

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:

Поточний вузол: Node A Переключити

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

Блок # 11 розповсюджено. Прийняли: 2 вузли з 3.

Register Wallet

Введіть ім'я власника гам Введіть Public Key XML Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_1870338034A6A0D13CA04CEC1C8FEE66072AB2A3	Copy addr	(Contract) PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%	0	<RSAKeyVal	2025-11-19 02:37:15Z
ADDR_5DBE943C27845D421A1979DE56A1FAC62CF98817	Copy addr	User_A	11,00000	<RSAKeyVal	2025-11-19 02:37:56Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
[ADDR_1870338034A6A0D13CA04CEC1C8FEE66072AB2A3](#)

Покласти у стейкінг

From Address

Amount

Fee

Private Key

Вивести зі стейкінгу

Address (Одержувач)

Amount

2. Після додавання транзакції в мемпул та майнінгу:

- з User_A списується 10 tokenів
- на адресу Контракту зараховується 10 tokenів.

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

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

Block_Chain Home Search

<RSAKeyValue>
<Modulus>9Xt5HOH
7ndNW1Twsyn22Pv
489SNUdriLPqOMIdf
Копіювати ключ

Public key =>
<RSAKeyValue>
<Modulus>9Xt5HOH
7ndNW1Twsyn22Pv

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

Поточний вузол: Node A Переключити

START DEMO

<RSAKeyValue><Modulus>

START MINE

Difficu

Задати

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

Register Wallet

Введіть ім'я власника гам Введіть Public Key XML Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_1870338034A6A0D13CA04CEC1C8FEE66072AB2A3	Copy addr	(Contract) PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%	10,00000	<RSAKeyVal	2025-11-19 02:37:15Z
ADDR_5DBE943C27845D421A1979DE56A1FAC62CF98B17	Copy addr	User_A	2,00000	<RSAKeyVal	2025-11-19 02:37:56Z

Mem pool

From Address (ADDR_...)

To Address (ADDR_...)

Amount

Fee

Private key

note

Додати у мемпул

Транзакцій немає

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	pkjuhlSlooe...	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...	01332AA42B9B...	19 листопада 2025 р, 02:38:00	RmvkoJaA0Vfv...	валідний	Edit Транзакції
6	22	0	01332AA42B9B...	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	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...	08BFC93E7D3D...	19 листопада 2025 р, 02:38:03	Cx1tGp7HRKPS...	валідний	Edit Транзакції
11	24	0	08BFC93E7D3D...	0EBB24F7027E...	19 листопада 2025 р, 02:38:04	26hNVSDzB2LW...	валідний	Edit Транзакції
12	3	0	0EBB24F7027E...	0BAAD9A71766...	19 листопада 2025 р, 02:40:30	q4Vik1ki6zOc...	валідний	Edit Транзакції

FromAddress	ToAddress	Amount	Fee	Stake/Unstake	Note	Confirmations
COINBASE	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF98B17	2,00000	0			
ADDR_5DBE943C27845D421A1979DE56A1FAC62CF98B17	ADDR_1870338034A6A0D13CA04CEC1C8FEE66072AB2A3	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:

Index - Block_Chain

localhost:7146/?nodeId=A

Введіть ім'я власника гам | Введіть Public Key XML | Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_1870338034A6A0D13CA04CEC1C8FEE66072AB2A3	Copy addr	(Contract) PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%	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_1870338034A6A0D13CA04CEC1C8FEE66072AB2A3

Покласти у стейкінг

From Address
From Address (ADDR...)

Amount
Amount

Fee
Fee

Private Key
Private Key

Stake

Вивести зі стейкінгу

Address (Одержувач)
ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817

Amount
10

Withdraw

Mem pool

From Address (ADDR...)

To Address (ADDR...)

Amount

Fee

Private key

note

Додати у мемпул

Транзакцій немає

Index - Block_Chain

localhost:7146/?nodeId=A

Private Key
Private Key

Stake

Mem pool

From Address (ADDR...)

To Address (ADDR...)

Amount

Fee

Private key

note

Додати у мемпул

From Address	To Address	Amount	Fee	Note
ADDR_1870338034A6A0D13CA04CEC1C8FEE66072AB2A3	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	8,00200	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	Edit Транзакції
1	8	0	0335235E8261...	06D5038AD551...	19 листопада 2025 р., 02:37:57	pkjujhiSlooe...	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	laicHbR6Lfp...	валідний	Edit Транзакції
5	37	0	0C9B9BD874EF...	01332AA42B9B...	19 листопада 2025 р., 02:38:00	RmrvkoJaA0Vfv...	валідний	Edit Транзакції
6	22	0	01332AA42B9B...	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	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	L9RxbGkDrDXi...	валідний	Edit Транзакції
10	27	0	035F8E29E427...	08BFC93E7D3D...	19 листопада 2025 р., 02:38:03	Cx1Gp7HRKPS...	валідний	Edit Транзакції
11	24	0	08BFC93E7D3D...	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	pKjujhiSlooe...	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	zGEnuGtyoNsv...	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	RmvkoJaA0Vfv...	валідний	Edit	Транзакції																					
6	22	0	01332AA42B98...	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	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	L9RxtGkDrDXi...	валідний	Edit	Транзакції																					
10	27	0	035F8E29E427...	0B8FC93E7D3D...	19 листопада 2025 р, 02:38:03	Cx1tGp7HRKPS...	валідний	Edit	Транзакції																					
11	24	0	0B8FC93E7D3D...	0EBB24F7027E...	19 листопада 2025 р, 02:38:04	26hNVSDzB2LW...	валідний	Edit	Транзакції																					
<table><tr><th>FromAddress</th><th>ToAddress</th><th>Amount</th><th>Fee</th><th>Note</th><th>Confirmations</th></tr><tr><td>COINBASE</td><td>ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817</td><td>1,00000</td><td>0</td><td></td><td></td></tr></table>										FromAddress	ToAddress	Amount	Fee	Note	Confirmations	COINBASE	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	1,00000	0											
FromAddress	ToAddress	Amount	Fee	Note	Confirmations																									
COINBASE	ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817	1,00000	0																											
12	3	0	0EBB24F7027E...	0BAAD9A71766...	19 листопада 2025 р, 02:40:30	q4Vik1ki6zOc...	валідний	Edit	Транзакції																					
<table><tr><th>FromAddress</th><th>ToAddress</th><th>Amount</th><th>Fee</th><th>Stake/Unstake</th><th>Note</th><th>Confirmations</th></tr><tr><td>COINBASE</td><td>ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817</td><td>2,00000</td><td>0</td><td></td><td></td><td></td></tr><tr><td>ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817</td><td>ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3</td><td>10,00000</td><td>1</td><td>Stake</td><td>Stake tokens</td><td>1</td></tr></table>										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
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	1RZpIIrCzbZA...	валідний	Edit	Транзакції																					
<table><tr><th>FromAddress</th><th>ToAddress</th><th>Amount</th><th>Fee</th><th>Stake/Unstake</th><th>Note</th><th>Confirmations</th></tr><tr><td>COINBASE</td><td>ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817</td><td>1,00000</td><td>0</td><td></td><td></td><td></td></tr><tr><td>ADDR_187033B034A6A0D13CA04CEC1C8FEE66072AB2A3</td><td>ADDR_5DBE943C27845D421A1979DE56A1FAC62CF9B817</td><td>8,00200</td><td>0</td><td>Unstake</td><td>Withdraw from staking</td><td>0</td></tr></table>										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
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:

Index - Block_Chain

localhost:7146/?nodeId=A

Register Wallet

Введіть ім'я власника гам

Введіть Public Key XML

Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABC0F0E495CBF0535E4421D4B0476C1C810649E	<div>Copy addr</div>	(Contract) PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
ADDR_7FF7CF500C808DA285B83883DBF5902F4EC1830C	<div>Copy addr</div>	User_A	2,00000	<RSAKeyVal	2025-11-19 02:57:17Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
ADDR_EFABC0F0E495CBF0535E4421D4B0476C1C810649E

Покласти у стейкінг

Вивести зі стейкінгу

From Address

From Address (ADDR...)

Amount

Amount

Fee

Fee

Private Key

Private Key

Stake

Address (Одержувач)

ADDR_7FF7CF500C808DA285B83883DBF5902F4EC1830C

Amount

25

Withdraw

Mem pool

From Address (ADDR...)

To Address (ADDR...)

Amount

Fee

Private key

note

Додати у мемпул

Транзакцій немає

Index - Block_Chain

localhost:7146/?nodeId=A

Register Wallet

Введіть ім'я власника гам

Введіть Public Key XML

Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABC0F0E495CBF0535E4421D4B0476C1C810649E	<div>Copy addr</div>	(Contract) PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
ADDR_7FF7CF500C808DA285B83883DBF5902F4EC1830C	<div>Copy addr</div>	User_A	2,00000	<RSAKeyVal	2025-11-19 02:57:17Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
ADDR_EFABC0F0E495CBF0535E4421D4B0476C1C810649E

Покласти у стейкінг

Вивести зі стейкінгу

From Address

From Address (ADDR...)

Amount

Amount

Fee

Fee

Private Key

Private Key

Stake

Address (Одержувач)

Address (ADDR...)

Amount

Amount

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 дострокове зняття коштів зі стейкінгу
- Можливу суму доступну до виводу
- Скільки блоків минуло / залишилось
- Статус виводу

<RSAKeyValue>

<Modulus>uKObAd3xvPWf9V1OE1uVG

DjPzlgm+2FZ/Ya/LM

Public key =>

<RSAKeyValue>

<Modulus>uKObAd3xvPWf9V1OE1uVG

Valid Chain => True

Difficulty => 1

Reward => 1,0

Копіювати ключ

Поточний вузол: Node A

Переключити

START DEMO

<RSAKeyValue> <Modulus>

START MINE

Difficu

Задати

Блок # 14 розповсюджено. Прийняли: 2 вузли з 3.

Register Wallet

Введіть ім'я власника гам

Введіть Public Key XML

Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCf0E495CBf0535E4421D4B0476C1C810649E	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

Штраф

Доступно до виводу

Блоків минуло/залишилось

Статус виводу

ADDR_7FF7CF500CB08DA...	12	10,0000	0,0200	2,0000	8,0200	Минуло 2 блоків. Залишилось 18 блоків до винагороди.	▲ Зі штрафом 20,0% до блоку 32.
-------------------------	----	---------	--------	--------	--------	--	---------------------------------

[ADDR_7FF7CF500CB08DA2858B3B83DBF5902F4EC1830C](#)

Copy addr

User_A

4,00000

<RSAKeyVal

2025-11-19 02:57:17Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
ADDR_EFABCf0E495CBf0535E4421D4B0476C1C810649E

Покласти у стейкінг

From Address

From Address (ADDR...)

Amount

Вивести зі стейкінгу

Address (Одержувач)

Address (ADDR...)

Amount

7

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

Index - Block_Chain

localhost:7146/?nodeId=A

Block_Chain Home Search

<RSAKeyValue> <Modulus> uKObAd 3xvPW9V1OE1uVG DjPzlgm+2FZ/Ya/LM <RSAKeyValue> <Modulus> uKObAd 3xvPW9V1OE1uVG Копіювати ключі

Public key => <RSAKeyValue> <Modulus> uKObAd 3xvPW9V1OE1uVG

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

Поточний вузол: Node A Переключити

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

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

Register Wallet

Введіть ім'я власника гам Введіть Public Key XML Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCF0E495CBF0535E4421D4B0476C1C810649E	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	Штраф	Доступно до виводу	Блоків минуло/залишилось	Статус виводу
ADDR_7FF7CF500C808DA...	12	10,0000	0,1900	2,0000	8,1900	Минуло 19 блоків. Залишилось 1 блоків до винагорода.	Зі штрафом 20,0% до блоку 32.

ADDR_7FF7CF500C808DA2858B3B83DBF5902F4EC1830C Copy addr User_A 21,00000 <RSAKeyVal 2025-11-19 02:57:17Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
ADDR_EFABCF0E495CBF0535E4421D4B0476C1C810649E

Покласти у стейкінг

Вивести зі стейкінгу

From Address Address (Одержувач)

From Address (ADDR...) Address (ADDR...)

Amount Amount

8

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_EFABC0E495CBF0535E4421D480476C1C810649E	Copy addr	(Contract) PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%	10,00000	<RSAKeyVal	2025-11-19 02:57:09Z
ADDR_7FF7CF500CB08DA2858B3883DBF5902F4EC1830C	Copy addr	User_A	28,00000	<RSAKeyVal	2025-11-19 02:57:17Z
ADDR_E9A6F2F8F498B4FAAC88B53AAEF600D7F2884093	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_EFABC0E495CBF0535E4421D480476C1C810649E

Покласти у стейкінг

From Address
From Address (ADDR...)

Amount
Amount

Fee
Fee

Private Key
Private Key

Stake

Вивести зі стейкінгу

Address (Одержувач)
ADDR_C68F5411A2DA499986300D27B4713E04ACD7CC7D

Amount
10

Withdraw

Index - Block_Chain

localhost:7146/?nodeId=A

LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%

ADDR_7FF7CF500CB08DA2858B3883DBF5902F4EC1830C	Copy addr	User_A	28,00000	<RSAKeyVal	2025-11-19 02:57:17Z
ADDR_E9A6F2F8F498B4FAAC88B53AAEF600D7F2884093	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_EFABC0E495CBF0535E4421D480476C1C810649E

Покласти у стейкінг

From Address
From Address (ADDR...)

Amount
Amount

Fee
Fee

Private Key
Private Key

Stake

Вивести зі стейкінгу

Address (Одержувач)
Address (ADDR...)

Amount
Amount

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 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 tokenів.

- Та додаємо транзакцію в мемпул:

6/?nodeId=A

Fee

Private Key

Private Key

Withdraw

Stake

Mem pool

From Address (ADDR_...)

To Address (ADDR_...)

Amount

Fee

Private key

note

Додати у мемпул

From Address

To Address

Amount

Fee

Note

ADDR_EFABCF0E495CBF0535E4421D4B0476C1C810649E

ADDR_7FF7CF500CB08DA2B58B3B83DBF5902F4EC1830C

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	<div>Edit</div> <div>Транзакції</div>
1	6	0	0335235E8261...	08433303D3B6...	19 листопада 2025 р., 02:57:17	h1Am/9AYitYQ...	валідний	<div>Edit</div> <div>Транзакції</div>
2	24	0	08433303D3B6...	097415552C76...	19 листопада 2025 р., 02:57:18	MmGoJAp+Qkhr...	валідний	<div>Edit</div> <div>Транзакції</div>
3	2	0	097415552C76...	0F143AA1FDFE...	19 листопада 2025 р., 02:57:18	TGpjQkp+h6ZH...	валідний	<div>Edit</div> <div>Транзакції</div>
4	31	0	0F143AA1FDFE...	057D6ADE3376...	19 листопада 2025 р., 02:57:19	hBakKoH2FqZp...	валідний	<div>Edit</div> <div>Транзакції</div>
5	3	0	057D6ADE3376...	08631A3765DD...	19 листопада 2025 р., 02:57:19	TUh5Tarwg5zR...	валідний	<div>Edit</div> <div>Транзакції</div>

10. Після додавання транзакції в мемпул та майнінгу:

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

Копіювати ключ

Поточний вузол: Node A

Переключити

START DEMO

<RSAKeyValue> <Modulus>

START MINE

Difficu

Задати

Блок # 74 розповсюджено. Прийняли: 2 вузли з 3.

Register Wallet

Введіть ім'я власника гам

Введіть Public Key XML

Register Wallet

Address	CopyAddress	Name	Amount	PublicKey	RegisteredAt
ADDR_EFABCF0E495CBF0535E4421D4B0476C1C810649E	Copy addr	(Contract) PenaltyStakingContract: RewardPerBlockPerToken = 0.001, LockPeriodInBlocks = 20, EarlyPenaltyPercent = 20.0%	-0,61000	<RSAKeyVal	2025-11-19 02:57:09Z
ADDR_7FF7CF500CB08DA2B58B3B83DBF5902F4EC1830C	Copy addr	User_A	39,61000	<RSAKeyVal	2025-11-19 02:57:17Z
ADDR_E9A6F2F8F49884FAAC88B53AAEF600D7F2884093	Copy addr	Ivan	5,00000	<RSAKeyVal	2025-11-19 03:06:23Z
ADDR_C68F5411A2DA499986300D2784713E04ACD7CC7D	Copy addr	Taras	30,00000	<RSAKeyVal	2025-11-19 03:06:23Z

Penalty Staking

Адреса смарт-контракту для стейкінгу:
ADDR_EFABCF0E495CBF0535E4421D4B0476C1C810649E

Покласти у стейкінг

From Address

Вивести зі стейкінгу

Address (Одержувач)

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 блокчейн-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.