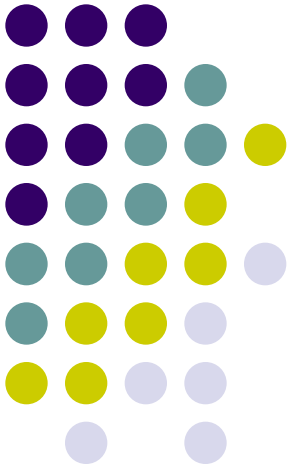
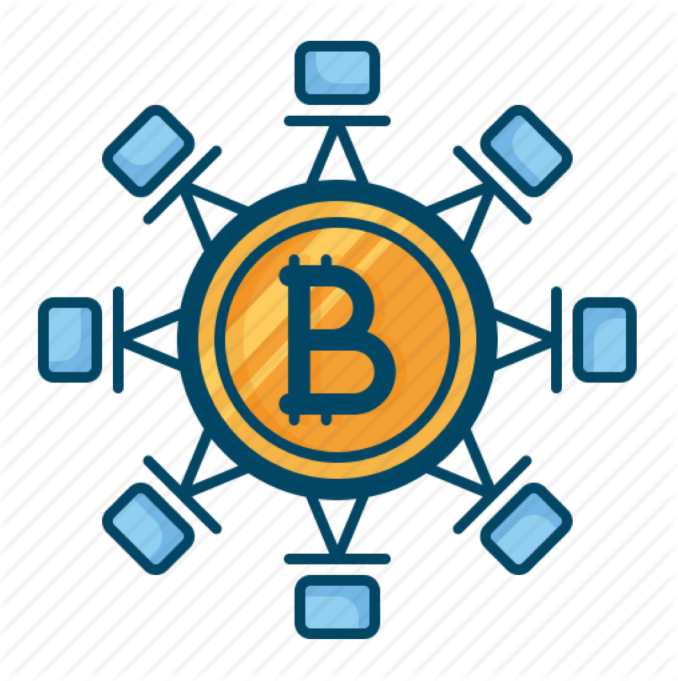
Криптографічні алгоритми для генерації ключів на основі технології Blockchain

Студент 2–го курсу групи КА-83мп
Панасюк І.В.
Науковий керівник
Кандидат фізтико-математичних наук, доцент
Шубенкова І.А.

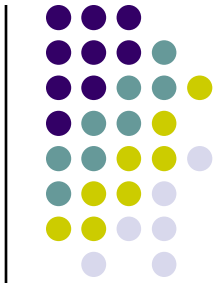




«When I first heard about Bitcoin, I thought it was impossible. How can you have a purely digital currency? Can't I just copy your hard drive and have your bitcoins? I didn't understand how that could be done, and then I looked into it and it was brilliant"»

Jeff Garzik

Зміст дисертації



- **Вступ**
- Розділ 1. Blockchain.Загальні риси
- Розділ 2. Платіжні системи та Bitcoin
- Розділ 3. Математика криптовалют
- Розділ 4. Реалізація застосування криптографічних алгоритмів
- Розділ 5. Проектування стартапу
- Висновок

Короткі відомості

- Об’єкт дослідження – технологія Blockchain основуючись на якій створенна більшість із криптовалют.
- Предмет дослідження – сучасна криптографія та технологія Blockchain.
- Методи дослідження – технологія блокчейн, концепції створення криптовалюти та сам принцип роботи BTC.

Актуальність:

Актуальність дослідження обумовлена:

- Необхідністю диверсифікації повноважень контролю фінансів.
- Відсутністю валютної едності.
- Потребі в безпеці та швидкості.

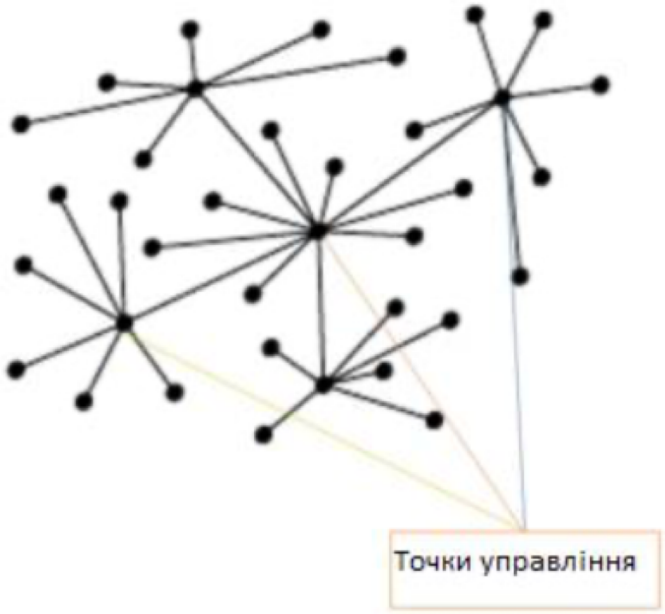
Ціль роботи

Проаналізувавши технологію Blockchain та принципи роботи криптовалюти Bitcoin, поглибленно і всебічно розглянути криптографію як спосіб захисту інвестиційних фінансів для збільшення довіри кінцевого користувача до технології Blockchain .

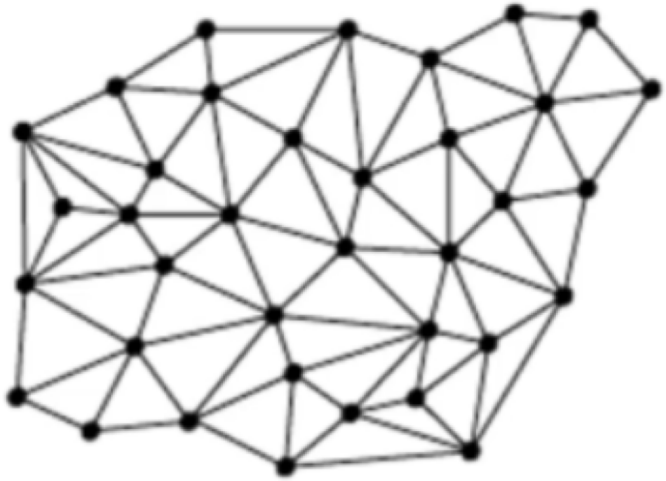
Задачі:

- Проведеня аналізу систем управління;
- Вивчення проблематик, розв'язуваних данною технологією;
- Аналіз різновидів платіжних систем;
- Дослідження процесів шифрування;
- Вивчення питань надійності технології;
- Розробка продукту з подальшим його розвитком.

Централізація чи децентралізація?



Розподілені системи



Всі точки мають рівні повноваження

- НЕ ІСНУЄ єдиної точки управління, або ж УСІ ТОЧКИ - є точками управління
- Фактично несприйнятливі до падінь
- Повністю горизонтальна ієрархія

Види платіжних систем

- Бартерна платіжна система
- Монетна платіжна система
- Паперова платіжна система
- Чекова платіжна система
- Платіжна система електронних гаманців

ЯК ПРАЦЮЄ BITCOIN?

Майнери створюють біткоїни, використовуючи комп'ютери для вирішення математичних функцій. Аналогічний й процес для підтвердження попередніх транзакцій в системі.

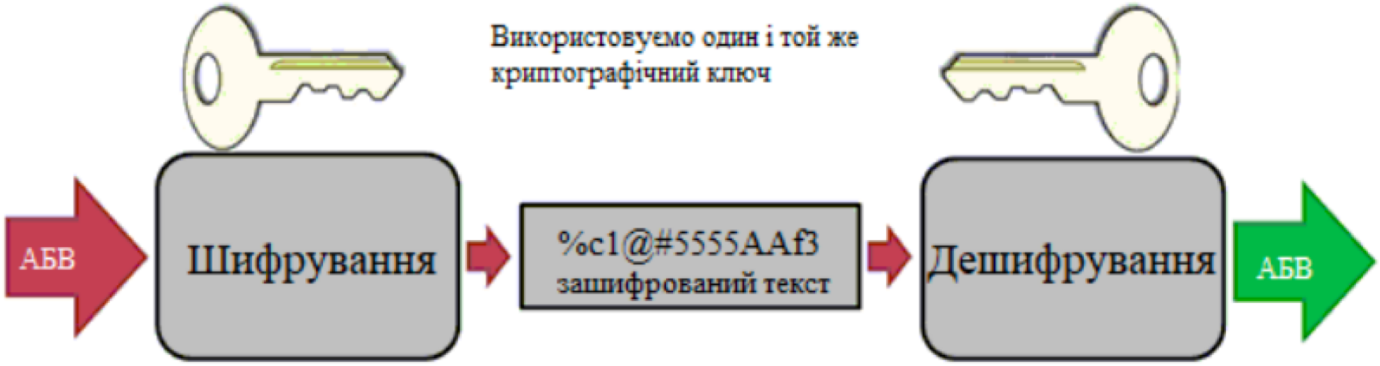
Обмін біткоїнами дозволяє виробляти торги з традиційними валютами, даючи "не-Майнерам" шлях на ринок, а також як спосіб обміну біткоїнів на фіатні гроші

Користувач завантажує біткоїн-гаманець, робота якого нагадує e-mail адресу, що забезпечує можливість зберігати та приймати електронні гроші. Біткоїни можна відправляти з одного гаманця на інший, використовуючи браузер або мобільний додаток

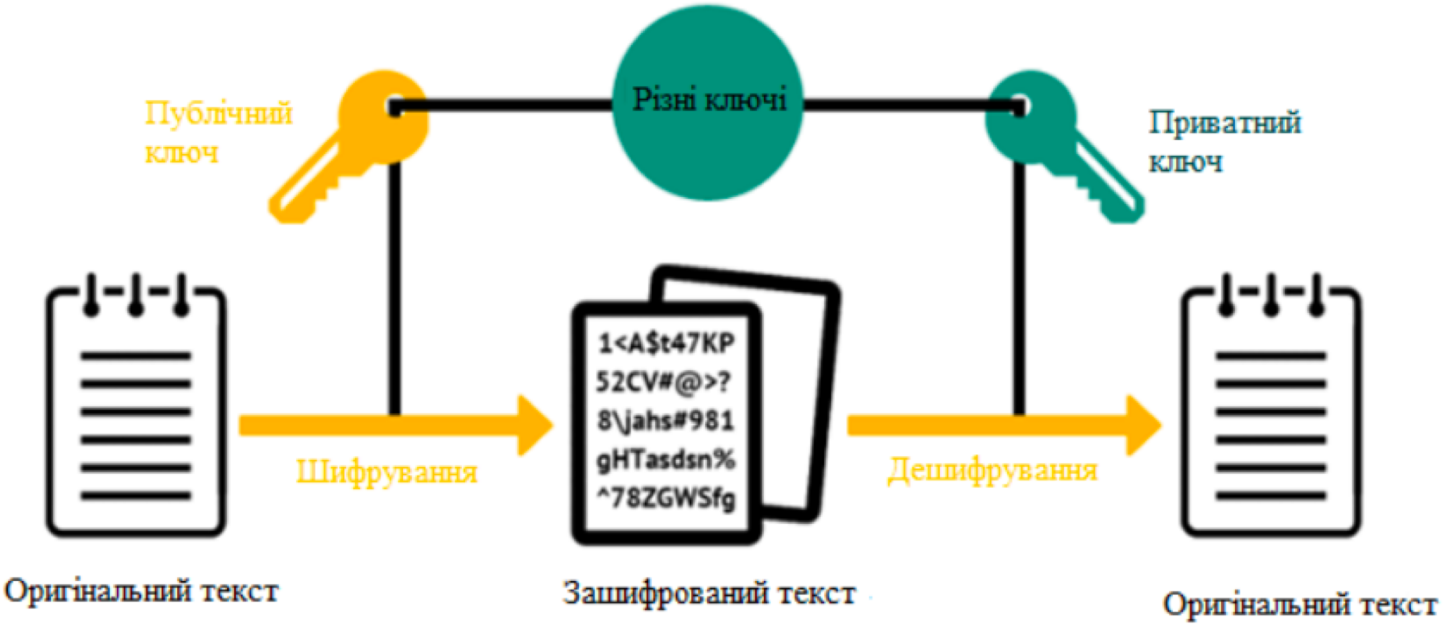
Для спрощення і прискорення оплати клієнти, можуть використовуватис QR-коди

Математика криптовалют

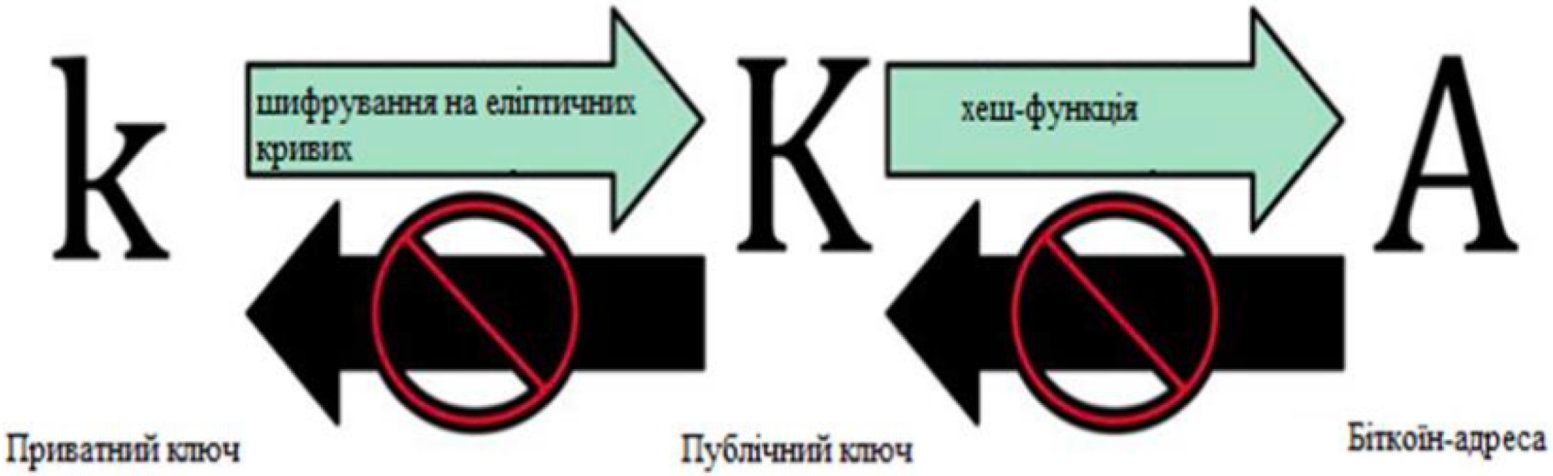
Симетричне шифрування



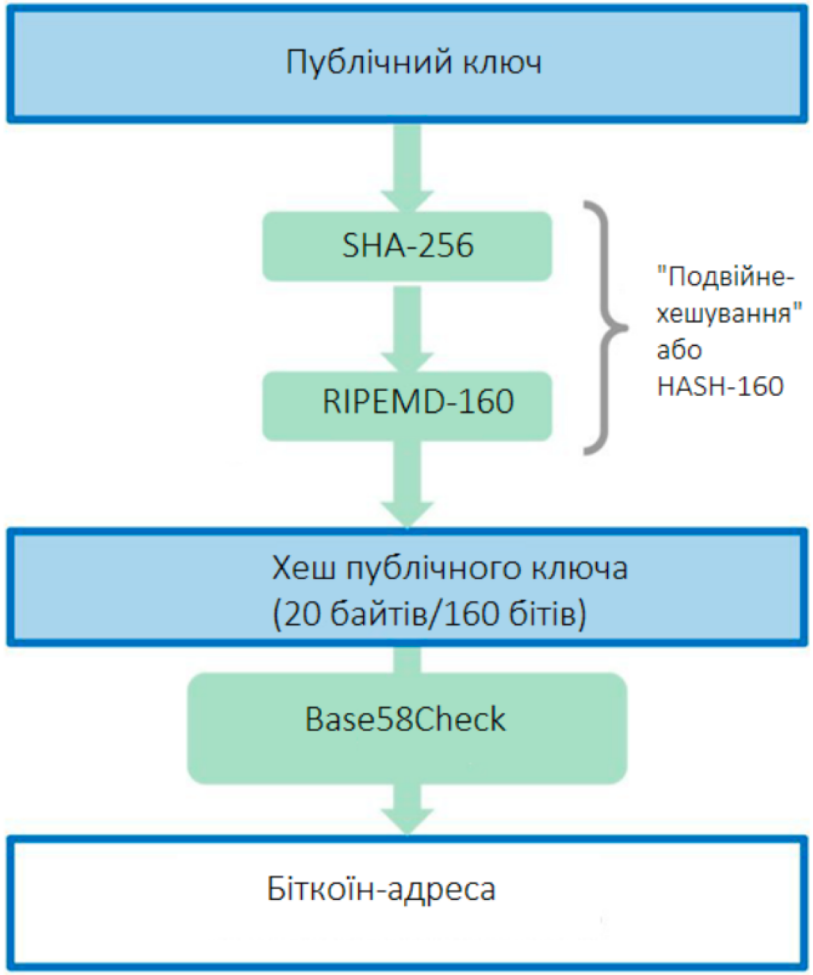
Асиметричне шифрування



Приватні та публічні ключі



Створення Біткоїн-адреси

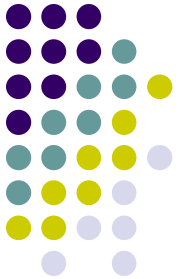


Висновок

В ході роботи було досліджено які саме криптографічні алгоритми використовуються на базі технології Blockchain в криптовалюті Bitcoin. Слід зазначити, що теоретична база хоч і активно розвивається і є перспективною, проте дана технологія є ще не надто добре вивчена.

На мій погляд, ті програмні продукти, які будуть базуватись на технології Blockchain є в апріорі перспективним напрямком сучасних досліджень по децентралізації сховищ даних та створенню смарт-контрактів.

Однією з цілей даної магістерської дисертації було переконатись і упевнитись, що технології блокчейн слід довіряти, адже вона має один з найцінніших, найперконливіших аргументів, - дана технологія побудована на математичних принцпипах, а математиці варто довіряти.



Дякую за увагу