Тема 1. Огляд технології блокчейн
Лекція 5.

Навчальні питання:

Блоки

1 Структура блокчейн реєстру Bitcoin

2 Магічне число (Magic_no)

3 Зв’язування блоків (prev_block)

4 Дерево Меркле (merkle_root)

4.1 Побудова дерева Меркле

4.2 Для чого потрібні геш-дерева

4.3 Аналоги дерев Меркле

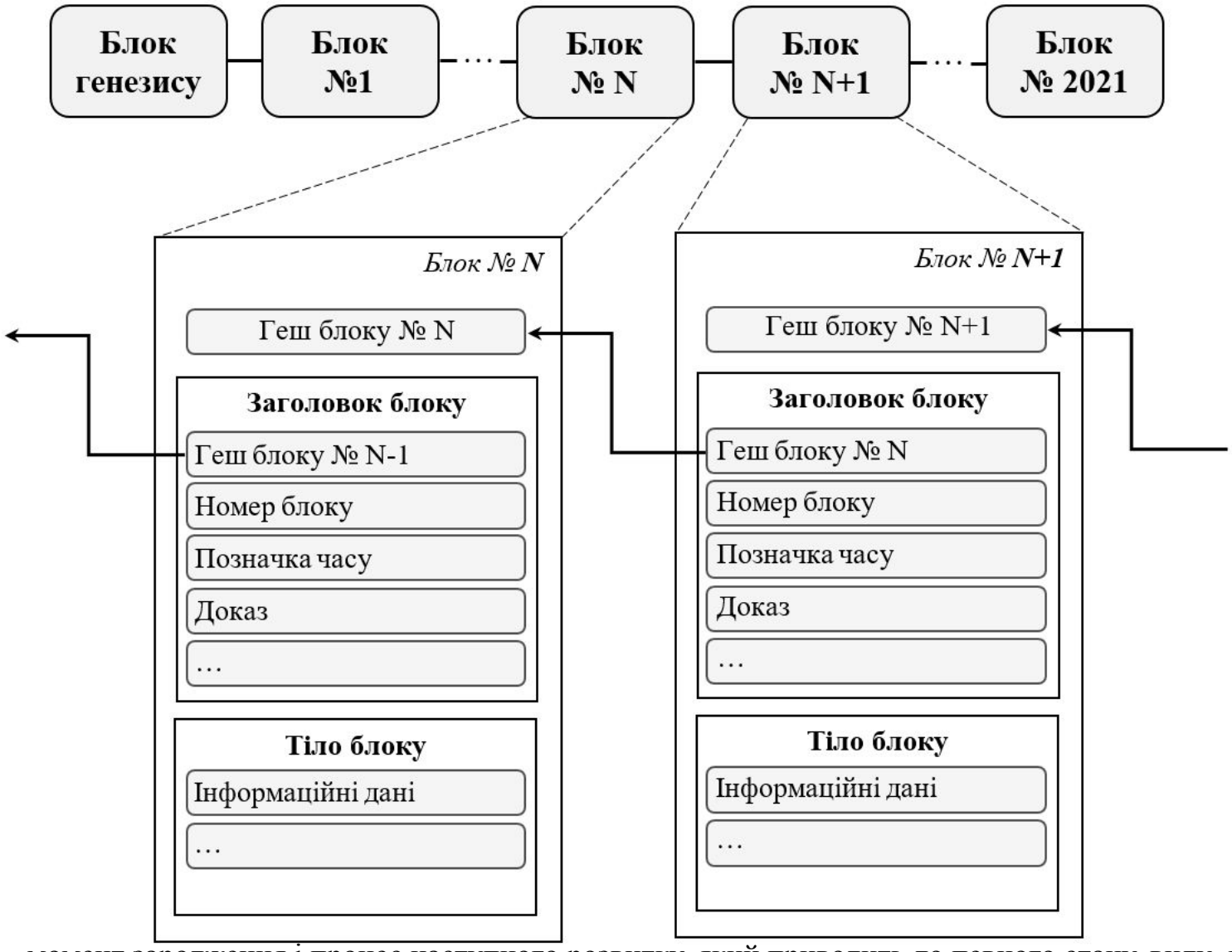
5 Позначка часу (timestamp)

6 Криптографічний одноразовий номер (Nonce)

7 Приклад записів блоків у мережі Біткойн

8 Валідація нового блоку

Узагальнена структура ланцюжку блоків блокчейн систем



Генезис – момент зародження і процес наступного розвитку, який приводить до певного стану, виду, явища. Синоніми: виникнення, походження, зародження. Походить від лат. genesis, далі від грец. γένεσις «народження»

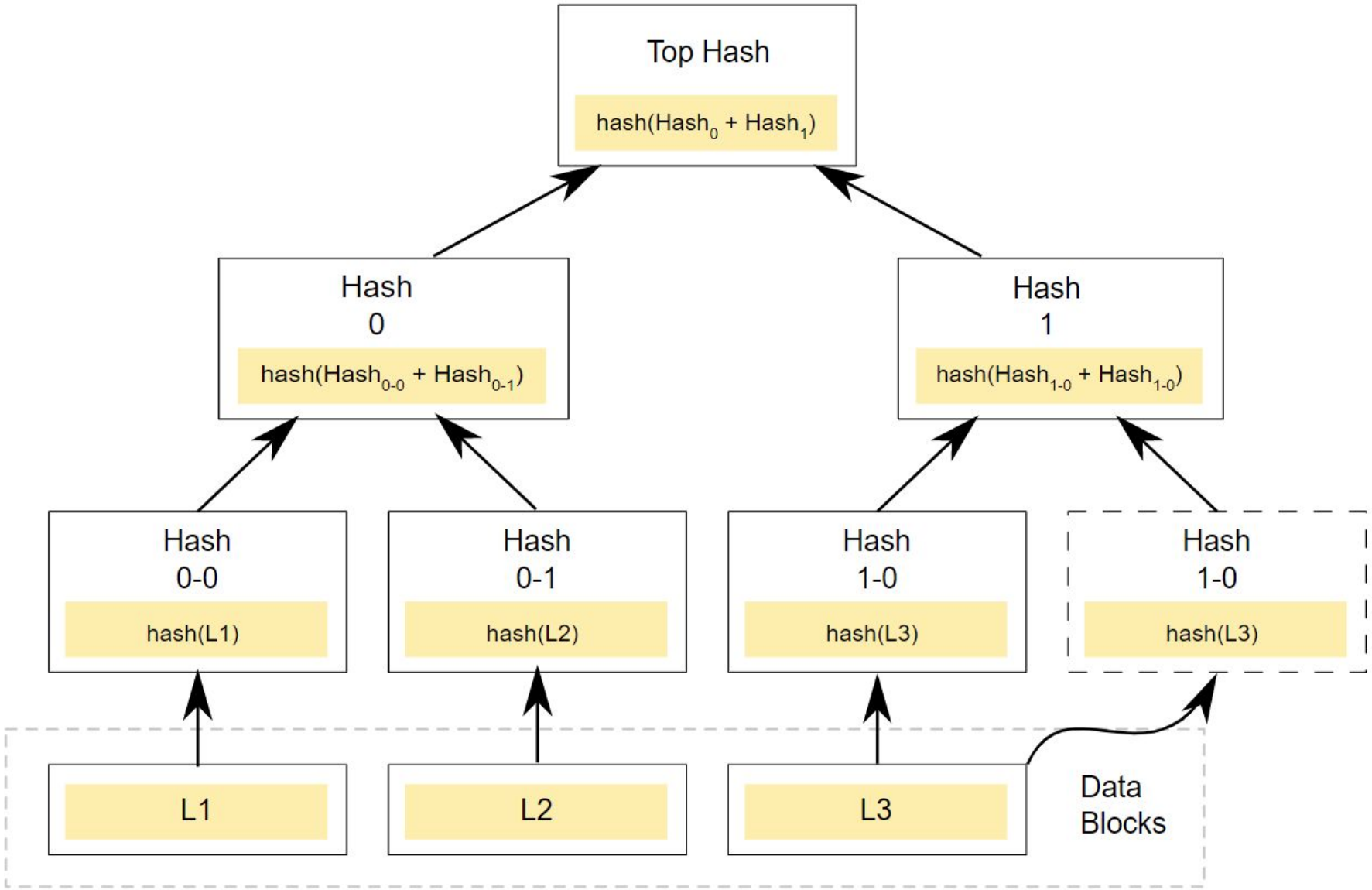
Будова блоку Bitcoin

Розмір поля (в байтах)	Опис	Коментарі
4	Magic_no	Магічне число, значення завжди дорівнює 0xD9B4BEF9
4	Block_size	Розмір блоку, зазначається число наступних байтів, що залишилися до кінця блоку
80	block_header	Заголовок блоку, складається з 6-ти компонентів
1+	txn_count	Число транзакцій в блоці (може приймати 8-, 16-, 32- і 64-бітове значення)
	txns	Список транзакцій в блоці

Заголовок блоку Bitcoin

Розмір поля (в байтах)	Опис	Тип даних	Коментарі
4	version	int32_t	Інформація про версію блоку
32	prev_block	char[32]	256-бітове значення хешу попереднього блоку, на який посилається даний блок
32	merkle_root	char[32]	256-бітове значення хешу підстави дерева Меркле, який є хешем всіх транзакцій, пов'язаних з цим блоком.
4	timestamp	uint32_t	Запис мітки часу створення блоку записаного в Unix форматі (в секундах з 1970-01-01T00: 00 UTC)
4	bits	uint32_t	Розрахована цільова складність використовується для цього блоку
4	nonce	uint32_t	32-бітове випадкове число, що використовується для генерації даного блоку

Дерево Меркле або геш-дерево



Позначка часу (time-stamp)

Позначка часу – цифрові дані в блокчейн системі, які пов'язують інші цифрові дані з конкретним періодом часу, встановлюючи свідоцтво того, що останні дані існували в певний момент часу. Крім того, для деяких алгоритмів консенсусу, позначка часу необхідна для визначення цільової складності, що дозволяє проводити регулювання виробництва блоків.

Позначки часу в блоках у блокчейн системах не зовсім точні. Наприклад, «позначка часу біткоінів можуть відрізнятися в годинах від часу, підтримуваного учасниками (вузлами) біткоінів, і теоретично можуть радикально відрізнятися від фактичного часу (тобто часу поза мережею біткоінів)».

Для мережі Біткойна, позначка часу може коливаються від мінімального значення (середнє значення між останніми 11 блоками, тобто у середньому менш на 35 хвилин від поточного часу) та максимально допустимого значення (2 години від поточного мережевого або системного часу) та не є гарантованим часом створення блоку.

Принцип відрізняється від рішень для цифрової позначки часу без блокчейна, де позначки часу блокчейна точні.

Позначка часу (timestamp)

Час формування перших 30 блоків мережі Біткойн

Номер блоку	Час формування (секунди)	Номер блоку	Час формування (секунди)	Номер блоку	Час формування (секунди)
1	463160	11	408	21	558
2	79	12	528	22	914
3	429	13	132	23	144
4	815	14	569	24	666
5	440	15	87157	25	369
6	361	16	12	26	1804
7	580	17	1033	27	123
8	374	18	543	28	30884
9	536	19	640	29	46
10	673	20	1021	30	619

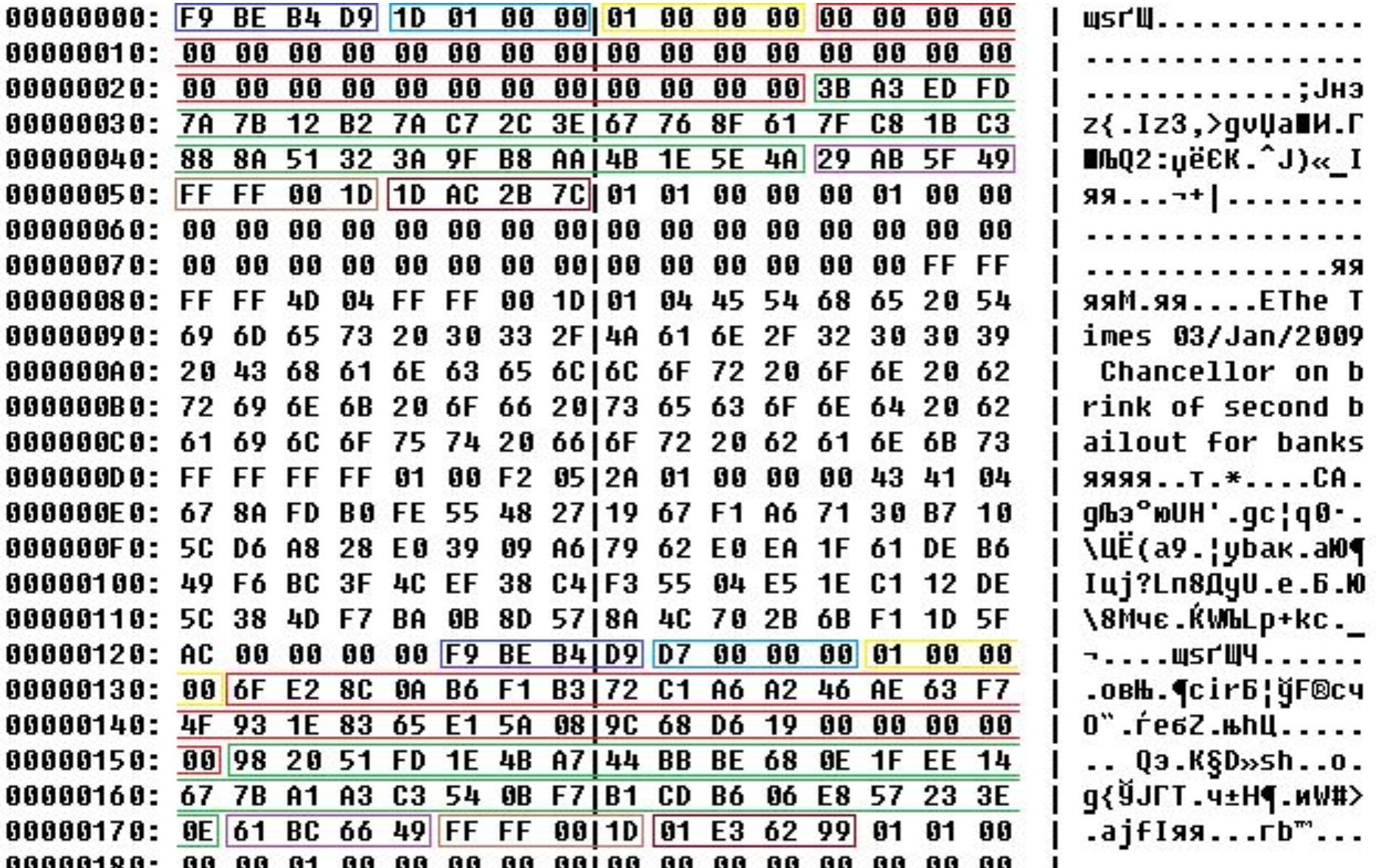
Криптографічний одноразовий номер (Nonce)

Криптографічний nonce (англ. nonce — «number that can only be used once» – число, яке може бути використано один раз) – це довільне число. Криптографічний nonce може бути об'єднаний з даними для створення різних геш-значень для кожного nonce:

$$hash(дані + nonce) = геш - значення$$

Тільки змінення значення одноразового номера забезпечує механізм отримання різних геш-значень при збереженні незмінними самих даних. Цей метод найбільш часто використовується в моделях консенсусу, заснованих на доказі виконаної роботи.

Фрагмент файлу «blk00000.dat» містить реєстр блокчейн Bitcoin



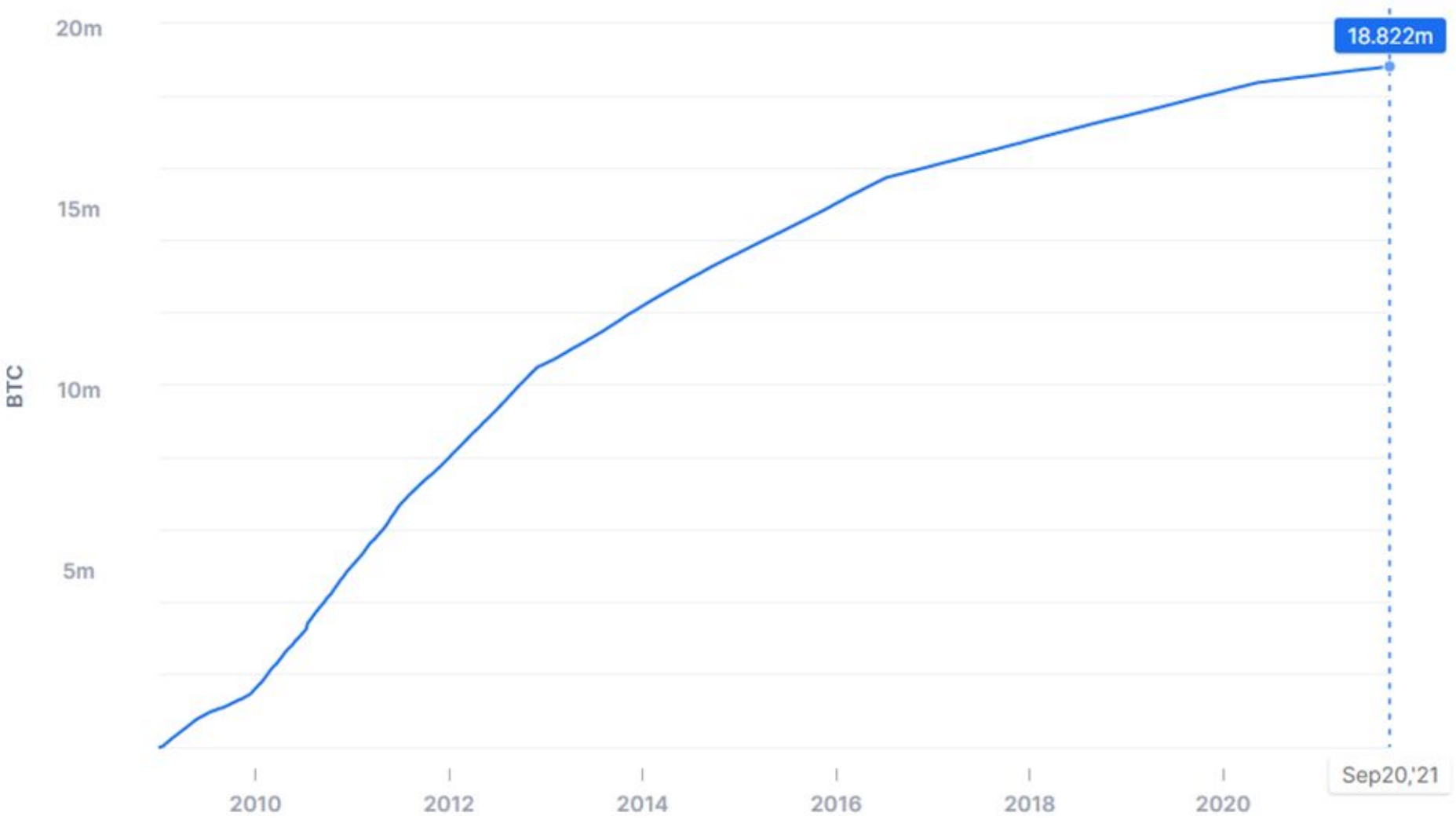
Валідація нового блоку

Коли вузол отримує новий блок, він перевіряє його по списку критеріїв, в разі незадоволення хоча б одного критерія блок відкидається. Для мережі Bitcoin ці критерії можна побачити в клієнті Bitcoin Core.

Перевірки можуть включати в себе (можлива зміна набору тестів при різних версіях):

- Геш заголовка блоку менше, ніж цільова складність.
- Структура блоку даних синтаксично правильна.
- Розмір блоку знаходиться в допустимих межах.
- Перша транзакція (і тільки перша) – це coinbase-транзакція.
- Позначка часу блоку знаходиться у заданому інтервалі часу.
- Усі транзакції усередині блоку проходять валідацію.

Загальна кількість здобутих біткойнів, які циркулюють в мережі



Скріншот з Bitnodes (https://www.blockchain.com/charts/total-bitcoins)

Розмір нагороди (BTC) за блок мережі Біткойн

Рік	Нагорода	Рік	Нагорода	Рік	Нагорода
2009	50	2056	0,01220703	2104	0,00000298
2012	25	2060	0,00610352	2108	0,00000149
2016	12,5	2064	0,00305176	2112	0,00000075
2020	6,25	2068	0,00152588	2116	0,00000037
2024	3,125	2072	0,00076294	2120	0,00000019
2028	1,5625	2076	0,00038147	2124	0,00000009
2032	0,78125	2080	0,00019073	2128	0,00000005
2036	0,390625	2084	0,00009537	2132	0,00000002
2040	0,1953125	2088	0,00004768	2136	0,00000001
2044	0,09765625	2092	0,00002384	2140	0,00000000
2048	0,04882813	2096	0,00001192		
2052	0,02441406	2100	0,00000596		