

## ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

# Аналіз та створення NFT за допомогою біткоїн інскрипцій

ЗДОБУВАЧ Матвій ЖИГАЛКА  
ГРУПА КІУКІ-21-2

Керівник ас. каф. Віталій  
СПІШКОВ

## Мета та задачі

2

- ▶ Метою кваліфікаційної роботи є дослідження інноваційного підходу до створення цифрових активів у мережі Bitcoin шляхом реалізації інскрипцій на основі протоколу Ordinals.

### Задачі

- ▶ Розглянути принцип та структуру блокчейну Bitcoin
- ▶ Дослідити розвиток протоколу Ordinals та концепції інскрипції
- ▶ Розглянути технологічні особливості створення NFT у мережі Bitcoin
- ▶ Реалізувати інскрипції у тестовій мережі Signet

3

## Основи Bitcoin

Поява у 2008–2009 роках

Мета — фінансова свобода без посередників

Унікальність — блокчейн, прозорість, обмежена емісія.



4

## Принципи роботи блокчейн

- Розподіленість між усіма вузлами;
- Незмінність і перевірка через консенсус;
- Захист від фальсифікацій.



5

## Що таке NFT?

- Унікальність (не існує двох однакових NFT)
- Прив'язка до блокчейну
- Можливість торгівлі на маркетплейсах



6

## Taproot, SegWit та поява Ordinals



### SegWit

Змінює структуру блоку, відокремивши дані підписів (witness) від основної транзакції



### Taproot

Довільні дані у поле witness



### Ordinals

Дозволяє зберігати зображення, текст, HTML та інші дані безпосередньо в блокчейні Bitcoin

# Ordinals Protocol

7

- Інскрипції в Bitcoin
- Прив'язка даних до сатоші
- NFT без токенів
- Дані зберігаються ончейн

# Signet

8

- ✓ Стабільність
- ✓ Підтримка Ordinals
- ✓ Faucet для токенів
- ✓ Придатність для розробки

## Підготовка середовища

9

```

root@DESKTOP-8B8GLU4:~# cd ord
root@DESKTOP-8B8GLU4:~/ord# ./target/release/ord \
  --s lgnrt \
  --bitcoin-rpc-url http://127.0.0.1:38332 \
  --bitcoin-rpc-username bitcoinuser \
  --bitcoin-rpc-password bitcoinpass123 \
  server
Listening on http://0.0.0.0:80

```

```

root@DESKTOP-8B8GLU4:~# bitcoin-cli -s signet getblockchaininfo
{
  "chain": "signet",
  "blocks": 255779,
  "headers": 256302,
  "bestblockhash": "000000004e7383909e22194c0507e5a171eddbf417b15571c86dc1e60",
  "difficulty": 0.04759951218839534,
  "time": 1749039815,
  "mediantime": 1749239099,
  "verificationprogress": 0.999345709132729,
  "initialblockdownload": true,
  "chainwork": "00000000000000000000000000000000000000000000000000000041fcb5a6d",
  "size_on_disk": 11298309981,
  "pruned": false,
  "warnings": ""
}
root@DESKTOP-8B8GLU4:~# bitcoin-cli -s signet getblockchaininfo
{
  "chain": "signet",
  "blocks": 256302,
  "headers": 256302,
  "bestblockhash": "00000000459a3f67b89c45489ca41f8cc75445828b46e8c386ae72b47062",
  "difficulty": 0.05017417001347472,
  "time": 1749042711,
  "mediantime": 1749029953,
  "verificationprogress": 0.999997388535378,
  "initialblockdownload": false,
  "chainwork": "00000000000000000000000000000000000000000000000000000045ca806e7b",
  "size_on_disk": 11023431145,
  "pruned": false,
  "warnings": ""
}

```

## Запуск утиліти ord

10

Синхронізація з Bitcoin Core  
 Індексція Taproot-транзакцій  
 Локальний HTTP-сервер

```

root@DESKTOP-8B8GLU4:~# cd ord
root@DESKTOP-8B8GLU4:~/ord# ./target/release/ord \
  --s lgnrt \
  --bitcoin-rpc-url http://127.0.0.1:38332 \
  --bitcoin-rpc-username bitcoinuser \
  --bitcoin-rpc-password bitcoinpass123 \
  server
Listening on http://0.0.0.0:80

```

## Запуск утиліти ord

10

Синхронізація з Bitcoin Core  
Індексація Taproot-транзакцій  
Локальний HTTP-сервер

```
root@DESKTOP-BR8GLU4:~# cd ord
root@DESKTOP-BR8GLU4:~/ord# ./target/release/ord \
--signet \
--bitcoin-rpc-url http://127.0.0.1:38332 \
--bitcoin-rpc-username bitcoinuser \
--bitcoin-rpc-password bitcoinpass123 \
server
Listening on http://0.0.0.0:80
```

## Отримання тестових токенів

12

Адреса <https://ordinals.com/address/00>

Confirmed balance	0.00000000 BTC	Unspendable	+0.00000000 BTC
Confirmed UTXOs	1	Pending UTXOs	0
Відомі транзакції	0.00000000 BTC	Тут	<a href="#">more</a>

1 of 1 transaction

```
root@DESKTOP-BR8GLU4:~/ord# ./target/release/ord --signet \
--bitcoin-rpc-url http://127.0.0.1:38332 \
--bitcoin-rpc-username bitcoinuser \
--bitcoin-rpc-password bitcoinpass123 \
wallet create
{
  "output": "0b6167a361097efccf0c9638a3f9d991586e8d31754883eca9f2a63a32391526",
  "txid": "3784d"
}
```

## Підготовка файлу для інскрипції

13



3.71 MB (3 896 137 байт)



884 байт (884 байт)

```
root@DESKTOP-BRGLQJ:~/ord# cwebp cats.png --resize 50 50 -q 20 -o cats.webp
Saving file 'cats.webp'
File:   cats.png
Dimension: 50 x 50 (with alpha)
Output: 884 bytes Y-U-V-All-PSNR 31.34 36.32 36.71 32.31 dB
        (7.83 bpp)
Block count:  intra0: 9 (56.25%)
              intra16: 7 (43.75%)
              skipped: 2 (12.50%)
bytes used:  header: 33 (5.7%)
              mode-partition: 47 (5.3%)
              transparency: 416 (99.0 dB)
Residuals bytes: segment 1|segment 2|segment 3|segment 4| total
macroblocks: 19% | 19% | 21% | 31% | 16
quantizer: 78 | 66 | 56 | 48 |
filter level: 38 | 15 | 9 | 7 |
Lossless-alpha compressed size: 415 bytes
* Header size: 39 bytes, image data size: 376
* Precision Bits: histogram=5 transform=5 cache=0
* Palette size: 151
```

## Створення інскрипції

14

```
root@DESKTOP-BRGLQJ:~/ord# ./target/release/ord --signet \
--bitcoin-rpc-url http://192.0.2.1:8332 \
--bitcoin-rpc-username bitcoinduser \
--bitcoin-rpc-password bitcoindpass123 \
mallet inscribe \
--fee-rate 50 \
--file cats.webp
{
  "commit": "79f704888036711e99ee8b7aeadbda0451dde1196803e15018b7a329d6f0b",
  "commit_p2sh": null,
  "inscriptions": [
    {
      "destination": "f01pvkpy70t9yzn19i0exrf6gqhl436cypz3sja2tfgafxsmu44h6x6tsnfjz2m",
      "id": "bf0642c5ecd1ba1cd863cd1e6c06491e4adc0ec3acc22b48858ab988879c9c0",
      "location": "bf498642c5ecd1ba1cd863cd1e6c06491e4adc0ec3acc22b48858ab988879c9c0:0"
    }
  ],
  "parents": [],
  "reveal": "bf498642c5ecd1ba1cd863cd1e6c06491e4adc0ec3acc22b48858ab988879c9c",
  "reveal_broadcast": true,
  "reveal_p2sh": null,
  "fee": null,
  "total_fee": 5118
}
```

- **Інскрипція (ID):**  
bf0642c5ecd1ba1cd863cd1e6c06491e4adc0ec3acc22b48858ab988879c9c0
- **Адреса призначення:**  
tb1pvkpy70t9yzn19i0exrf6gqhl436cypz3sja2tfgafxsmu44h6x6tsnfjz2m
- **Місце знаходження в блокчейні:**  
bf0642c5ecd1ba1cd863cd1e6c06491e4adc0ec3acc22b48858ab988879c9c:0:0
- **Коміт-транзакція (commit):**  
707fdd00036731e59ee8b7aeadbda0451dde1196803e15018b7a329d6f0b

**Транзакція** [bf0642c5ecd1ba1cd863cd1e6c06491e4adc0ec3acc22b48858ab988879c9c0](#)

Назва: 2023-09-14 17:50:51

Вартість: 1.570 BTC (150 USD)

Процедура: Після 4 днів

Стан коміт: 100

Еквівалент: **0.00000000 BTC**

**Потік**

**Входи і Виходи**

**Деталі**

Код	134	Вартість	2
Корупційний розмір	2903	Назва блокчейна	0
Корупційний вказівник ID	2903	Стор. ID	0

## Перевірка результату

15



## Висновки

16

- ▶ В ході кваліфікаційної роботи було створено NFT за допомогою біткоїн інскрипцій.

Задачі які було вирішено

- ▶ Розглянуто принципи та структура блокчейну Bitcoin
- ▶ Досліджено розвиток протоколу Ordinals та концепції інскрипції
- ▶ Розглянуто технологічні особливості створення NFT у мережі Bitcoin
- ▶ Реалізована інскрипція у тестовій мережі Signet