TITLE OF YOUR REPORT

YOUR NAMES

DECEMBER 23, 2023

ABSTRACT. **This sample file is about the DeFi project Ordinals.** The Ordinals protocol applies ordinal theory to the Bitcoin blockchain, endowing the smallest Bitcoin unit, the satoshi, with unique identifiers, enabling tracking, transferring, and assigning meaning. This technology allows for inscriptions on the Bitcoin blockchain, transforming it into a platform for storing digital assets and broadening its application scope. Its main use includes issuing NFTs on Bitcoin, allowing artworks to be stored on the blockchain. Despite Ordinals bringing innovation to Bitcoin, it still faces several developmental limitations.

1 Introduction

This project utilizes a method known as "Ordinal Theory." Simply put, it assigns a unique identifier to every smallest unit of Bitcoin, called satoshi. You can add special elements to these identifiers, like images, text, or videos. This renders each satoshi unique and meaningful, akin to an NFT.

2 Core Technology: Assigning Ordinals

The goal of the Ordinals project is to provide stable identifiers for Bitcoin. In this system, the first transaction of each Bitcoin block, known as the coinbase transaction, includes the block reward, comprising new bitcoins created in the block (subsidy) plus transaction fees as the miner's reward. The subsidy, a fixed number of bitcoins, corresponds to the smallest bitcoin unit in the new block. The numbering scheme is 0-based, assigning numbers to each satoshi as they are mined. The transfer mechanism is first-in-first-out and handles transactions with duplicate IDs, prioritizing new transactions over old ones.

The key points are expressed in a bullet-point format as follows:

- **Coinbase Transaction**: The first transaction in a block.
  - **Block Reward**: Equals the subsidy (new bitcoins created in the block) plus transaction fees.
    - **Subsidy**: A fixed number of bitcoins for miners, equal to the smallest bitcoin unit in the new block.

  - **Implicit Input**: Inputs not originating from previous transactions.
    - **Coinbase**: Transactions with implicit input equal to the subsidy.

- **Numerating Scheme**:
  - 0-based "ordinals."
  - Each satoshi is numbered in the order it is mined.

- **Transferring Scheme**:
  - Input to output: FIFO (First-In, First-Out).
  - Handling duplicate IDs: New outputs take priority, invalidating unspent outputs in old transactions with the same ID.

The algorithm is as follows:

```python
# subsidy of block at given height
def subsidy(height):
    return 50 * 100000000 >> height // 210000

# first ordinal of subsidy of block at given height
def first_ordinal(height):
    start = 0
    for height in range(height):
        start += subsidy(height)
    return start

# assign ordinals in given block
def assign_ordinals(block):
    first = first_ordinal(block.height)
    last = first + subsidy(block.height)
    coinbase_ordinals = list(range(first, last))

    for transaction in block.transactions[1:]:
        ordinals = []
        for input in transaction.inputs:
            ordinals.extend(input.ordinals)

        for output in transaction.outputs:
            output.ordinals = ordinals[:output.value]
            del ordinals[:output.value]

        coinbase_ordinals.extend(ordinals)

    for output in block.transaction[0].outputs:
        output.ordinals = coinbase_ordinals[:output.value]
        del coinbase_ordinals[:output.value]
```

In the Ordinals system, each new satoshi created at the beginning of a blockchain block (equal to the subsidy) is assigned an ordinal number. The ordinal numbers within each block range from `first` to `first + subsidy`, and these are stored in `coinbase_ordinals[]`.

- **First Ordinal Calculation:** It is the cumulative sum of all subsidies starting from 0 for each block height.

```
def first_ordinal(height):
    start = 0
    for height in range(height):
        start += subsidy(height)
    return start
```

- **Subsidy Calculation:** The subsidy for each block height.

```
def subsidy(height):
    return 50 * 100_000_000 >> height // 210_000
```

- **Assigning Ordinals:** Starting from the second transaction, 'input.ordinals' equals the 'output.ordinals' of the previous transaction. The 'output.ordinals' are assigned from the list of available ordinals and then removed to avoid duplication.

Sat Point: The location of a satoshi in an output is defined as 'transaction ID : output ID : offset of the sat in this output'.

2.1 Embedding NFTs in Bitcoin Transactions

Having learned how to assign an identifier to each satoshi, we arrive at an even more crucial question: How do we embed our desired content into transactions, similar to NFTs Embedding NFTs in Bitcoin transactions involves the use of a scripting language.

There are two types of scripts:

- **ScriptPubKey**: Located in the transaction output, it defines the conditions to spend the output.
- **ScriptSig**: Located in the transaction input, it provides the necessary data to meet the conditions set by ScriptPubKey.

When a transaction occurs, ScriptPubKey combines with ScriptSig, and the script is executed. If the script executes successfully, the transaction is validated.

Key Points:

- Scripts are collections of opcodes, which are commands or instructions performing specific operations.
- The opcode `OP_RETURN` allows embedding arbitrary data onto a transaction. However, it renders the transaction unspendable, meaning no satoshi is actually carried by this output.

- **Relation to Ordinals:** The idea is to associate specific data with a group of satoshis. This is done by embedding the data onto the blockchain through transactions with `OP_RETURN`, associating it with the transaction's outputs (satoshis).

3 Key advantages of Ordinals

1. **Immutable Digital Content Integration:** Ordinals directly integrates immutable digital content into the Bitcoin blockchain. This process, requiring no additional layers or protocol changes, leverages the inherent security and immutability of the blockchain, enhancing the value and authenticity of digital assets like art.

2. **BRC-20 Tokens on Bitcoin Blockchain:** The Ordinals protocol facilitates the creation of BRC-20 tokens, a type of fungible token on the Bitcoin chain. This is achieved by embedding script files into the blockchain, representing specific satoshis as tokens, providing a novel way of token representation on Bitcoin.

3. **Enhancing Bitcoin's Utility:** By enabling the storage of digital assets on the blockchain, Ordinals maximizes the utility of Bitcoin. It potentially paves the way for future applications like off-chain colored-coins and decentralized DNS alternatives, leveraging blockchain's transparency and security.

4 Challenges Faced by Ordinals

1. **Development Bottlenecks and Limited Tools:** Given its recent introduction, coupled with inherent development constraints such as Bitcoin's inability to run smart contracts and incompatibility with EVM, the tools available for building and trading on Ordinals are still limited. Additionally, it competes with BTC for the valuable block space, potentially leading to higher transaction fees and strain on the Layer 2 solutions.

2. **Lack of Recognition by Bitcoin Blockchain:** The Bitcoin blockchain does not inherently recognize the numbering system used by Ordinals. Furthermore, the official stance of Bitcoin does not particularly favor the development of Ordinals, presenting an additional challenge to its adoption and integration within the Bitcoin ecosystem.

5 Related Tools for Ordinals in Bitcoin Blockchain

5.1 Ordinals: A Tool for Bitcoin Blockchain Inscriptions

The Ordinals project introduces a novel tool named `'ord'`, specifically designed to facilitate inscriptions on the Bitcoin blockchain. These inscriptions serve as a method to embed various forms of data directly into the Bitcoin blocks, thus expanding the blockchain's utility beyond just financial transactions. Detailed instructions and operational guidelines for using the `'ord'`

tool can be found at Ordinals Documentation. The key steps involved in utilizing `'ord'` for blockchain inscriptions are as follows:

5.1.1 Step 1: Installing and Configuring Bitcoin Core

The initial step requires the installation and configuration of Bitcoin Core, the software that serves as the backbone for running a full Bitcoin node. This process involves synchronizing with the entire Bitcoin blockchain, ensuring that the user has a local copy of all transactions ever recorded on the network.

5.1.2 Step 2: Creating a Bitcoin Core Wallet Using `'ord'`

Once Bitcoin Core is set up, the next step is to use the `'ord'` tool to create a dedicated wallet within Bitcoin Core. The `'ord'` tool is versatile, enabling users to receive Satoshis (the smallest unit of Bitcoin), create inscriptions by specifying files and setting transaction fees, and send or receive inscribed transactions. It's important to note that the size of the inscription directly influences the transaction fees incurred.

5.1.3 Step 3: Inscribing Data on the Bitcoin Blockchain

The final step involves the actual inscription process, where the selected data gets permanently embedded in a specific Bitcoin transaction. This action ensures that the inscription becomes an immutable part of the Bitcoin blockchain, accessible and verifiable by anyone using the blockchain.

5.2 Automation Tools for Inscription Processes

In addition to the manual process using the `'ord'` tool, several online platforms offer automated solutions for creating inscriptions on the Bitcoin blockchain. One such platform is Gamma (https://gamma.io/ordinals), which simplifies the process, making it more accessible to users without deep technical knowledge of the underlying blockchain technology.

6 Conclusion

In conclusion, the Ordinals project represents a significant step forward in the realm of Bitcoin and blockchain technology. By uniquely identifying each satoshi and enabling the embedding of rich, varied content directly onto the blockchain, Ordinals not only enhances the utility of Bitcoin but also opens up a new world of possibilities for digital assets. While it faces challenges and limitations in its current form, the potential of Ordinals to revolutionize how we view and interact with blockchain technology is undeniable. As the project evolves, it may play a pivotal role in shaping the future of digital transactions and asset management.

References

[1] The Text shown in the document

[2] GitHub of Ordinals