

# ЕКЗАМЕН

## ЗАВДАННЯ 1.

### 1. Створив клас `public class PenaltyStakingContract : ISmartContract`

- контракт створений для демонстрації логіки Proof-of-Stake.
- користувач може «заморозити» свої токени на певний період.
- на період «заморозки» токенів користувач отримує винагороду за кожний новий блок.
- користувач може повернути свої токени з **винагородою** після того як пройде період «заморозки».
- користувач може повернути свої токени зі **штрафом** до того як пройде період «заморозки».

### 2. Транзакція з контракту → користувача:

- визначає, скільки блоків користувач тримав депозит;
- якщо блоків достатньо: повертає `principal + reward`;
- якщо блоків недостатньо: застосовує штраф `earlyPenaltyPercent` та зменшує суму, яку користувач отримає;
- перевіряє, що користувач не може вивести більше, ніж дозволено;
- у разі порушення — транзакція відхиляється (`return false`).

### 3. Інтегрував контракт у `BlockChainService`

- зареєстрував окремий гаманець для контракту (адреса + приватний ключ).
- додав екземпляр `PenaltyStakingContract` у словник `Contracts`.
- у `CreateTransaction(...)` додав виклики `ValidateTransaction` для:
  - \* `FromAddress`
  - \* `ToAddress`
- Якщо будь-який контракт повертає `false` — транзакція не потрапляє у `Mempool`.

## ЗАВДАННЯ 2.

### 1. Додав відображення адреси `PenaltyStaking`-контракту

### 2. Реалізував дві UI-форми:

#### Форма «Покласти у `PenaltyStaking`»

- Поля: `FromAddress`, `Amount`, `Fee`, `PrivateKey`.
- Створює транзакцію:
  - `FromAddress` = користувач
  - `ToAddress` = `PenaltyStakingContract`
- Транзакція підписується приватним ключем користувача.

#### Форма «Вивести з `PenaltyStaking`»

- Поля: `UserAddress`, `Amount`.
- Створює транзакцію:
  - `FromAddress` = `PenaltyStakingContract`
  - `ToAddress` = користувач
- Підпис виконується приватним ключем контрактного гаманця, який зберігається на сервері.

### 3. Відобразив у таблиці транзакцій для кожного блоку транзакцій, де бере участь `PenaltyStaking`-контракт;

- Додаткову колонку: "Stake" — депозит / "Unstake" — виведення

### ЗАВДАННЯ 3.

1. Реалізував окрему таблицю, яка показує \*\*стан PenaltyStaking-контракту\*\*. Для кожного користувача:

- Адреса стейкера
- Блок початку стейкінгу
- Загальна застейкана сума
- Винагорода, яка обчислюється після кожного нового блоку
- Можливий штраф за досркове зняття коштів зі стейкінгу
- Можливу суму доступну до виводу
- Скільки блоків минуло / залишилось
- Статус виводу

### Практичне застосування:

1. Для «заморозки» своїх токенів User\_A заповнює таблицю «Staking» та відправляє транзакцію в мемпул на суму 10 токенів з комісією 1 токен:

The screenshot shows a web-based blockchain application interface. At the top, there's a header bar with tabs for 'Index - Block\_Chain'. Below the header, a green bar indicates the current node is 'Node A'. There are several buttons at the top: 'START DEMO', '<RSAKeyValue><Modulus>', 'START MINE', 'Difficu', and 'Задати'. A message in a green box says 'Блок # 11 розповсюджено. Прийняли: 2 вузли з 3.'

The main area has two sections:

- Register Wallet:** A table showing wallet details:

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
<a href="#">ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3</a>	<a href="#">Copy addr</a>	(Contract)	0	<RSAKeyValue>	2025-11-19 02:37:15Z
<a href="#">ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817</a>	<a href="#">Copy addr</a>	User_A	11,00000	<RSAKeyValue>	2025-11-19 02:37:56Z
- Penalty Staking:** A form for staking tokens:

Адреса смарт-контракту для стейкінгу: <a href="#">ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3</a>	<b>Покласти у стейкінг</b>	<b>Вивести зі стейкінгу</b>
From Address: <input type="text" value="ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817"/>	Address (ADDR...): <input type="text"/>	Amount: <input type="text"/>
Amount: <input type="text" value="10"/>	Fee: <input type="text" value="1"/>	<a href="#">Withdraw</a>
Private Key: <RSAKeyValue><Modulus>9Xt5HOh7ndNW1Twnsym22Pv4895NUDrILPqOMIDft+A		
<b>Stake</b>		

## 2. Після додавання транзакції в мемпул та майнінгу:

- з User\_A списується 10 токенів
- на адресу Контракту зараховується 10 токенів.

### У таблиці транзакцій для кожного блоку, де бере участь PenaltyStaking-контракт:

- Додав колонку: "Stake" — депозит / "Unstake" — виведення

**Index - Block\_Chain**

localhost:7146/?nodeId=A

Block\_Chain Home Search

Public key => <RSAKeyValue> <Modulus>9Xt5HOh  
 7ndNW1Twnsyn22Pv <Modulus>9Xt5HOh  
 4895NUDrLpQOMIDf 7ndNW1Twnsyn22Pv

Valid Chain => True  
 Difficulty => 1  
 Reward => 1,0

Копіювати ключ  
 Поточний вузол: Node A ▾ Переключити

START DEMO <RSAKeyValue><Modulus> START MINE Dificu Задати

Блок # 12 розповсюджене. Прийняли: 2 вузли з 3.

**Register Wallet**

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
<a href="#">ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3</a>	<a href="#">Copy addr</a>	(Contract)	10,00000	<RSAKeyValue>	2025-11-19 02:37:15Z
<a href="#">ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817</a>	<a href="#">Copy addr</a>	User_A	2,00000	<RSAKeyValue>	2025-11-19 02:37:56Z

**Mem pool**

From Address (ADDR_...)	To Address (ADDR_...)	Amount	Fee	Private key	note
<a href="#">Добавити у мемпул</a>					

Транзакцій немає

Index	Nonce	MiningDurationMs	PrevHash	Hash	Timestamp	Signature	Статус підпису	
0	6	0		0335235E8261...	01 січня 2025 р., 00:00:00		валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
1	8	0	0335235E8261...	06D5038AD551...	19 листопада 2025 р., 02:37:57	pkjujh!Slooe...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
2	11	0	06D5038AD551...	0A0DA698E2EE...	19 листопада 2025 р., 02:37:58	jyoxA8RIG+KZ...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
3	16	0	0A0DA698E2EE...	00598FF5B991...	19 листопада 2025 р., 02:37:59	zGEHuGTyoNsV...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
4	21	0	00598FF5B991...	0C9B9BDB74EF...	19 листопада 2025 р., 02:38:00	laicHbR6Lfp...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
5	37	0	0C9B9BDB74EF...	01332AA42B9B...	19 листопада 2025 р., 02:38:00	RmvkoJaA0Vfv...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
6	22	0	01332AA42B9B...	04FE21819E14...	19 листопада 2025 р., 02:38:01	1nrg61BZJ/Vo...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
7	2	0	04FE21819E14...	0012F5DBC123...	19 листопада 2025 р., 02:38:02	SvtBMMaQ8kTO...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
8	7	0	0012F5DBC123...	0F7AA24617B7...	19 листопада 2025 р., 02:38:02	UCBnAoIh86U0...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
9	38	0	0F7AA24617B7...	035F8E29E427...	19 листопада 2025 р., 02:38:02	L9RhxGkDrDXi...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
10	27	0	035F8E29E427...	0BBFC93E7D3D...	19 листопада 2025 р., 02:38:03	Cx1tGp7HRKPS...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
11	24	0	0BBFC93E7D3D...	0EBB24F7027E...	19 листопада 2025 р., 02:38:04	26hNVSDzB2LW...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>
12	3	0	0EBB24F7027E...	0BAAD9A71766...	19 листопада 2025 р., 02:40:30	q4Vlk1ki6zOc...	валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>

FromAddress	ToAddress	Amount	Fee	Stake/Unstake	Note	Confirmations
COINBASE	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	2,00000	0			
ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3	10,00000	1	Stake	Stake tokens	0

The diagram illustrates the token flow process. It starts with a yellow arrow pointing down from the wallet table to the mempool table, indicating tokens being added to the mempool. From there, another yellow arrow points up to the contract table, indicating tokens being deposited into the contract. Red arrows also point from the wallet table to the mempool table and from the mempool table to the contract table, further detailing the transaction flow between these components.

**3. На адресі смарт-контракту «заморожується» 10 токетів користувача User\_A до того часу коли буде добуто блок № 32. Якщо намагатися вивести токени прямо зараз, то транзакція потрапляє в мемпул зі штрафом:**

The screenshot shows the 'Penalty Staking' interface. At the top, there's a table of existing staking entries:

Address	Name	Amount	PublicKey	RegisteredAt
ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3	(Contract)	10,00000	<RSAKeyVal	2025-11-19 02:37:15Z
ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	User_A	2,00000	<RSAKeyVal	2025-11-19 02:37:56Z

Below this is the 'Penalty Staking' form:

**Penalty Staking**

Адреса смарт-контракту для стейкінгу:  
ADDR\_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3

**Покласти у стейкінг**

From Address: ADDR\_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3

Amount: 1d

Fee: 0

Private Key: (input field)

**Вивести зі стейкінгу**

Address (Одержанувач): ADDR\_5DBE943C27845D421A1979DE56A1FAC62CF9B817

Amount: 1d

Fee: 0

Private Key: (input field)

**Stake**

**Mem pool**

From Address (ADDR...): ADDR\_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3

To Address (ADDR...): ADDR\_5DBE943C27845D421A1979DE56A1FAC62CF9B817

Amount: 8,00200

Fee: 0

Private key: (input field)

Note: Withdraw from staking

The screenshot shows the 'Mem pool' page. At the top, there's a form to add a new transaction:

Private Key: (input field)

**Stake**

Below this is the 'Mem pool' table:

**Mem pool**

From Address	To Address	Amount	Fee	Note
ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	8,00200	0	Withdraw from staking

Below the table is a detailed view of the transaction:

Index	Nonce	MiningDurationMs	PrevHash	Hash	Timestamp	Signature	Статус підпису	Edit	Транзакції
0	6	0		0335235E8261...	01 січня 2025 р., 00:00:00		валідний	Edit	Транзакції
1	8	0	0335235E8261...	06D5038AD551...	19 листопада 2025 р., 02:37:57	pkjujh!Sloee...	валідний	Edit	Транзакції
2	11	0	06D5038AD551...	0A0DA698E2EE...	19 листопада 2025 р., 02:37:58	jyxoA8RIG+KZ...	валідний	Edit	Транзакції
3	16	0	0A0DA698E2EE...	00598FF5B991...	19 листопада 2025 р., 02:37:59	zGEHuGTyoNsV...	валідний	Edit	Транзакції
4	21	0	00598FF5B991...	0C9B9BD74EF...	19 листопада 2025 р., 02:38:00	laicHbR6Lff...	валідний	Edit	Транзакції
5	37	0	0C9B9BD74EF...	01332AA42B9B...	19 листопада 2025 р., 02:38:00	RmvkoJa0Vfv...	валідний	Edit	Транзакції
6	22	0	01332AA42B9B...	04FE21819E14...	19 листопада 2025 р., 02:38:01	InrG618ZJ/Vo...	валідний	Edit	Транзакції
7	2	0	04FE21819E14...	0012F5DBC123...	19 листопада 2025 р., 02:38:02	SvItBMMAQ8kTO...	валідний	Edit	Транзакції
8	7	0	0012F5DBC123...	0F7AA24617B7...	19 листопада 2025 р., 02:38:02	UCBnAoIh86U0...	валідний	Edit	Транзакції
9	38	0	0F7AA24617B7...	035F8E29E427...	19 листопада 2025 р., 02:38:02	L9RxhGkDrDXi...	валідний	Edit	Транзакції
10	27	0	035F8E29E427...	0BBFC93E7D3D...	19 листопада 2025 р., 02:38:03	Cx1tGp7HRKPS...	валідний	Edit	Транзакції
11	24	0	0BBFC93E7D3D...	0EBB24F7027E...	19 листопада 2025 р., 02:38:04	26hNVSDzB2LW...	валідний	Edit	Транзакції
12	3	0	0EBB24F7027E...	0BAAD9A71766...	19 листопада 2025 р., 02:40:30	q4Vik1k6zOc...	валідний	Edit	Транзакції

#### 4. У таблиці транзакцій для кожного блоку, де бере участь PenaltyStaking-контракт:

- З'являється додаткова колонка: "Stake" — депозит / "Unstake" — виведення

Index - Block\_Chain

localhost:7146/?nodeId=A

0	6	0		0335235E8261...	01 січня 2025 р., 00:00:00		валідний	Edit	Транзакції		
1	8	0	0335235E8261...	06D5038AD551...	19 листопада 2025 р., 02:37:57	pkjujhISloo...	валідний	Edit	Транзакції		
2	11	0	06D5038AD551...	0A0DA698E2EE...	19 листопада 2025 р., 02:37:58	jyoxA8RIG+KZ...	валідний	Edit	Транзакції		
3	16	0	0A0DA698E2EE...	00598FF5B991...	19 листопада 2025 р., 02:37:59	zGEHuGtyoNsV...	валідний	Edit	Транзакції		
4	21	0	00598FF5B991...	0C9B9DB74EF...	19 листопада 2025 р., 02:38:00	laicHbR6lfp...	валідний	Edit	Транзакції		
5	37	0	0C9B9DB74EF...	01332AA42898...	19 листопада 2025 р., 02:38:00	RmvkoJaA0Vfv...	валідний	Edit	Транзакції		
6	22	0	01332AA42898...	04FE21819E14...	19 листопада 2025 р., 02:38:01	1nrg61BZJ/Vo...	валідний	Edit	Транзакції		
7	2	0	04FE21819E14...	0012F5DBC123...	19 листопада 2025 р., 02:38:02	SVtBMMaQ8kTO...	валідний	Edit	Транзакції		
8	7	0	0012F5DBC123...	0F7AA24617B7...	19 листопада 2025 р., 02:38:02	UCBnAoIh86U0...	валідний	Edit	Транзакції		
9	38	0	0F7AA24617B7...	035F8E29E427...	19 листопада 2025 р., 02:38:02	L9RxhGkDrDXi...	валідний	Edit	Транзакції		
10	27	0	035F8E29E427...	0BBFC93E7D3D...	19 листопада 2025 р., 02:38:03	Cx1tGp7HRKPs...	валідний	Edit	Транзакції		
11	24	0	0BBFC93E7D3D...	0EBB24F7027E...	19 листопада 2025 р., 02:38:04	26hNVSDz2LW...	валідний	Edit	Транзакції		
FromAddress	ToAddress	Amount	Fee	Note	Confirmations						
COINBASE	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	1,00000	0								
12	3	0	0EBB24F7027E...	08AAD9A71766...	19 листопада 2025 р., 02:40:30	q4Vlk1ki6zOc...	валідний	Edit	Транзакції		
FromAddress	ToAddress	Amount	Fee	Stake/Unstake	Note	Confirmations					
COINBASE	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	2,00000	0								
ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3	10,00000	1	Stake		Stake tokens					1
13	9	0	0BAAD9A71766...	0F02ED826900...	19 листопада 2025 р., 02:53:27	1RZpIRCzbZA...	валідний	Edit	Транзакції		
FromAddress	ToAddress	Amount	Fee	Stake/Unstake	Note	Confirmations					
COINBASE	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	1,00000	0								
ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	8,00200	0	Unstake		Withdraw from staking					0



© 2025 - Block\_Chain\_Example\_1 - [Privacy](#)

## 5. Моделюю ситуацію заново і намагаюся Вивести зі стейкінгу більшу суму ніж поклав. Отримую попередження. Транзакція до мемпулу не потрапляє:

Screenshot of the Block\_Chain application interface showing the wallet registration and staking process.

**Register Wallet**

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCFOE495CBF0535E4421D4B0476C1C810649E	<a href="#">Copy addr</a>	(Contract)	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C	<a href="#">Copy addr</a>	User_A	2,00000	<RSAKeyVal	2025-11-19 02:57:17Z

**Penalty Staking**

Address смарт-контракту для стейкінгу:  
ADDR\_EFABCFOE495CBF0535E4421D4B0476C1C810649E

**Покласти у стейкінг**

From Address: ADDR\_EFABCFOE495CBF0535E4421D4B0476C1C810649E

Amount: 25

Fee: 0

Private Key: (Input field)

**Вивести зі стейкінгу**

Address (Одержанувач): ADDR\_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C

Amount: 25

[Withdraw](#)

**Mem pool**

From Address (ADDR...) To Address (ADDR...) Amount Fee Private key note  
[Додати у мемпул](#)

Транзакцій немає

Screenshot of the Block\_Chain application interface showing the wallet registration and staking process.

**Register Wallet**

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCFOE495CBF0535E4421D4B0476C1C810649E	<a href="#">Copy addr</a>	(Contract)	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C	<a href="#">Copy addr</a>	User_A	2,00000	<RSAKeyVal	2025-11-19 02:57:17Z

**Penalty Staking**

Address смарт-контракту для стейкінгу:  
ADDR\_EFABCFOE495CBF0535E4421D4B0476C1C810649E

**Покласти у стейкінг**

From Address: ADDR\_EFABCFOE495CBF0535E4421D4B0476C1C810649E

Amount: 25

Fee: 0

Private Key: (Input field)

**Вивести зі стейкінгу**

Address (Одержанувач): ADDR\_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C

Amount: 25

[Withdraw](#)

**Mem pool**

From Address (ADDR...) To Address (ADDR...) Amount Fee Private key note  
[Додати у мемпул](#)

Транзакцій немає

Неможливо вивести зі стейкінгу. Запитана сума 25 перевищує внесену 10.

6. При натисканні на адресу Контракта, виводиться таблиця \*\*стан PenaltyStaking-контракту\*\*. Для кожного користувача:

- Адреса стейкера
- Блок початку стейкінгу
- Загальна застейкана сума
- Винагорода, яка обчислюється після кожного нового блоку
- Можливий штраф за досркове зняття коштів зі стейкінгу
- Можливу суму доступну до виводу
- Скільки блоків минуло / залишилось
- Статус виводу

The screenshot displays a user interface for managing a blockchain wallet and interacting with a PenaltyStaking contract.

**Top Section:**

- Address bar: /?nodeId=A
- Contract details (under RSAKeyValue):
  - Public key => uKObAd
  - Modulus => 3xvPWF9V1OE1uVG
  - Reward => 1,0
- Buttons: Копіювати ключ (Copy key), Поточний вузол: Node A, Переключити (Switch node).

**Middle Section:**

- Buttons: START DEMO, <RSAKeyValue> <Modulu, START MINE, Difficu, Задати.
- Message: Блок # 14 розповсюджене. Прийняли: 2 вузли з 3.
- Register Wallet:**
  - Fields: Введіть ім'я власника гам, Введіть Public Key XML, Register Wallet.
  - Table:
 

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCFOE495CBF0535E4421D4B0476C1C810649E	Copy addr	(Contract)	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z

PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%
- Right Arrow:** Points to the "Penalty Staking" section.
- Penalty Staking Section:**
  - Address of the smart contract for staking: ADDR\_EFABCFOE495CBF0535E4421D4B0476C1C810649E
  - Buttons: Покласти у стейкінг (Deposit into staking), Вивести зі стейкінгу (Withdraw from staking).
  - Inputs: From Address (ADDR...), Amount.

## 7. З кожним новим добутим блоком «Нарахована винагорода» - збільшується:

Index - Block\_Chain    localhost:7146/?nodeId=A

Block\_Chain Home Search

<RSAKeyValue> Public key => <RSAKeyValue>  
 <Modulus> uKObAd <Modulus> uKObAd  
 3xvPWf9V1OE1uVG 3xvPWf9V1OE1uVG  
 DjPzIgm+2FZ/Ya/LM

Valid Chain => True  
 Difficulty => 1  
 Reward => 1,0

Поточний вузол: Node A

**Блок # 31 розповсюджено. Прийняли: 2 вузли з 3.**

**Register Wallet**

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCFOE495CBF0535E4421D4B0476C1C810649E	<input type="button" value="Copy addr"/>	(Contract) PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, earlyPenaltyPercent = 20.0%	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z

**Адреса стейкера** **Блок початку стейкінгу** **Сума** **Винагорода** **Доступно до виводу** **Штраф** **Блоків минуло/залишилось** **Статус виводу**

ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C	12	10,0000	0,1900	2,0000	8,1900	Минуло 19 блоків. Залишилось 1 блоків до винагороди.	<span style="color: orange;">⚠️ Зі штрафом 20,0% до блоку 32.</span>
---	----	---------	--------	--------	--------	--	--

User\_A 21,00000 <RSAKeyVal 2025-11-19 02:57:17Z

**Penalty Staking**

Адреса смарт-контракту для стейкінгу:  
 ADDR\_EFABCFOE495CBF0535E4421D4B0476C1C810649E

**Покласти у стейкінг** **Вивести зі стейкінгу**

From Address	Address (Одержанувач)
<input type="text" value="From Address (ADDR...)"/>	<input type="text" value="Address (ADDR...)"/>

Amount

## 8. Якщо чужий користувач намагається отримати 10 токенів зі стейкінгу, то отримує попередження. Транзакція до мемпулу не потрапляє:

Screenshot of the Block\_Chain application interface showing the 'Penalty Staking' section.

The table shows three staking entries:

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
<a href="#">ADDR_EFABCFOE495CBF0535E4421D4B0476C1C810649E</a>	<a href="#">Copy addr</a>	(Contract)	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
<a href="#">ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C</a>	<a href="#">Copy addr</a>	User_A	28,00000	<RSAKeyVal	2025-11-19 02:57:17Z
<a href="#">ADDR_E9A6F2F8F498B4FAAC88B53AAFF600D7F2884093</a>	<a href="#">Copy addr</a>	Ivan	5,00000	<RSAKeyVal	2025-11-19 03:06:23Z
<a href="#">ADDR_C68F5411A2DA499986300D27B4713E04ACD7CC7D</a>	<a href="#">Copy addr</a>	Taras	30,00000	<RSAKeyVal	2025-11-19 03:06:23Z

The 'Penalty Staking' form is displayed, with a red arrow pointing from the 'From Address' field to the 'Address (Одержанувач)' field. The 'Amount' field contains '1d'.

Red arrows also point to the 'Withdraw' button and the 'Stake' button.

Screenshot of the Block\_Chain application interface showing the 'Penalty Staking' section.

The table shows the same three staking entries as the previous screenshot.

The 'Penalty Staking' form is displayed, with a red arrow pointing from the 'From Address' field to the 'Address (Одержанувач)' field. The 'Amount' field contains '1d'.

Red arrows also point to the 'Withdraw' button and the 'Stake' button.

Screenshot of the Block\_Chain application interface showing the 'Mem pool' section.

A large red arrow points from the top of the page down to this section.

The 'Mem pool' table is empty:

Index	Nonce	MiningDurationMs	PrevHash	Hash	Timestamp	Signature	Статус підпису	
0	6	0		0335235E8261...	01 січня 2025 р., 00:00:00		валідний	<a href="#">Edit</a> <a href="#">Транзакції</a>

A red box highlights the message: "Неможливо вивести зі стейкінгу. Запитана сума 10 перевищує внесену 0."

**9.** Заповнюємо таблицю «Вивести зі стейкінгу» для користувача User\_A на суму 10 токенів.

- Та додаємо транзакцію в мемпул:

The screenshot shows a user interface for managing a blockchain node. At the top, there's a header with a close button ('x') and a plus sign ('+') for adding new transactions. Below it, the URL is 6/?nodeId=A. The main area has sections for 'Fee' (input field), 'Private Key' (input field), and a green 'Stake' button. To the right is a yellow 'Withdraw' button with a small icon. A large orange arrow points from the top section down to a table titled 'Mem pool'. The table lists a single transaction entry:

From Address	To Address	Amount	Fee	Note
ADDR_EFABCF0E495CBF0535E4421D4B0476C1C810649E	ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C	10,61000	0	Withdraw from staking

Below this table is another table titled 'Index' containing six rows of transaction details, each with an 'Edit' button and a 'Transakci' button. The columns include Index, Nonce, MiningDurationMs, PrevHash, Hash, Timestamp, Signature, Status, and Edit/Transakci buttons.

**10.** Після додавання транзакції в мемпул та майнінгу:

- User\_A отримує 10 токенів з винагородою**
- з адреси Контракту списується 10 токенів та списується винагорода.

The screenshot shows a dashboard with several sections. At the top, there are buttons for 'Копіювати ключ' (Copy key), 'Поточний вузол: Node A' (Current node: Node A), and 'Переключити' (Switch). Below this are buttons for 'START DEMO', '<RSAKeyValue><Modulus>', 'START MINE', 'Difficu', and 'Задати' (Assign).

A green banner at the top indicates: 'Блок # 74 розповсюдженено. Прийняли: 2 вузли з 3.'

The next section is 'Register Wallet' with fields for 'Введіть ім'я власника гам' (Enter owner name) and 'Введіть Public Key XML' (Enter Public Key XML). It includes a 'Register Wallet' button and a table of wallet entries:

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCF0E495CBF0535E4421D4B0476C1C810649E	Copy addr	(Contract)	-0,61000	<RSAKeyValue>	2025-11-19 02:57:09Z
ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C	Copy addr	User_A	39,61000	<RSAKeyValue>	2025-11-19 02:57:17Z
ADDR_E9A6F2F8F498B4FAACB8B53AAEF600D7F2B84093	Copy addr	Ivan	5,00000	<RSAKeyValue>	2025-11-19 03:06:23Z
ADDR_C68F5411A2DA499986300D27B4713E04ACD7CC7D	Copy addr	Taras	30,00000	<RSAKeyValue>	2025-11-19 03:06:23Z

A large orange arrow points from the wallet section down to the 'Penalty Staking' section. This section has a green header and contains a table with one row:

Адреса смарт-контракту для стейкінгу: ADDR_EFABCF0E495CBF0535E4421D4B0476C1C810649E	Покласти у стейкінг	Вивести зі стейкінгу
From Address		Address (Одержуваць)

## **Висновок:**

У даній екзаменаційній роботі було реалізовано та інтегровано смарт-контракт PenaltyStakingContract, який моделює принципи Proof-of-Stake із підтримкою винагороди за стейкінг та застосуванням штрафів за дострокове зняття коштів.

Створений функціонал забезпечує повний життєвий цикл взаємодії користувача зі стейкінговим контрактом: заморожування токенів, нарахування винагороди за кожний новий блок, а також можливість коректного виведення коштів відповідно до визначених правил.

Контракт успішно інтегровано у BlockChainService: реалізовано окремий гаманець смарт-контракту, логіку перевірки транзакцій, відхилення некоректних операцій та обробку депозитів і виведень.

Створено відповідні UI-форми, що дозволяють користувачам інтуїтивно взаємодіяти зі стейкінгом, а також механізм відображення транзакцій із позначенням типу операції («Stake» / «Unstake»).

Окремо реалізовано таблицю стану PenaltyStaking-контракту, яка в реальному часі відображає ключові параметри для кожного стейкера: суми депозитів, початковий блок, накопичену винагороду, строки та можливі штрафи. Це забезпечує прозорість роботи контракту та контроль коректності всіх розрахунків.

Практичні сценарії, продемонстровані в ході роботи, підтвердили правильність функціонування алгоритмів стейкінгу, нарахування винагород, визначення штрафів, валідації транзакцій та безпеки доступу до коштів. Всі механізми працюють відповідно до технічних вимог.

Таким чином, поставлені завдання виконано повністю: реалізовано смарт-контракт, інтегровано його у блокчайн-інфраструктуру, розроблено користувацький інтерфейс та забезпечено прозоре відображення стану стейкінгової системи. Отриманий результат демонструє розуміння принципів роботи блокчейну, механізмів транзакцій, підпису, а також логіки стейкінгових систем із винагородами та штрафами.