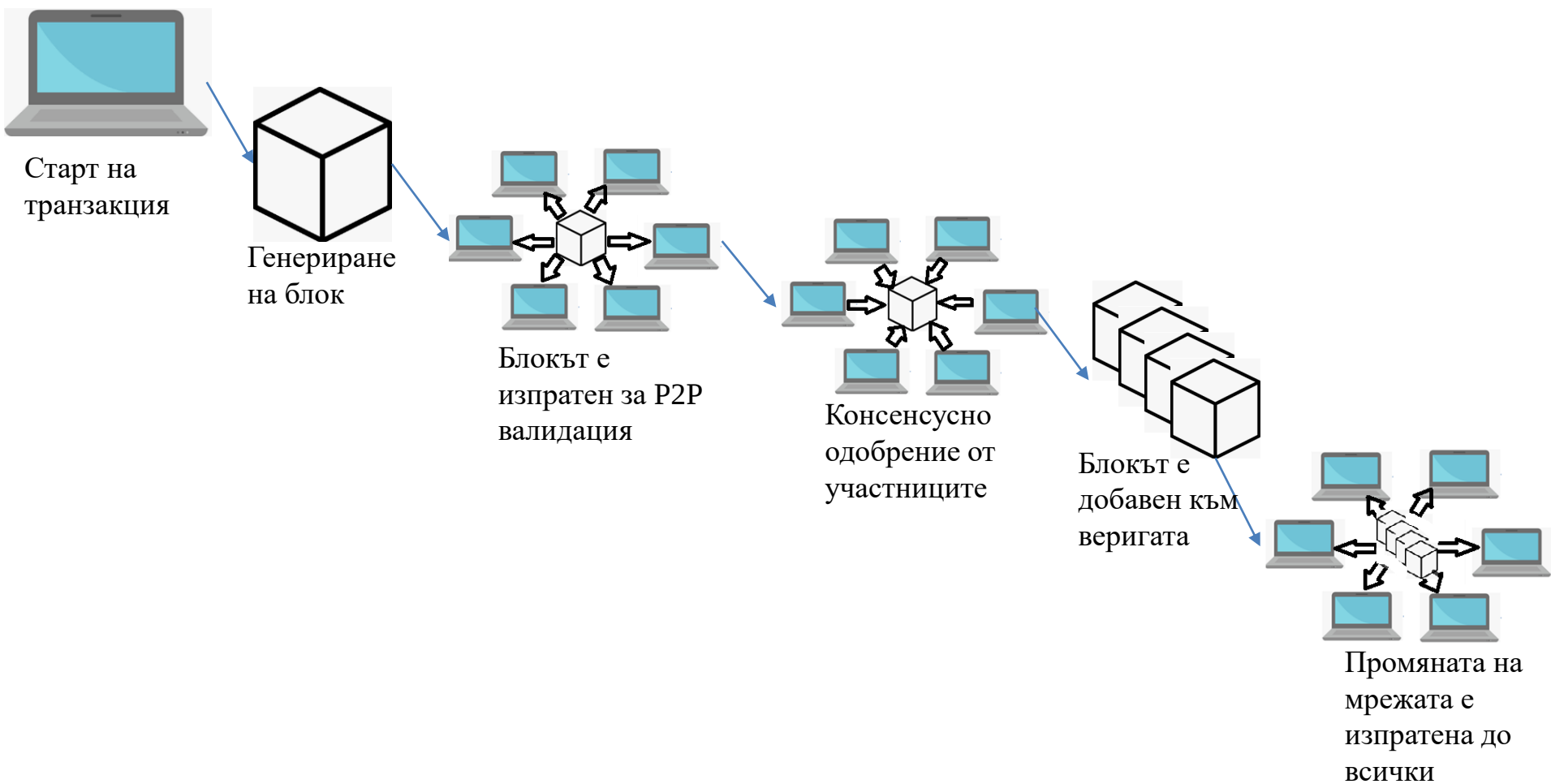
Абстрактен модел

Приложен слой	• Интерфейс за връзка с потребители • Бизнес логика • Интеграция на приложения
Слой за услуги	• Управление на събития, проследяване, оракули, портфейли • Цифрова идентификация • Разпределена БД • Умни договори • Разпределено съхранение на файлове
Мрежа и протоколи	• Permissionless • Permissioned • Консенсусни механизми за потвърждение
Инфраструктурен слой	• Nodes • Интернет мрежа • Виртуализация • Mining as a service

Алексиева - Абстрактен модел

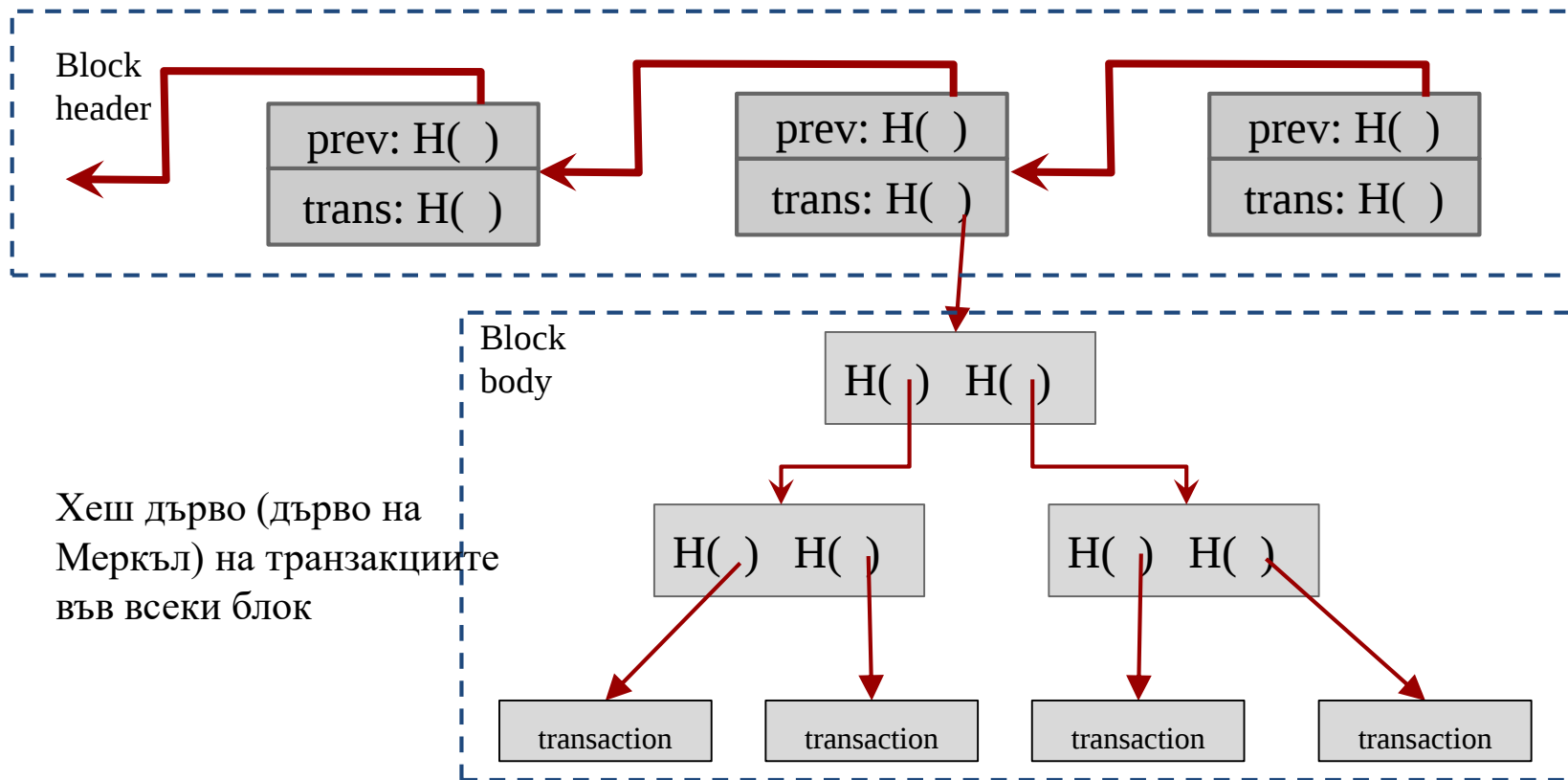


Добавяне на данни в блокчейна



Структура на блок

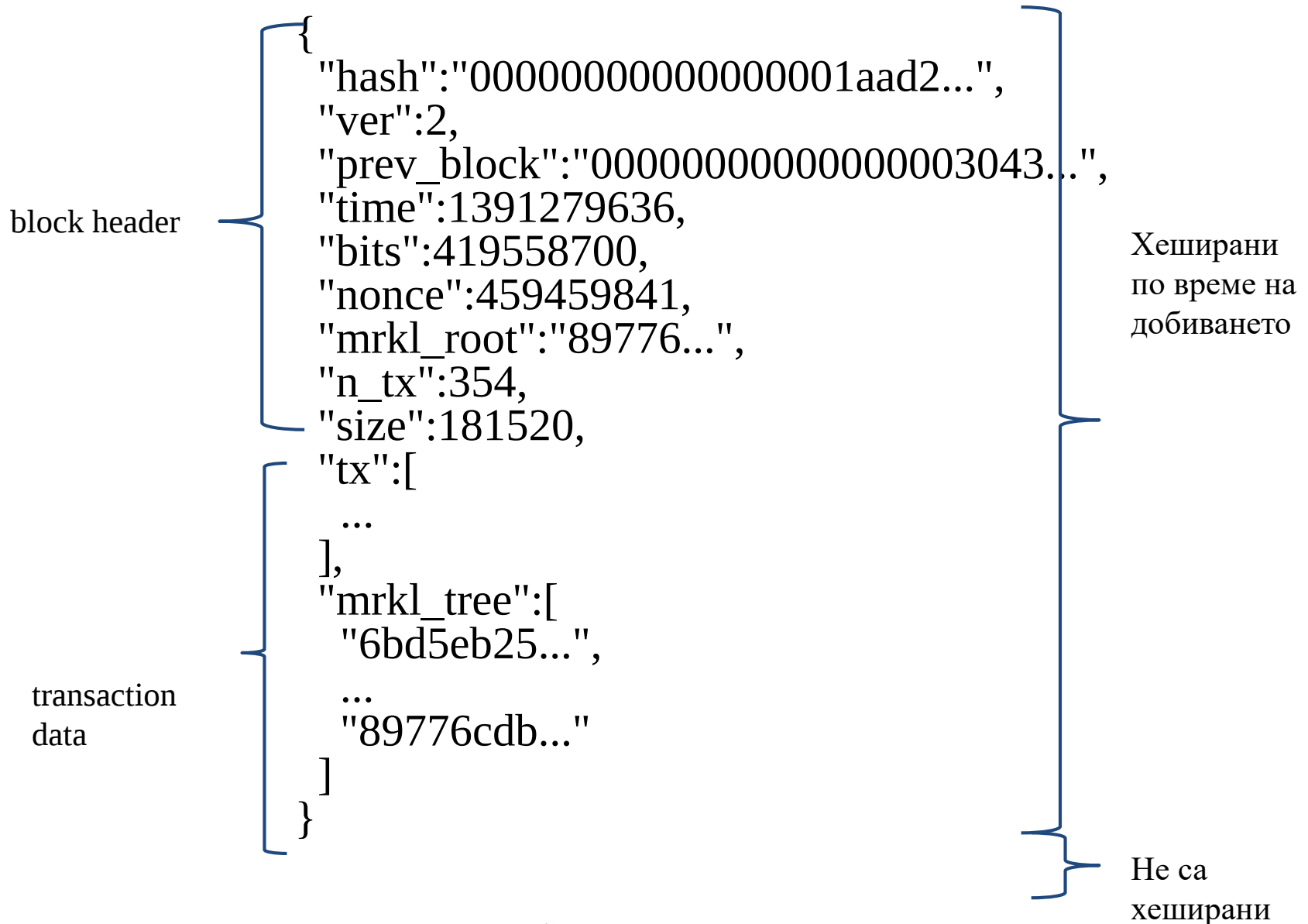
Hash chain of blocks



Хеш дърво (дърво на Меркъл) на транзакциите във всеки блок

- Блок – header и тяло. Съдържа подробности за транзакциите в дърво на Меркъл, хеша както на предишния, така и на текущия блок, и еднократен номер (nonce)
- Верига от блокове -блокове, свързани помежду си в хронологичен ред

Блок



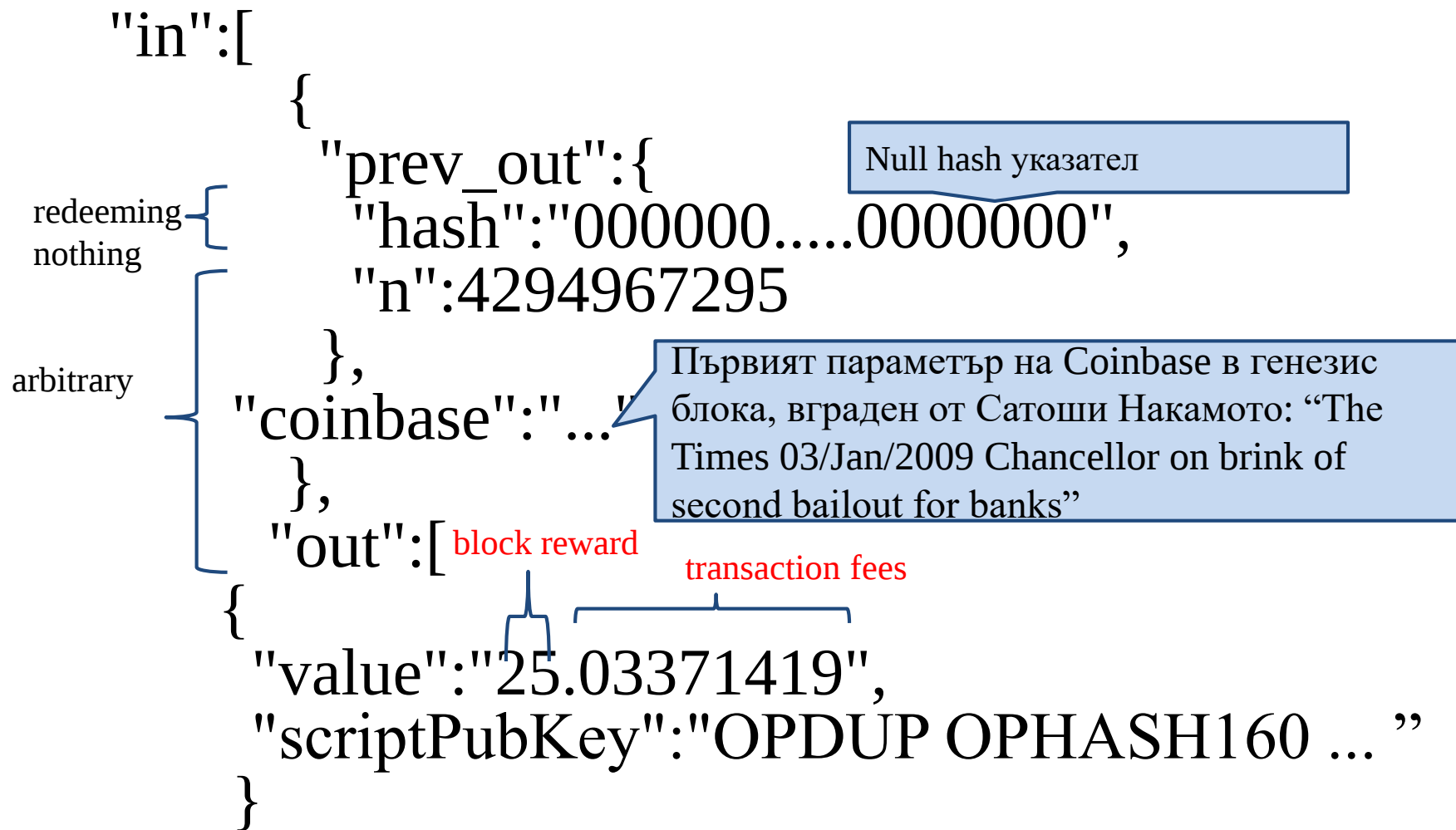
Блок

Добиване
(mining) → {
"hash":"000000000000000001aad2...",
"ver":2,
"prev_block":"000000000000000003043...",
"time":1391279636,
"bits":419558700,
пъзел → "nonce":459459841,
"mrkl_root":"89776...",
"n_tx":354,
"size":181520,
"tx":[
...
],
информация → "mrkl_tree":[
"6bd5eb25...",
...
"89776cdb..."
]
}

Coinbase транзакция

- Bitcoin емитира валута с добиване на блокове.
- Всеки блок започва със специална транзакция в coinbase, която генерира нови монети за този, който е добил блока.
- По-късните транзакции могат да харчат само пари, създадени от по-ранна coinbase – може да се проследи всяко плащане до блока, който е генерирал средствата.

Coinbase транзакция в блока



https://www.blockchain.com/explorer/transactions/btc

Blockchain

Home

Prices

Charts

SnapMarkets NEW

NFTs

DeFi

Prediction Markets

Academy

News

Developers

Wallet

Bitcoin

Ethereum

Solana

Search Blockchain, Transactions, Addresses, Prediction Markets and Blocks

Q

⚙

Sign In

Play

Gaming

TX

USD

Bitcoin Transaction

Broadcasted on 23 Jul 2026 04:53:10 GMT+3

Hash ID

3b482b285a4c4d0d007c5fc91b2d3a383c3ed9e0e17b86e774b7d7f81e9bc9a

Amount

0.00267814 BTC • \$173.72

Fee

209 SATS • \$0.14

From

bc1qu-hpuf2

To

2 Outputs

Pending

✓

This transaction is efficient, no issues detected.

Summary

This transaction was first broadcasted on the Bitcoin network on July 23, 2026 at 04:53 AM GMT+3. The transaction currently has 959,264 confirmations on the network. The current value of this transaction is now \$173.72.

Advanced Details

Hash	3b48-bc9a	Time	23 Jul 2026 04:53:10
Age	0m 12s	Inputs	2
Input Value	0.00268023 BTC	Outputs	2
	\$173.86	Output Value	0.00267814 BTC
Fee	0.00000209 BTC		\$173.72
	\$0.14	Fee/B	0.562 sat/B
Fee/VB	1.000 sat/vByte	Size	372 Bytes
Weight	834	Weight Unit	0.251 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1	BTC Price	\$64,867.50

Overview

JSON

From

1

bc1qu7dlmqwnvj7cvtlwj25uq8x99r4lsxpdqphpuf2

0.00002621 BTC • \$1.70

2

bc1qu7dlmqwnvj7cvtlwj25uq8x99r4lsxpdqphpuf2

0.00265402 BTC • \$172.16

To

1

bc1qpz8c783hnh8ta75mqare72jfa56szjvkcutv40

0.00265111 BTC • \$171.97

2

bc1qu7dlmqwnvj7cvtlwj25uq8x99r4lsxpdqphpuf2

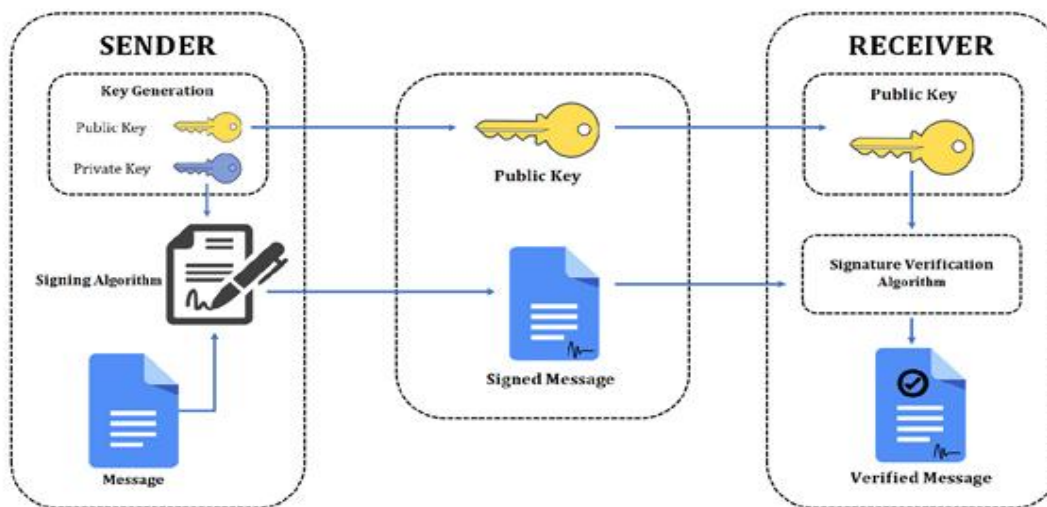
0.00002703 BTC • \$1.75

9/1/2026

проф. д-р инж. Венета Алексиева

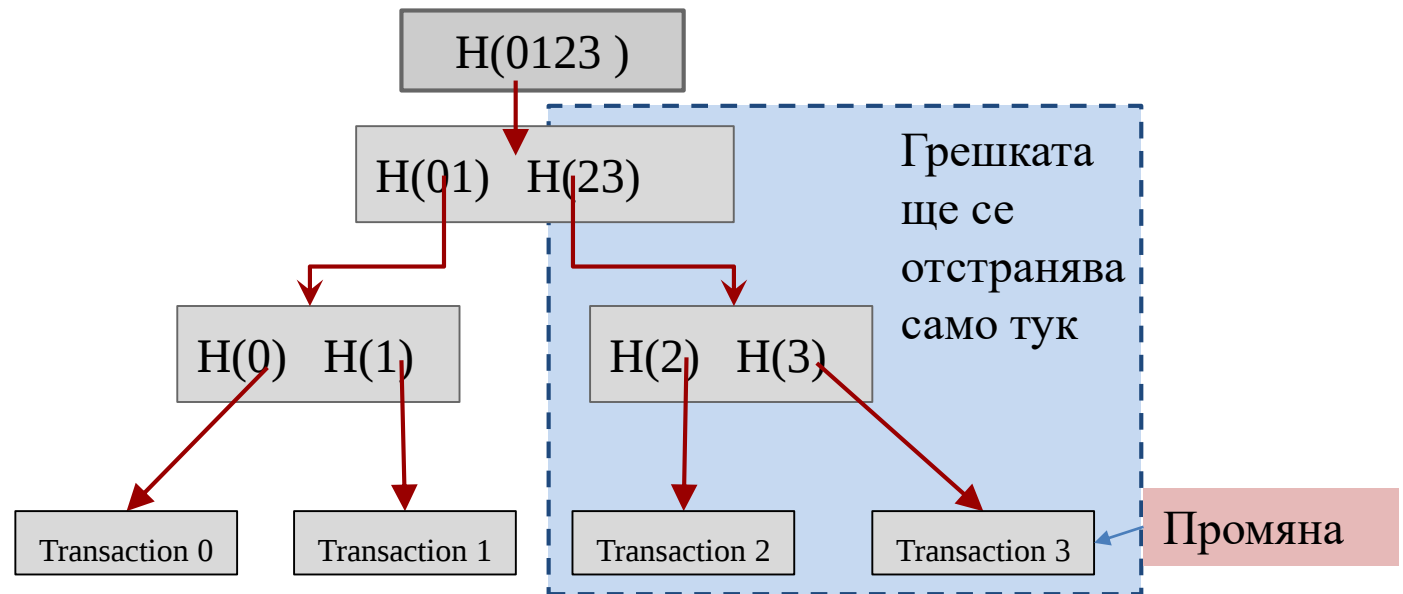
15

Процес на проверка на транзакцията



- Криптографският **Public-key** е асиметричен механизъм за криптиране, използван за гарантиране на автентичността и сигурността на данните в блокчейн мрежа.
- Всеки възел притежава двойка криптографски ключове: частен ключ, който е достъпен само за неговия собственик, и публичен ключ, който е свободно достъпен в мрежата.
- Когато данните се предават, те се криптират с помощта на публичния ключ на получателя, което гарантира, че само получателят може да ги декриптира със своя частен ключ.
- Транзакцията се счита за валидна само след като е подписана цифрово от подателя, използвайки неговия частен ключ.
- Наистина добита транзакция е необратима.

Дърво на Меркъл



- Дървото на Меркъл е структура от данни, използвана за съхраняване на хешираното съдържание на блок по йерархичен начин, опростявайки проверката на данните.
- Повишава ефективността, като ограничава процеса на отстраняване на грешки до засегнатия клон, вместо да изисква проверка на целия набор от данни.

Хеширане

- Чрез криптографска *хеш* функция, базирана на математически алгоритъм, входните данни се преобразуват в изходен низ с фиксирана дължина, наричан *хеш*, *хеш стойност* или *цифров подпис*.
- Характеристики на хеш функция :
 - хеш стойността се генерира лесно;
 - декриптирането (т.е. възстановяването на оригиналните входни данни на база на хеша) е невъзможно;
 - не е възможно за различни входни данни да се получи еднаква хеш стойност.
- Например в блокчейна на биткойн се използва SHA- 256 (*Secure Hesh Algoritm 256 – bit*), който генерира 256 – битова (32 байта) хеш стойност. Тя се представя като шестнадесетично число, състоящо се от 64 цифри.

Хеш функция

- Хеш функцията е математическа трансформация на входни данни с произволна дължина в кратък уникален низ с фиксирана дължина.
- Анализът на хеш функциите се използва за проверка на целостта на важни файлове от операционна система, програми, данни.
- Алгоритъмът за хеширане е еднопосочен - не трябва да има математическа възможност за определяне на първоначалните данни от резултата.
- Резултатът от хеширане се нарича хеш, хеш код, дайджър на съобщението.

Хеширане с SHA-256

- **SHA-256** е един от най-сигурните и широко използвани криптографски алгоритми за хеширане в света, разработен от Агенцията за национална сигурност на САЩ (NSA)
- **SHA-256** преобразува всякакви входни данни в уникален **256-битов низ** (представен като 64 шестнадесетични символа)
- Използва се в:
 - Биткойн мрежата за Proof of Work и свързване на блоковете,
 - SSL сертификати / цифрови подписи
 - Проверка за модификация на файлове
 - защита на пароли

SHA-256 в Linux

- Linux има вграден инструмент `sha256sum` в почти всяка дистрибуция:
 - Хеширане на файл: `sha256sum text.txt`
 - Хеширане на текст директно в терминала: `echo -n „тук_е_текста“ | sha256sum`
- Windows има вграден инструмент `CertUtil` през командния ред или PowerShell:
 - Хеширане на файл през PowerShell:
`Get-FileHash text.txt -Algorithm SHA256`
 - Хеширане на текст директно през PowerShell:
`[System.Security.Cryptography.SHA256]::Create().ComputeHash([System.Text.Encoding]::UTF8.GetBytes("тук_е_текста")) |
ForEach-Object { "{0:x2}" -f $_ } |
Write-Host -NoNewline`

Пример

hello се хешира с SHA-256 в:

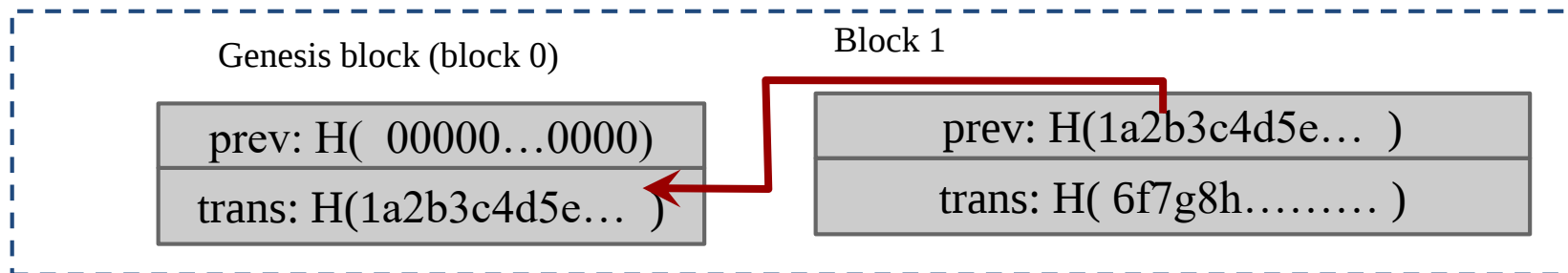
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1
fa7425e73043362938b9824

Technical University of Varna се хешира с
SHA-256 в:

90da3ee22bca315e15a04ce762a9bb12ed37c4eab
15684ef21b86ed52caf546a

Пример при блокчейн

Hash chain of blocks



- **Промяната в данните** на Блок 1 веднага ще смени неговия сегашен хеш от **6f7g8h...** на нещо съвсем различно, например **9a9b9c99999...**
- **Разкъсване на веригата** при несанкционирана промяна на съдържанието на съобщението в Блок 1, блок 2 ще стане невалиден, защото неговото поле „Хеш на предишния блок“ (prev: H) все още ще изисква 6f7g8h..., а Блок 1 вече има друг хеш.
- **Защита на мрежата:** Тъй като тази база данни се пази едновременно на хиляди компютри по света (nodes), останалите компютри веднага ще забележат разминаването в Блок 1 и Блок 2 и ще отхвърлят фалшификацията на хакера.

И отново...

- Транзакции
 - кой на кого плаща и колко
- Промяна на плащане на един пиър
 - цялата му верига се прекъсва от този блок нататък и копието му вече не съвпада с останалите пиъри
- Защита на мрежата
 - Еднакви копия при всички пиъри

The image displays a simulation of a blockchain network with three peers, labeled Peer A, Peer B, and Peer C. Each peer's interface shows a list of transactions (TX) and a block of data (BLOCK). The transactions are as follows:

- Peer A:**
 - TX 1: \$10.10, Kitty → Elizabeth
 - TX 2: \$62.19, Darcy → Wickham
- Peer B:**
 - TX 1: \$8.44, Mazy → Jane
 - TX 2: \$14.00, Elizabeth → Darcy
 - TX 3: \$31.75, Bingley → Lydia
- Peer C:**
 - TX 1: \$12.00, Lydia → Kitty
 - TX 2: \$9.87, Jane → Mazy

The block data for each peer is as follows:

- Peer A:**
 - BLOCK # 3
 - NONCE: 26233
 - PREV: 000035e7a10003bde764cb5956f24aa9f32b577ea0c3a77bc915d7298c4d86ea
 - HA SH: 00004a212d121143680a3f6187fac95bfc65eae51ecf5e07a0d3fca842a5907
- Peer B:**
 - BLOCK # 4
 - NONCE: 29596
 - PREV: 00004a212d121143680a3f6187fac95bfc65eae51ecf5e07a0d3fca842a5907
 - HA SH: 0000126efc8d1e03c4c1df0d3309e263a7824f27076af8045a063ebb21466c25
- Peer C:**
 - BLOCK # 5
 - NONCE: 1274
 - PREV: 0000126efc8d1e03c4c1df0d3309e263a7824f27076af8045a063ebb21466c25
 - HA SH: 000055cf934263128068ff91add6a9dcabc24ba6049dd1843efb40438e124c38

Добиване(mining) на bitcoin

- Създават се като възнаграждение за извършена изчислителна работа по криптиране.
- При всеки успешно преминат етап на изчисление на масив от големи числа (хеширане) се получават по 25 биткойна. Участниците в изчисленията обаче обикновено са повече от един и биткойните се делят помежду им, в зависимост от тяхното участие.
- Популярни програми за добив са: CGminer и BFGminer.

Транзакция

- Хеш – Цялата транзакция е събрана в един низ и за да е уникална, се използва хеш-функция
- Входове – Адрес/и (публичен ключ, а не IP адрес), от които е получена сумата, използвана в транзакцията.
- Изходи – Адрес/и (публичен ключ, а не IP адрес), към които е пратена сумата, използвана в транзакцията.
- Електронен подпис – Създаден е от частния ключ на изпращащия, за да го автентичира.
- Такса – Количество пратено към „копача“, който е преработил транзакцията.
- Не е задължително да има само един изпращач или един получател в една транзакция.

Копач

Копачът потвърждава на транзакцията:

- „копачът“ проверява електронния подпис закачен към транзакцията.
- Ако транзакцията е валидна, копачът я записва в „блок“, заедно с други получени и валидни транзакции. Той прибавя този блок към блокчейна, след последния „изкопан“ блок.
- Транзакцията се счита за потвърдена веднъж, след като е прибавена в „блок“.
- “Копачът” за да създаде блок, той освен да прибави валидни транзакции, трябва и да реши даден математически проблем.

Решаване на математически проблем

- Биткойн ползва SHA-256 хеш-функция, за да създаде този математически проблем.
- Изисква се копачът да създаде хеш с определен брой нули в началото.
- Това отнема много време, дори с мощен хардуер и е по-лесно за решаване с повече и по-мощни машини, които извършват повече опити за по-малко време.
- Ако се включат твърде много „копачи“, системата се настройва сама така, че изчисленията да стават по-трудни.

Възнаграждение

- Копачите биват възнаградени, когато създадат блок.
- Наградата се разпределя между всички копачи на блока.
- Целта е да не може един копач с много мощни машини да изкопае всичката криптовалута сам.

Bitcoin портфейл

- Bitcoin портфейлът е съвкупност от множество биткойн адреси, в които може да се съхраняват различни баланси от биткойни.
- Bitcoin портфейлите са софтуерни програми, които дават възможност за лесно управление на биткойни, без да е необходимо техническо познаване на биткойн протокола.
- Потребителите могат да се сдобиват с нови bitcoin адреси, които се съхраняват в портфейл с линкове към криптографски пароли или „частни ключове“, които осигуряват достъп до трансфер на биткойни
- За всеки потребител, който си инсталира BitCoin софтуера, се генерира виртуален портфейл.

Въпроси ?

Благодаря за вниманието !