СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 9](#_3whwml4)

[1](#_30j0zll) КРИПТОГРАФИЯ В НЕАБЕЛЕВЫХ ГРУППАХ 11

[1.1](#_3znysh7) Основы криптографии с открытым ключом 12

[1.2](#_2bn6wsx) Основы криптографии на свободных группах 18

[1.3](#_2et92p0) Обмен публичными ключами с помощью неабелевых групп 25

[1.4](#_tyjcwt) Трехэтапный протокол Шамира и протоколы обмена ключами 29

[1.5](#_3dy6vkm) Криптография в полициклических группах 31

[2](#_1t3h5sf) ИСПОЛЬЗОВАНИЕ ДНК В КРИПТОГРАФИИ 34

[2.1 Хранение данных с использование ДНК](#_4d34og8) 34

[2.2 Процесс кодирования информации 36](#_2s8eyo1)

[2.3 ДНК-криптография 38](#_17dp8vu)

[2.3.1 Криптосистема ДНК с использованием замены 39](#_3rdcrjn)

[2.4 Преимущество и недостатки в использовании ДНК 41](#_26in1rg)

[3](#_lnxbz9) КРИПТОГРАФИЯ ОСНОВАННАЯ НА ХАОСЕ 42

[3.1](#_35nkun2) Внедрение хаотических систем 42

[3.2](#_1ksv4uv) Внедрение криптосистем 43

[3.3](#_44sinio) Анализ безопасности 45

[3.4](#_z337ya) Базовые правила формирования устойчивой криптосистемы 47

[ВЫВОДЫ 48](#_3j2qqm3)

[ПЕРЕЧЕНЬ ССЫЛОК 49](#_1y810tw)

[ПРИЛОЖЕНИЕ А ВХОДНЫЕ И ПОЛУЧЕННЫЕ ДАННЫЕ 51](#_4i7ojhp)

[ПРИЛОЖЕНИЕ Б ИСХОДНЫЕ КОДЫ ПРОГРАММЫ 52](#_2xcytpi)

# ВСТУП

У сучасному світі технології швидко розвиваються, надаючи людям безліч можливостей та засобів для спілкування, розваги, навчання та роботи. Зокрема, блокчейн-технології стали одним з найбільш перспективних і впливових напрямків, що впливають на відносини між людьми, державами, і компаніями. Ці технології революціонізують традиційні підходи до ведення бізнесу, фінансових операцій та управління даними, адже вони надають надійність, прозорість та ефективність у вирішенні різноманітних завдань.

Одним із ключових компонентів успішної реалізації блокчейн-технологій є смарт-контракти, які дозволяють створювати автоматизовані договори, що виконуються без посередників. Смарт-контракти відкривають нові можливості в різних сферах, таких як фінанси, логістика, нерухомість, охорона авторських прав та навіть голосування. Система Ethereum, що базується на блокчейн, є одним з найвідоміших прикладів використання смарт-контрактів. Її гнучкість та можливості розширення дозволяють розробникам створювати різноманітні додатки на основі смарт-контрактів.

Враховуючи величезний потенціал смарт-контрактів та системи Ethereum, вивчення їх особливостей, проблем та можливостей стає вкрай актуальним для науковців, розробників, юристів та представників бізнесу. Дослідження цих питань дасть можливість краще зрозуміти тенденції розвитку технологій, виявити їх переваги та недоліки, а також знайти способи оптимізації та покращення існуючих рішень на базі смарт-контрактів.

Однак, поряд з численними перевагами, смарт-контракти та система Ethereum мають свої виклики та обмеження. Вони включають питання правового регулювання та правового статусу смарт-контрактів, безпеки розробки та використання, а також проблеми масштабування та швидкодії. Вивчення цих аспектів є необхідним для розробки ефективних стратегій управління ризиками та формування рекомендацій щодо впровадження смарт-контрактів у різних відносинах.

Також важливим аспектом є розробка смарт-контрактів, що залежить від вибору мови програмування, налагодження взаємодії зі зовнішніми додатками та платформами, а також дотримання кращих практик розробки для забезпечення стабільності та безпеки коду.

У цій роботі ми спробуємо відповісти на вищезазначені питання та аналізувати особливості застосування смарт-контрактів в системі Ethereum. Ми розглянемо актуальні тенденції, дослідимо різні аспекти смарт-контрактів, а також надамо рекомендації щодо оптимізації їх використання. Це допоможе створити загальне розуміння особливостей смарт-контрактів в системі Ethereum та їх потенціалу в різних сферах життя людей, компаній та держав.

# Огляд концепції смарт-контрактів та їхні основні принципи виконання у системі Ethereum

* 1. Визначення та історія смарт-контрактів

Смарт-контракти є цифровими протоколами, які спрощують, автоматизують та забезпечують виконання умов контракту між сторонами. Вони дозволяють виконувати транзакції та угоди без потреби в посередниках, які зазвичай забезпечують довіру між сторонами. Смарт-контракти базуються на блокчейн-технології, що забезпечує надійність, безпеку та прозорість їх виконання.

Ідея смарт-контрактів була вперше запропонована у 1994 році американським криптографом та комп'ютерним науковцем Ніком Сабо. Він описав смарт-контракти як протоколи, які автоматизують виконання угод на основі прямих та об'єктивних правил, вбудованих у код контракту (1). Проте на той час не існувало відповідної технологічної бази для реалізації смарт-контрактів.

Вирішення цієї проблеми настав у 2009 році з появою блокчейн-технології та створенням першої криптовалюти - Біткоїн, запропонованої Сатоші Накамото (2). Однак, платформа Біткоїн мала обмежені можливості для створення смарт-контрактів. Це спонукало дослідників та розробників до пошуку нових підходів та технологій для реалізації смарт-контрактів.

У 2013 році Віталік Бутерін, співзасновник та головний розробник системи Ethereum, представив концепцію нової блокчейн-платформи з універсальним механізмом для реалізації смарт-контрактів (3). Система Ethereum була офіційно запущена у 2015 році та надала широкі можливості для реалізації смарт-контрактів. Вона дозволила розробникам створювати різноманітні децентралізовані додатки (dApps) та проекти, які здійснюються на основі смарт-контрактів, та стала основою для їх масового розповсюдження.

Однією з ключових особливостей смарт-контрактів є те, що вони працюють на децентралізованих мережах, таких як Ethereum. Це означає, що вони не залежать від одного центрального сервера чи організації, а виконуються розподіленими вузлами мережі, що забезпечують надійність та безпеку виконання контрактів.

Смарт-контракти працюють на основі принципу "if-then" (якщо-то), де умови та дії, які мають відбутися при їх виконанні, програмуються безпосередньо у коді контракту. Це дозволяє автоматично виконувати взаємопов'язані транзакції, коли виконуються певні умови, без потреби в людському втручанні.

З ростом популярності смарт-контрактів стали з'являтися різні платформи та інструменти для їх реалізації. Наприклад, було розроблено мову програмування Solidity, що спеціально призначена для створення смарт-контрактів на платформі Ethereum. Сучасні розробники та організації можуть використовувати ці інструменти для створення різноманітних dApps та сервісів, забезпечуючи зручність, ефективність та децентралізацію.

З розвитком смарт-контрактів та їх широким застосуванням у різних галузях, таких як фінанси, страхування, логістика, нерухомість та інші, стали з'являтися проблеми, пов'язані з їх правовим статусом, регулюванням та стандартами безпеки. У зв'язку з цим ряд країн почав активно розробляти законодавчі норми та регуляторні рамки для смарт-контрактів, що сприяють їхньому легітимному використанню та інтеграції в національні правові системи.

Одним з прикладів успішної адаптації смарт-контрактів на законодавчому рівні є США, де деякі штати вже прийняли закони, що визнають смарт-контракти як правомірні та обов'язкові до виконання. Це допомагає забезпечити юридичну опору та впевненість у використанні смарт-контрактів як альтернативи традиційним контрактам.

Тим не менш, застосування смарт-контрактів у системі Ethereum також має свої виклики та проблеми. Наприклад, можуть виникати питання щодо безпеки, масштабування та швидкодії системи, а також необхідності вдосконалення механізмів управління та голосування всередині децентралізованих організацій. Для вирішення цих проблем розробники Ethereum працюють над постійними оновленнями платформи та впровадженням нових технологій, таких як шардінг, протоколи стійкості до відмов та інші рішення.

Незважаючи на виклики, смарт-контракти на платформі Ethereum продовжують набирати обертів, перетворюючи багато традиційних бізнес-процесів та галузей на більш автоматизовані, прозорі та ефективні системи. Вони відкривають нові можливості для розвитку децентралізованих технологій та сприяють створенню глобальної, відкритої та взаємозв'язаної економіки.

* 1. Основні характеристики смарт-контрактів

Смарт-контракти є інноваційною технологією, яка змінює спосіб укладання та виконання угод у різних галузях. Вони мають ряд ключових характеристик, що відрізняють їх від традиційних контрактів:

1. Автоматизація: Смарт-контракти автоматично виконуються та контролюються комп'ютерною програмою, що дозволяє зменшити витрати на адміністрування та виконання угод.
2. Непохідність: Смарт-контракти записуються на блокчейні, що гарантує їх незмінність та неможливість зміни умов контракту без згоди всіх сторін.
3. Децентралізація: Смарт-контракти виконуються в децентралізованій мережі, як Ethereum, що позбавляє їх залежності від одного центрального органу чи сервера.
4. Прозорість: Умови смарт-контрактів доступні для перегляду всіма учасниками мережі, що забезпечує високий рівень прозорості та довіри між сторонами.
5. Ефективність: Завдяки автоматизації, смарт-контракти можуть знизити витрати на проведення та виконання угод, в той же час підвищуючи швидкість виконання.

Ці характеристики роблять смарт-контракти привабливими для ряду застосувань та галузей. Вони можуть бути використані для створення децентралізованих фінансових систем, в яких позики, депозити та страхові поліси можуть бути автоматично укладені та виконані без посередництва традиційних банків або фінансових установ.

Смарт-контракти також можуть бути використані в логістиці та постачанні, де вони можуть автоматизувати процеси, пов'язані з відстеженням вантажів, виконанням оплати та підтвердженням доставки товарів. У нерухомості смарт-контракти можуть спростити процес передачі права власності, автоматично виконуючи угоди та перевіряючи документи.

Основні характеристики смарт-контрактів роблять їх потужним інструментом для розвитку технологій та галузей в умовах децентралізації, автоматизації та прозорості. Завдяки їх широким можливостям, смарт-контракти продовжують залучати увагу користувачів та розробників по всьому світу.

Смарт-контракти надають можливості для реалізації децентралізованих додатків (dApps), які можуть функціонувати відкрито, безпечно та автономно на платформах, таких як Ethereum. dApps можуть мати різні форми, від простих голосувань та лотерей до складних платформ для децентралізованого фінансування та управління компаніями.

Одним з ключових аспектів смарт-контрактів є їх взаємодія з криптовалютами, такими як Ether (ETH) на платформі Ethereum. За допомогою смарт-контрактів користувачі можуть створювати токени, які представляють цінності або активи, та передавати їх іншим учасникам мережі, створюючи екосистеми власних криптовалют та децентралізованих економічних систем.

Загалом, смарт-контракти мають ряд основних характеристик, які роблять їх важливим інструментом для розвитку блокчейн-технологій та децентралізованих систем. Вони пропонують автоматизацію, непохідність, децентралізацію, прозорість та ефективність, що відкриває нові можливості для різних галузей та застосувань.

* 1. Принципи виконання смарт-контрактів на платформі Ethereum

Смарт-контракти в системі Ethereum використовують мережу блокчейн для забезпечення децентралізованого, безпечного та прозорого виконання угод. Розглянемо основні принципи виконання смарт-контрактів на платформі Ethereum:

1.3.1. Віртуальна машина Ethereum (EVM)

Віртуальна машина Ethereum (EVM) є середовищем, в якому виконуються смарт-контракти в мережі Ethereum. EVM є механізмом, який дозволяє розробникам створювати та виконувати децентралізовані додатки (dApps) на блокчейні Ethereum (4).

1.3.2. Газ

Газ є внутрішнім механізмом виміру ресурсів, необхідних для виконання операцій на платформі Ethereum, включаючи створення, виконання та взаємодію з смарт-контрактами. Газ вимірюється в одиницях та має певну вартість, яка виражається в криптовалюті Ether (ETH) .

1.3.3. Функції смарт-контрактів

Смарт-контракти в Ethereum містять функції, які виконують певні дії або завдання. Функції можуть виконуватись автоматично або в результаті взаємодії з іншими контрактами або користувачами. Кожна функція має певні вхідні та вихідні параметри та може змінювати стан смарт-контракту.

1.3.4. Тригери смарт-контрактів

Тригери смарт-контрактів - це події, які активують виконання певних функцій смарт-контракту. Тригери можуть бути зовнішніми (наприклад, взаємодія з користувачем або іншим контрактом) або внутрішніми (наприклад, виконання певної умови або досягнення певного часу). Тригери дозволяють смарт-контрактам реагувати на зміни умов та виконувати відповідні дії відповідно до вбудованих логічних правил.

1.3.5. Стан смарт-контрактів

Смарт-контракти в Ethereum мають певний стан, який зберігається на блокчейні. Стан смарт-контракту може включати різні дані, такі як баланси рахунків, інформацію про власників та інші змінні, пов'язані з логікою контракту. Зміни стану смарт-контракту здійснюються в результаті виконання функцій та взаємодії з іншими контрактами або користувачами.

1.3.6. Консенсус

Для забезпечення децентралізації та безпеки в системі Ethereum використовується механізм консенсусу, який дозволяє учасникам мережі погоджуватись на правильність виконання смарт-контрактів та стан блокчейну. До 15.09.22 Ethereum використовув механізм консенсусу Proof of Work (PoW), але з оновленням “The Merge” здійснив перехід на Proof of Stake (PoS).

PoS забезпечує безпеку та стабільність мережі, залучаючи учасників до процесу валідації транзакцій та формування блоків на основі їхньої "ставки" у формі криптовалюти Ether (ETH). Цей підхід замінює попередній механізм Proof of Work (PoW), який вимагав значних обчислювальних потужностей та енергоспоживання.

Зміна консенсусного механізму на PoS також впливає на роботу смарт-контрактів, забезпечуючи швидше та екологічно стале виконання угод та децентралізованих додатків на платформі Ethereum.

Загалом, смарт-контракти на платформі Ethereum виконуються в децентралізованому середовищі за допомогою віртуальної машини Ethereum (EVM). Основні принципи виконання смарт-контрактів включають використання газу, функцій, тригерів, стану та механізмів консенсусу, які спільно дозволяють створювати автоматичні, безпечні та прозорі взаємодії між учасниками мережі.

# Дослідження проблем регулювання та правового статусу смарт-контрактів у різних країнах світу

2.1 Правове регулювання смарт-контрактів у США.

Правове регулювання смарт-контрактів у США знаходиться на етапі розвитку, але вже встановлені певні правила та норми, які регулюють сферу криптовалют та технологій блокчейн, включаючи смарт-контракти.

2.1.1 Федеральне регулювання

На федеральному рівні, смарт-контракти регулюються декількома установами. Наприклад, Комісія з цінних паперів та бірж (SEC) має право регулювати смарт-контракти, якщо вони відносяться до цінних паперів, зокрема у сфері ICO (первинних розміщень монет) та токенів.

Крім того, Фінансові злочини мережі правоохоронних органів (FinCEN) можуть відстежувати смарт-контракти, якщо вони використовуються для передачі віртуальних валют, які підпадають під дію банківського секретаріату.

2.1.2 Штатні закони

Деякі штати у США також розглядають смарт-контракти в контексті своїх законодавчих актів. Наприклад, штат Аризона в 2017 році прийняв закон, який визнає смарт-контракти як законні угоди. Закон забезпечує, що смарт-контракти мають те ж саме правове значення, що й традиційні контракти, якщо вони відповідають всім необхідним вимогам.

2.1.3 Визначення правового статусу

Оскільки смарт-контракти є новим і відносно маловивченим

явищем, визначення їх правового статусу у США є складним завданням. Загалом, смарт-контракти можуть вважатися дійсними та обов'язковими угодами, якщо вони відповідають основним вимогам до угод, встановленим у договірному праві. Це включає волевиявлення сторін, предмет угоди, умови виконання та відповідність законодавству.

У контексті смарт-контрактів можливі юридичні питання, такі як відповідальність сторін за помилки або зловживання, встановлення особи, що несе відповідальність за виконання смарт-контракту, а також можливість вирішення суперечок у судовому порядку.

2.1.4 Майбутнє правового регулювання

В майбутньому правове регулювання смарт-контрактів у США, ймовірно, буде розвиватися разом із розвитком технології блокчейн та криптовалют. Це може включати розширення дії існуючих законодавчих актів або створення нових норм, що спеціально стосуються смарт-контрактів. Зокрема, можуть з'явитися нові норми щодо захисту споживачів, прозорості та безпеки, а також стандарти для розвитку та використання смарт-контрактів.

2.2 Правове регулювання смарт-контрактів у Європейському Союзі.

2.3 Правове регулювання смарт-контрактів у Азійських країнах.

2.4 Порівняльний аналіз правового регулювання смарт-контрактів у різних країнах.

# Розгляд особливостей програмування смарт-контрактів на мові Solidity та їхні взаємодії зі зовнішніми додатками

* 1. Основи мови програмування Solidity.
  2. Створення та виконання смарт-контрактів на Solidity.
  3. Взаємодія смарт-контрактів зі зовнішніми додатками.
  4. Рішення та платформи для розробки та виконання смарт-контрактів.

# Аналіз проблем безпеки, що виникають при розробці та використанні смарт-контрактів у системі Ethereum

4.1 Загальні проблеми безпеки смарт-контрактів.

4.2. Типові атаки на смарт-контракти та способи їх запобігання.

4.3. Приклади значущих інцидентів з безпекою смарт-контрактів в Ethereum.

# ВИСНОВОК

# ПЕРЕЛІК ПОСИЛАНЬ

# ДОДАТОК А

# ДОДАТОК Б

# Вихідний код контракту

Функция

Функция