

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 дострокове 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 buttons for 'START DEMO', '<RSAKeyValue><Modulus>', 'START MINE', 'Difficu', and 'Задати'. A message in a green box says 'Блок # 11 розповсюджено. Прийняли: 2 вузли з 3.' Below this, the 'Register Wallet' section shows a table of wallet registrations. One entry for 'User_A' has an amount of 11,00000 tokens. The 'Penalty Staking' section shows a form where a user can stake tokens. An orange arrow points to the 'Stake' button in this section. The 'Penalty Staking' form includes fields for 'Address' (containing 'ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817'), 'Amount' (set to 10), 'Fee' (set to 1), and a 'Private Key' input field containing a long RSA key value. To the right of the form, there are sections for 'Покласти у стейкінг' and 'Вивести зі стейкінгу'.

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

Screenshot of the Block_Chain application interface showing the wallet registration process and the mempool table.

Wallet Registration:

The screenshot shows the "Register Wallet" section where a new wallet is being created with the address [ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3](#). A red arrow points from the "Register Wallet" button down to the "Mem pool" table.

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

Mem pool:

The mempool table lists 12 transactions. A red arrow points up from the bottom of the mempool table towards the "FromAddress" column of the table below.

Index	Nonce	MiningDurationMs	PrevHash	Hash	Timestamp	Signature	Статус підпису	
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	pkjujhSlsooe...	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...	0C9B9BD874EF...	19 листопада 2025 р., 02:38:00	laicHbR6Lffp...	валідний	Edit Транзакції
5	37	0	0C9B9BD874EF...	01332AA42B9B...	19 листопада 2025 р., 02:38:00	RmvkoJaA0Vfv...	валідний	Edit Транзакції
6	22	0	01332AA42B9B...	04FE21819E14...	19 листопада 2025 р., 02:38:01	1nrG618ZJ/Vo...	валідний	Edit Транзакції
7	2	0	04FE21819E14...	0012F5DBC123...	19 листопада 2025 р., 02:38:02	SvtBMMaQBkTO...	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	q4Vlk1ki6zOc...	валідний	Edit Транзакції

Transactions in Mem pool:

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

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:

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

Penalty Staking	
Адреса смарт-контракту для стейкінгу: ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3	Вивести зі стейкінгу
Покласти у стейкінг	Вивести зі стейкінгу
From Address	Address (Одержання)
<input type="text" value="From Address (ADDR...)"/>	<input type="text" value="ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817"/>
Amount	Amount
<input type="text" value="Amount"/>	<input type="text" value="1d"/>
Fee	Withdraw
<input type="text" value="Fee"/>	<input type="button" value="Withdraw"/>
Private Key	
<input type="text" value="Private Key"/>	
<input type="button" value="Stake"/>	

Mem pool

From Address (ADDR...)	To Address (ADDR...)	Amount	Fee	Private key	Note
Додати у мемпул					

Транзакцій немає

Mem pool						
From Address	To Address	Amount	Fee	Private key	Note	
Додати у мемпул						
ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	8,00200	0		Withdraw from staking	
Index	Nonce	MiningDurationMs	PrevHash	Hash	Timestamp	Статус підпису
0	6	0	0335235E8261...	0335235E8261...	01 січня 2025 р., 00:00:00	валідний
1	8	0	0335235E8261...	06D5038AD551...	19 листопада 2025 р., 02:37:57	валідний
2	11	0	06D5038AD551...	0A0DA698E2EE...	19 листопада 2025 р., 02:37:58	валідний
3	16	0	0A0DA698E2EE...	00598FF5B991...	19 листопада 2025 р., 02:37:59	валідний
4	21	0	00598FF5B991...	0C9B9BD874EF...	19 листопада 2025 р., 02:38:00	валідний
5	37	0	0C9B9BD874EF...	01332AA42B98...	19 листопада 2025 р., 02:38:00	валідний
6	22	0	01332AA42B98...	04FE21819E14...	19 листопада 2025 р., 02:38:01	валідний
7	2	0	04FE21819E14...	0012F5DBC123...	19 листопада 2025 р., 02:38:02	валідний
8	7	0	0012F5DBC123...	0F7AA24617B7...	19 листопада 2025 р., 02:38:02	валідний
9	38	0	0F7AA24617B7...	035F8E29E427...	19 листопада 2025 р., 02:38:02	валідний
10	27	0	035F8E29E427...	0BBFC93E7D3D...	19 листопада 2025 р., 02:38:03	валідний
11	24	0	0BBFC93E7D3D...	0EBB24F7027E...	19 листопада 2025 р., 02:38:04	валідний
12	3	0	0EBB24F7027E...	0BAAD9A71766...	19 листопада 2025 р., 02:40:30	валідний

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	pkjujh1Slooe...		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...	0C9B9BD874EF...	19 листопада 2025 р., 02:38:00	laicHbR6lffp...		валідний	Edit	Транзакції	
5	37	0	0C9B9BD874EF...	01332AA42B98...	19 листопада 2025 р., 02:38:00	RmvkoJaA0Vf...		валідний	Edit	Транзакції	
6	22	0	01332AA42B98...	04FE21819E14...	19 листопада 2025 р., 02:38:01	1nrgG1BZJ/Vo...		валідний	Edit	Транзакції	
7	2	0	04FE21819E14...	0012F5DBC123...	19 листопада 2025 р., 02:38:02	SVtBMMaQBkTO...		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	
FromAddress	ToAddress	Amount	Fee	Note	Confirmations						
COINBASE	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	1,00000	0								
12	3	0	0EBB24F7027E...	08AAD9A71766...	19 листопада 2025 р., 02:40:30	q4Vlk1k16zOc...		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	1RZplIRCzbZA...		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 web interface showing the wallet registration and staking process.

Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCFC0E495CBF0535E4421D4B0476C1C810649E	Copy addr	(Contract)	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C	Copy addr	User_A	2,00000	<RSAKeyVal	2025-11-19 02:57:17Z

Penalty Staking

Address смарт-контракту для стейкінгу:
ADDR_EFABCFC0E495CBF0535E4421D4B0476C1C810649E

Покласти у стейкінг

From Address: ADDR_EFABCFC0E495CBF0535E4421D4B0476C1C810649E

Amount: 25

Fee: 0

Private Key: (Placeholder)

Вивести зі стейкінгу

Address (Одержанувач): ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C

Amount: 25

Fee: 0

[Withdraw](#)

Mem pool

From Address (ADDR...) To Address (ADDR...) Amount Fee Private key note

Додати у мемпул

Транзакцій немає

Screenshot of the web interface showing the wallet registration and staking process.

Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCFC0E495CBF0535E4421D4B0476C1C810649E	Copy addr	(Contract)	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C	Copy addr	User_A	2,00000	<RSAKeyVal	2025-11-19 02:57:17Z

Penalty Staking

Address смарт-контракту для стейкінгу:
ADDR_EFABCFC0E495CBF0535E4421D4B0476C1C810649E

Покласти у стейкінг

From Address: ADDR_EFABCFC0E495CBF0535E4421D4B0476C1C810649E

Amount: 25

Fee: 0

Private Key: (Placeholder)

Вивести зі стейкінгу

Address (Одержанувач): ADDR_7FF7CF500CB08DA2B5BB3B83DBF5902F4EC1830C

Amount: 25

Fee: 0

[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.

Index	Nonce	MiningDurationMs	PrevHash	Hash	Timestamp	Signature	Статус підпису
-------	-------	------------------	----------	------	-----------	-----------	----------------

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 staking. It includes sections for wallet registration, staking status, and penalty staking.

Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABC0E495CBF0535E4421D4B0476C1C810649E	Copy addr	(Contract)	10,00000	<RSAKeyValue>	2025-11-19 02:57:09Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
[ADDR_EFABC0E495CBF0535E4421D4B0476C1C810649E](#)

Адреса стейкера	Блок початку стейкінгу	Сума	Винагорода	Штраф	Доступно до виводу	Блоків минуло/залишилось	Статус виводу
ADDR_7FF7CF500CB08DA2B5BB3883D8F5902F4EC1830C	12	10,0000	0,0200	2,0000	8,0200	Минуло 2 блоків. Залишилось 18 блоків до винагороди.	⚠️ Зі штрафом 20,0% до блоку 32.

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

Index - Block_Chain localhost:7146/?nodeId=A

Block_Chain Home Search

<RSAKeyValue> <input type="button" value="Public key =>"/> <Modulus> uKObAd <input type="button" value="RSAKeyValue"/> 3xvPWf9V1OE1uVG <input type="button" value="Modulus"/> uKObAd DjPzigm+2FZ/Ya/LM <input type="button" value="3xvPWf9V1OE1uVG"/> <input type="button" value="Копіювати ключ"/> Поточний вузол: Node A <input type="button" value="Переключити"/>	Valid Chain => True Difficulty => 1 Reward => 1,0
---	---

→ 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)	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%					

→

Penalty Staking

Адреса стейкера	Блок початку стейкінгу	Сума	Винагорода	Доступно до Штраф виводу	Блоків минуло/залишилось	Статус виводу
ADDR_7FF7CF500CB08DA2B5B83B83DBF5902F4EC1830C	12	10,0000	0,1900	2,0000 8,1900	Минуло 19 блоків. Залишилось 1 блоків до винагороди.	! Зі штрафом 20,0% до блоку 32.

User_A 21,00000 <RSAKeyVal 2025-11-19 02:57:17Z

Покласти у стейкінг

From Address:

Вивести зі стейкінгу

Address (Одержання):

Amount:

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

Index - Block_Chain

localhost:7146/?nodeId=A

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABC0E495CBF0535E4421D4B0476C1C810649E	Copy addr	(Contract)	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
PenaltyStakingContract: RewardPerBlockPerToken = 0.001; LockPeriodInBlocks = 20; EarlyPenaltyPercent = 20.0%					
Адреса стейкера	Блок початку стейкінгу	Сума	Винагорода	Штраф виводу	Доступно до виводу
ADDR_7FF7CF500CB08DA...	12	10,0000	0,6100	0,0000	10,6100
Блоків минуло/залишилось					
Минуло 61 блоків. Залишилось 0 блоків до винагороди.					
Статус виводу					
✓ Без штрафу					
ADDR_7FF7CF500CB08DA2B5BB3883DBF5902F4EC1830C	Copy addr	User_A	28,00000	<RSAKeyVal	2025-11-19 02:57:17Z
ADDR_E9A6F2F8F49884FAAC88853AAEF600D7F2884093	Copy addr	Ivan	5,00000	<RSAKeyVal	2025-11-19 03:06:23Z
ADDR_C68F5411A2DA499986300D27B4713E04ACD7CC7D	Copy addr	Taras	30,00000	<RSAKeyVal	2025-11-19 03:06:23Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
[ADDR_EFABC0E495CBF0535E4421D4B0476C1C810649E](#)

Покласти у стейкінг

From Address: ADDR_7FF7CF500CB08DA2B5BB3883DBF5902F4EC1830C

Amount: 10

Fee: 0

Private Key:

Вивести зі стейкінгу

Address (Одержанувач): ADDR_C68F5411A2DA499986300D27B4713E04ACD7CC7D

Amount: 10

Withdraw

Index - Block_Chain

localhost:7146/?nodeId=A

Address	Copyaddr	Name	Amount	PublicKey	RegisteredAt
ADDR_7FF7CF500CB08DA2B5BB3883DBF5902F4EC1830C	Copy addr	User_A	28,00000	<RSAKeyVal	2025-11-19 02:57:17Z
ADDR_E9A6F2F8F49884FAAC88853AAEF600D7F2884093	Copy addr	Ivan	5,00000	<RSAKeyVal	2025-11-19 03:06:23Z
ADDR_C68F5411A2DA499986300D27B4713E04ACD7CC7D	Copy addr	Taras	30,00000	<RSAKeyVal	2025-11-19 03:06:23Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
[ADDR_EFABC0E495CBF0535E4421D4B0476C1C810649E](#)

Покласти у стейкінг

From Address: ADDR_7FF7CF500CB08DA2B5BB3883DBF5902F4EC1830C

Amount: 10

Fee: 0

Private Key:

Вивести зі стейкінгу

Address (Одержанувач): ADDR_C68F5411A2DA499986300D27B4713E04ACD7CC7D

Amount: 10

Withdraw

Mem pool

From Address (ADDR...)	To Address (ADDR...)	Amount	Fee	Private key	note
Добавити у мемпул					

Транзакцій немає

Неможливо вивести зі стейкінгу. Запитана сума 10 перевищує внесену 0.

Index	Nonce	MiningDurationMs	PrevHash	Hash	Timestamp	Signature	Статус підпису	
0	6	0		0335235E8261...	01 січня 2025 р., 00:00:00		валідний	Edit Транзакції

9. Заповнюємо таблицю «Вивести зі стейкінгу» для користувача User_A на суму 10 токенів.

- Та додаємо транзакцію в мемпул:

Fee

Private Key

Stake

Withdraw

Mem pool

From Address (ADDR...)	To Address (ADDR...)	Amount	Fee	Private key	Note
ADDR_EFABC...	ADDR_7FF...	10,61000	0		Withdraw from staking

From Address To Address Amount Fee Note

ADDR_EFABC...

ADDR_7FF...

10,61000 0 Withdraw from staking

Index	Nonce	MiningDurationMs	PrevHash	Hash	Timestamp	Signature	Статус підпису	
0	6	0		0335235E8261...	01 січня 2025 р., 00:00:00		валідний	<button>Edit</button> Транзакції
1	6	0	0335235E8261...	0843303D3B6...	19 листопада 2025 р., 02:57:17	h1Am/9AytYQ...	валідний	<button>Edit</button> Транзакції
2	24	0	0843303D3B6...	097415552C76...	19 листопада 2025 р., 02:57:18	MmGoAp+Qkhr...	валідний	<button>Edit</button> Транзакції
3	2	0	097415552C76...	0F143AA1FDDE...	19 листопада 2025 р., 02:57:18	TGpjQkp+h6ZH...	валідний	<button>Edit</button> Транзакції
4	31	0	0F143AA1FDDE...	057D6ADE3376...	19 листопада 2025 р., 02:57:19	hBakKoH2FqZr...	валідний	<button>Edit</button> Транзакції
5	3	0	057D6ADE3376...	08631A3765DD...	19 листопада 2025 р., 02:57:19	TUh5Targw5zR...	валідний	<button>Edit</button> Транзакції

10. Після додавання транзакцій в мемпул та майнінгу:

- User_A отримує 10 токенів з винагородою**
- з адреси Контракту списується 10 токенів та списується винагорода.

CopyKey

Potockyiy vuzok: Node A

START DEMO <RSAKeyValue><Modulu> START MINE Difficu Задати

Блок # 74 розповсюджено. Прийшли 2 вузли з 3.

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABC...	Copy addr	(Contract)	-0,61000	<RSAKeyValue>	2025-11-19 02:57:09Z
ADDR_7FF...	Copy addr	User_A	39,61000	<RSAKeyValue>	2025-11-19 02:57:17Z
ADDR_E9A...	Copy addr	Ivan	5,00000	<RSAKeyValue>	2025-11-19 03:06:23Z
ADDR_C68...	Copy addr	Taras	30,00000	<RSAKeyValue>	2025-11-19 03:06:23Z

Register Wallet

Penalty Staking

Adres smart-kontraktu dla steykingu:
ADDR_EFABC...

Покласти у стейкінг
From Address

Вивести зі стейкінгу
Address (Одержанувач)

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 досркове 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 блокчайну, механізмів транзакцій, підпису, а також логіки стейкінгових систем із винагородами та штрафами.