

Swinburne University of Technology

Project Design Document

Marco Giacoppo (104071453)

Corey Santarossa (103389809)

Chaitanya Sood (103501933)

Tuesday 10:30

2023 Semester 2

Table of Contents

[Project Design Document 1](#_Toc149908318)

[PROJECT INFORMATION 2](#_Toc149908319)

[1 PROJECT NAME: Uniswap V3 Core 2](#_Toc149908320)

[2 PROJECT DESCRIPTION 2](#_Toc149908321)

[3 TEAM INFORMATION 2](#_Toc149908322)

[4 VERSION INFORMATION 3](#_Toc149908323)

[EXECUTIVE SUMMARY 4](#_Toc149908324)

[ABI ILLUSTRATION 4](#_Toc149908325)

[CALL GRAPH DISCUSSION 5](#_Toc149908326)

[INHERITANCE GRAPH DISCUSSION 9](#_Toc149908327)

[Appendix 10](#_Toc149908328)

## PROJECT INFORMATION

### 1 PROJECT NAME: Uniswap V3 Core

### 2 PROJECT DESCRIPTION

The Uniswap V3 Core smart contract represents a fundamental building block of the Uniswap decentralized exchange protocol. This protocol is at the forefront of the decentralized finance (DeFi) movement, enabling trust less and automated exchange of cryptocurrency assets on the Ethereum blockchain. Uniswap, with its innovative approach to liquidity provision, offers users the opportunity to swap tokens, provide liquidity to pools, and earn fees in a decentralized, non-custodial, and permissionless manner.

### 3 TEAM INFORMATION

We are a team of computer scientists from Swinburne University, brought together by our shared dedication to innovation and technology. As students pursuing our Bachelor of Computer Science degrees, we are excited to embark on the journey of creating an NFT trading platform that seamlessly merges the worlds of art, technology, and finance.

* Marco Giacoppo (104071453)
* Corey Santarossa (103380809)
* Chaitanya Sood (103501933)

Collectively, we bring a fusion of technical competency, design finesse, and strategic thinking to this project. With or education at Swinburne as the foundation, we are eager to learn, collaborate, and make a meaningful contribution to blockchain technology and NFTs.

### 4 VERSION INFORMATION

**Smart Contract Version:**

The Uniswap V3 Core smart contract, as of the time of this analysis, is in 1.0.1 version. It’s essential to note that smart contracts can evolve over time as developers make updates and improvements to the protocol. Therefore, the version specified here may change in the future. Please note that the "Smart Contract Version" corresponds to the version of the Uniswap V3 Core smart contracts, which is 1.0.1 in this case. The "Dependencies Version" section lists the versions of libraries and frameworks used within the project. These versions are based on the information provided in the `package.json` file of the Uniswap V3 Core project.

**Dependencies Version:**

Uniswap V3 Core, like many Ethereum-based projects, relies on various libraries and frameworks to enhance its functionality and security. In the context of Ethereum, libraries such as OpenZeppelin are commonly utilized to provide standardized, secure smart contract functionality.

At the time of this analysis, the specific version of dependencies used in the Uniswap V3 Core project were as follows:

* `**@nomiclabs/hardhat-ethers**` : ^2.0.2
* **`@nomiclabs/hardhat-etherscan**` : ^2.1.8
* **`@nomiclabs/hardhat-waffle**` : ^2.0.1
* **`@typechain/ethers-v5`** : ^4.0.0
* **`@types/chai**` : ^4.2.6
* **`@types/mocha**` : ^5.2.7
* `**chai**` : ^4.2.0
* `**decimal.js**` : ^10.2.1
* `**ethereum-waffle**` : ^3.0.2
* `**ethers**` : ^5.0.8
* `**hardhat**` : ^2.2.0
* `**hardhat-typechain**` : ^0.3.5
* `**mocha**` : ^6.2.2
* `**mocha-chai-jest-snapshot**` : ^1.1.0
* **`prettier**` : ^2.0.5
* `**prettier-plugin-solidity**` : ^1.0.0-alpha.59
* `**solhint**` : ^3.2.1
* **`solhint-plugin-prettier**` : ^0.0.5
* **`ts-generator**` : ^0.1.1
* `**ts-node**` : ^8.5.4
* `**typechain**` : ^4.0.0
* `**typescript**` : ^3.7.3

Please note that the versions of these dependencies are subject to updates and changers as the project develops. It is crucial for developers and auditors to stay informed about the most current versions to ensure the smart contract’s security and compatibility.

## EXECUTIVE SUMMARY

This report presents a comprehensive analysis of the Uniswap V3 Core smart contract, a cornerstone of the Uniswap decentralized exchange protocol. Uniswap’s pivotal role in the decentralized finance (DeFi) landscape necessitates a deep understanding of its core components, and this analysis focuses on uncovering the inner working of the Uniswap V3 Core contract. By examining the contract’s ABI, call graph, and inheritance hierarchy, we gain valuable insights into the contract’s design, functionality, and its place within the broader DeFi ecosystem.

This report provides an in-depth exploration of the Uniswap V3 Core smart contract at a specific point in time. It is imperative to acknowledge that smart contracts, by their nature, are dynamic and can evolve over time as developers implement upgrades and optimizations. As such, this analysis provides a snapshot of the contract's state and its functional aspects during the time of examination.

Comprehending the intricacies of the Uniswap V3 Core smart contract is essential for developers, auditors, and stakeholders who engage with the Uniswap V3 protocol. By offering these insights, we aim to contribute to a deeper understanding of decentralized exchange platforms within the broader blockchain ecosystem. Our analysis seeks to empower users and developers by enhancing transparency and knowledge of the Uniswap V3 Core contract's operation.

## ABI ILLUSTRATION

The ABI (Application Binary Interface) of the Uniswap V3 Core smart contract serves as the gateway to its functions. Our analysis of the ABI revealed not only the technical structure of the contract but also the extent to which it leverages documentation and comments to enhance its transparency. This detailed examination unearthed the primary logic and functionality of individual functions within the contract, affording us an invaluable glimpse into its codebase. We will now provide an analysis on the main contracts within the Uniswap codebase (minus the bytecode).

1. **NoDelegateCall ABI (See Appendix A)**

The ABI in NoDelegateCall is an empty array. This is because the contract only has one function which is private, therefore not shown in the ABI. The contract itself is a base contract providing a modifier for other contracts. The commenting in this contract is clear and concise, as is the code structure.

Functions:

* checkNotDelegateCall: checks that the contract being used is the original contract by comparing the contract address to the original address.

1. **UniswapV3Factory ABI (See Appendix B)**

The ABI in UniswapV3Factory contains a combination of the constructor, events and functions. The code appears to have clear structure and clear commenting.

Functions:

* createPool: A non-payable function taking in two tokens and a fee. This function creates a pool to prepare for a tokenswap and returns the pool address.
* enableFeeAmount: Enables a new fee amount.
* SetOwner: Takes an address and sets it as the new contract owner. The user calling the function must be the contract owner, and they provide a new address which will become the new owner address.

1. **UniswapV3Pool ABI (See Appendix C)**

This is main smart contract within the Uniswap codebase. There are many functions and limited commenting descriptions in this file. Where there are comments, it is helpful, but a lot of the function functionality has to be understood from reading the code itself. Some of the functions are incredibly long and complicated in this file such as the swap function.

Functions:

* checkTicks: Ensures that price ranges are within the tick limits.
* \_blockTimestamp: Returns the timestamp of the block.
* Balance0: Finds the balance of token0 in the pool.
* Balance1: Finds the balance of token1 in the pool.
* snapshotCumulativesInside: A function that queries the data about liquidity and price within the pool.
* observe: This function provides queries about ticks and liquidity at points in the pools history.
* increaseObservationCardinalityNext: Increases the storage capacity for observations in the pool.
* initialize: This function initializes the pools price and observation array. This is called when the pool is created.
* \_modifyPosition: This function monitors the change in liquidity within the pool depending on the ticks.
* \_updatePosition: Updates the liquidity position in the pool.
* Mint: This function mints new liquidity to a pool and checks for correct token amounts.
* Collect: This function allows liquidity providers to collect their rewards for providing the liquidity.
* Burn: This allows liquidity providers to remove their position within the pool and receive it in their wallet.
* Swap: The swap function allows users to swap one token for another.
* Flash: Allows users to loan funds from the pool, where they must return the funds with added fees later.
* setFeeProtocol: Allows the fees in a pool to be changed.
* collectProtocol: Allows the Factory Owner to withdraw protocol fees.

1. **UniswapV3PoolDeployer ABI (See Appendix D)**

This contract is used to deploy new pools. It is very specific to that action, so the code is small, clean and concise, with great comment usage.

Functions:

Deploy: Creates a pool including parameters for factory, two tokens, a fee and a tick spacing.

## CALL GRAPH DISCUSSION

The Uniswap V3 Core contract's call graph analysis unveiled a complex web of interactions. By dissecting this graph, we uncovered the intricate relationships between functions, both within the contract and with external libraries. The call graph exposed the underlying logic that governs the execution of different functions, revealing key features that define the contract's operation. This analysis enhances our understanding of how the smart contract handles transactions and orchestrates its various components.

1. **‘NoDelegateCall.sol’:**

This contract is relatively simple and mainly focused on preventing delegate calls to its methods. The call graph for **‘*NoDelegateCall*.sol’** is straightforward:

A yellow oval with black text

Description automatically generated

Figure 1: NoDelegateCall Call Graph.

* ***NoDelegateCall*** (constructor)
* ***checkNotDelegateCall*** (private method)
* ***noDelegateCall*** (modifier)

In this contract, the primary purpose is to ensure that the contract’s methods cannot be invoked through delegate calls, which is achieved by the ‘***noDelegateCall’*** modifier. It does this by checking that the contract’s address remains the same as the original address. As defined in the constructor.

1. **‘UniswapV3Factory.sol’:**

The ‘***UniswapV3Factory*.sol’** contract is more complex and integral to the Uniswap V3 protocol. The call graph for this contract involves multiple functions, including those inherited from the ‘***UniswapV3PoolDeployer’*** and the modifier from ‘***NoDelegateCall’***. Here are the key functions in the call graph:

A diagram of a diagram

Description automatically generated

Figure 2: UniswapV3Factory Call Graph.

* ***UniswapV3Factory*** (constructor)
* ***createPool*** (external function)
* ***setOwner*** (external function)
* ***enableFeeAmount*** (external function)
* ***deploy*** (function inherited from UniswapV3PoolDeployer)
* ***checkNotDelegateCall*** (modifier inherited from NoDelegateCall)

Additionally, there are some state variables like ‘***owner’***, ‘***feeAmountTickSpacing’***, and ‘***getPool’***, which are essential for the factory’s operation and management of Uniswap V3 pools.

1. **‘UniswapV3Pool.sol’:**

This contract is integral to the Uniswap V3 protocol, responsible for managing liquidity, price observations, and protocol fees for a specific pool. It inherits the ‘***NoDelegateCall’*** modifier, which prevents delegate calls to its methods.

Key Aspects on the Contract:

A diagram of a diagram

Description automatically generated

Figure 3: UniswapV3Pool Call Graph section1.

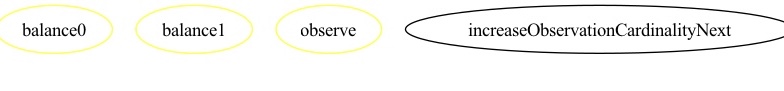


Figure 4: UniswapV3Pool Call Graph section2.

A diagram of different types of objects

Description automatically generated with medium confidence

Figure 5: UniswapV3Pool Call Graph section3.

A diagram of a burn diagram

Description automatically generated

Figure 6: UniswapV3Pool Call Graph section4.

A diagram of a diagram

Description automatically generated

Figure 7: UniswapV3Pool Call Graph section5.

1. Contract Initialization and State:

* The contract initialized its state during deployment by setting the ‘**factory’, ‘token0’, ‘token1’,** and **‘tickSpacing’** based on parameters from the ‘***IUniswapV3PoolDeployer’*** contract.

1. Modifiers:

* The contract utilized two custom modifiers:
  + - ‘**lock’:** Ensures mutual exclusivity and re-entrancy protection for various functions.
    - ‘**onlyFactoryOwner’:** Restricts access to certain functions to the owner of the factory contract.

1. Utility Functions:

* The contract contains several utility functions:
* ‘**\_blockTimestamp’:** Returns the truncated 32-bit block timestamp.
* ‘**balance0’,** and **‘balance1’:** Retrieve the token balances of ‘**token0’,** and **‘token1’.**
* **‘checkTicks’**: Checks if provided tick values form a valid range.

1. View Functions:

* The contract offers view functions that allow external callers to access specific data:
* **‘snapshotCumulativesInside’**: Returns tick cumulative, seconds per liquidity, and seconds inside for a specified tick range.
* **‘observe’**: Provides historical observations for specified timestamps.

1. State Variables:

* The contract maintains various state variables, including ‘**slot0’**, ‘**ticks’**, ‘**tickBitmap’**, ‘**positions’**, ‘**observations’**, ‘**liquidity’**, **feeGrowthGlobal0X128**, ‘**feeGrowthGlobal1X128’**, and ‘**protocolFees’**. These state variables store critical information about the pool's current state.

1. Initialization Function:

* The ‘**initialize’** function sets up the initial state of the pool, including the square root price, tick, and observation parameters. This function can be called only once to initialize the pool.

1. Increasing Observation Cardinality:

* The ‘**increaseObservationCardinalityNext’** function allows increasing the maximum number of observations that can be stored in the pool. This is an administrative function to manage observation data efficiently.

1. Modify Position Params Struct:

* The contract defines a data structure called ‘**ModifyPositionParams’** for specifying owner, tick range, and liquidity changes when modifying positions within the pool.

1. **‘UniswapV3PoolDeployer.sol’:**

This contract is responsible for deploying Uniswap V3 pools with specific parameters. Here is the Call Graph Discussion:

A close-up of a logo

Description automatically generated

Figure : UniswapV3PoolDeployer call graph.

1. Struct Parameters:

* The contract defines a ‘**Parameters’** struct to store the parameters required for deploying a Uniswap V3 pool. These parameters include ‘**factory’**, ‘**token0’**, ‘**token1’**, ‘**fee’**, and ‘**tickSpacing’**.

1. Function Deploy:

* The ‘**deploy’** function is the core function of this contract.
* It takes the following parameters: ‘**factory’**, ‘**token0’**, ‘**token1’**, ‘**fee’**, and ‘**tickSpacing’**.
* It sets the ‘**parameters’** struct to store the provided parameters.
* It deploys a new Uniswap V3 pool contract using the ‘**new UniswapV3Pool{salt: keccak256(abi.encode(token0, token1, fee))}()’** syntax. The ‘**salt’** value ensures that the deployed contract has a unique address.
* After deploying the pool contract, it deletes the ‘**parameters’** to clear the parameter storage.

1. State Variable Parameters:

* The state variable ‘**parameters’** is used to store the pool deployment parameters temporarily during the deployment process.

The call graph for this contract primarily revolves around the ‘**deploy’** function, which involves setting parameters, deploying the Uniswap V3 pool contract, and then clearing the parameters. The interactions are relatively straightforward, focusing on the deployment of new Uniswap V3 pool contracts with specific configurations.

## INHERITANCE GRAPH DISCUSSION

The inheritance hierarchy of the Uniswap V3 Core contract was meticulously explored. Inheritance is a fundamental concept in Solidity, allowing developers to build upon and extend existing code. Our analysis identified multiple facets of the inheritance hierarchy, including the relationships between contracts, code reuse, function and state variable overriding, changes in visibility and access control, and the application of modifiers. By dissecting this hierarchy, we gained deeper insights into the building blocks of the contract and the degree to which it leverages and extends code from other contracts.

## Appendix

Appendix A (NoDelegateCall ABI):

{

  "\_format": "hh-sol-artifact-1",

  "contractName": "NoDelegateCall",

  "sourceName": "contracts/NoDelegateCall.sol",

  "abi": [],

  "bytecode": "0x",

  "deployedBytecode": "0x",

  "linkReferences": {},

  "deployedLinkReferences": {}

}

Appendix B (UniswapV3Factory ABI without bytecode):

{

  "\_format": "hh-sol-artifact-1",

  "contractName": "UniswapV3Factory",

  "sourceName": "contracts/UniswapV3Factory.sol",

  "abi": [

    {

      "inputs": [],

      "stateMutability": "nonpayable",

      "type": "constructor"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": true,

          "internalType": "uint24",

          "name": "fee",

          "type": "uint24"

        },

        {

          "indexed": true,

          "internalType": "int24",

          "name": "tickSpacing",

          "type": "int24"

        }

      ],

      "name": "FeeAmountEnabled",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": true,

          "internalType": "address",

          "name": "oldOwner",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "address",

          "name": "newOwner",

          "type": "address"

        }

      ],

      "name": "OwnerChanged",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": true,

          "internalType": "address",

          "name": "token0",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "address",

          "name": "token1",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "uint24",

          "name": "fee",

          "type": "uint24"

        },

        {

          "indexed": false,

          "internalType": "int24",

          "name": "tickSpacing",

          "type": "int24"

        },

        {

          "indexed": false,

          "internalType": "address",

          "name": "pool",

          "type": "address"

        }

      ],

      "name": "PoolCreated",

      "type": "event"

    },

    {

      "inputs": [

        {

          "internalType": "address",

          "name": "tokenA",

          "type": "address"

        },

        {

          "internalType": "address",

          "name": "tokenB",

          "type": "address"

        },

        {

          "internalType": "uint24",

          "name": "fee",

          "type": "uint24"

        }

      ],

      "name": "createPool",

      "outputs": [

        {

          "internalType": "address",

          "name": "pool",

          "type": "address"

        }

      ],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "uint24",

          "name": "fee",

          "type": "uint24"

        },

        {

          "internalType": "int24",

          "name": "tickSpacing",

          "type": "int24"

        }

      ],

      "name": "enableFeeAmount",

      "outputs": [],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "uint24",

          "name": "",

          "type": "uint24"

        }

      ],

      "name": "feeAmountTickSpacing",

      "outputs": [

        {

          "internalType": "int24",

          "name": "",

          "type": "int24"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "address",

          "name": "",

          "type": "address"

        },

        {

          "internalType": "address",

          "name": "",

          "type": "address"

        },

        {

          "internalType": "uint24",

          "name": "",

          "type": "uint24"

        }

      ],

      "name": "getPool",

      "outputs": [

        {

          "internalType": "address",

          "name": "",

          "type": "address"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "owner",

      "outputs": [

        {

          "internalType": "address",

          "name": "",

          "type": "address"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "parameters",

      "outputs": [

        {

          "internalType": "address",

          "name": "factory",

          "type": "address"

        },

        {

          "internalType": "address",

          "name": "token0",

          "type": "address"

        },

        {

          "internalType": "address",

          "name": "token1",

          "type": "address"

        },

        {

          "internalType": "uint24",

          "name": "fee",

          "type": "uint24"

        },

        {

          "internalType": "int24",

          "name": "tickSpacing",

          "type": "int24"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "address",

          "name": "\_owner",

          "type": "address"

        }

      ],

      "name": "setOwner",

      "outputs": [],

      "stateMutability": "nonpayable",

      "type": "function"

    }

  ],

Appendix C (UniswapV3Pool ABI without bytecode):

{

  "\_format": "hh-sol-artifact-1",

  "contractName": "UniswapV3Pool",

  "sourceName": "contracts/UniswapV3Pool.sol",

  "abi": [

    {

      "inputs": [],

      "stateMutability": "nonpayable",

      "type": "constructor"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": true,

          "internalType": "address",

          "name": "owner",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "int24",

          "name": "tickLower",

          "type": "int24"

        },

        {

          "indexed": true,

          "internalType": "int24",

          "name": "tickUpper",

          "type": "int24"

        },

        {

          "indexed": false,

          "internalType": "uint128",

          "name": "amount",

          "type": "uint128"

        },

        {

          "indexed": false,

          "internalType": "uint256",

          "name": "amount0",

          "type": "uint256"

        },

        {

          "indexed": false,

          "internalType": "uint256",

          "name": "amount1",

          "type": "uint256"

        }

      ],

      "name": "Burn",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": true,

          "internalType": "address",

          "name": "owner",

          "type": "address"

        },

        {

          "indexed": false,

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "int24",

          "name": "tickLower",

          "type": "int24"

        },

        {

          "indexed": true,

          "internalType": "int24",

          "name": "tickUpper",

          "type": "int24"

        },

        {

          "indexed": false,

          "internalType": "uint128",

          "name": "amount0",

          "type": "uint128"

        },

        {

          "indexed": false,

          "internalType": "uint128",

          "name": "amount1",

          "type": "uint128"

        }

      ],

      "name": "Collect",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": true,

          "internalType": "address",

          "name": "sender",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "indexed": false,

          "internalType": "uint128",

          "name": "amount0",

          "type": "uint128"

        },

        {

          "indexed": false,

          "internalType": "uint128",

          "name": "amount1",

          "type": "uint128"

        }

      ],

      "name": "CollectProtocol",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": true,

          "internalType": "address",

          "name": "sender",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "indexed": false,

          "internalType": "uint256",

          "name": "amount0",

          "type": "uint256"

        },

        {

          "indexed": false,

          "internalType": "uint256",

          "name": "amount1",

          "type": "uint256"

        },

        {

          "indexed": false,

          "internalType": "uint256",

          "name": "paid0",

          "type": "uint256"

        },

        {

          "indexed": false,

          "internalType": "uint256",

          "name": "paid1",

          "type": "uint256"

        }

      ],

      "name": "Flash",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": false,

          "internalType": "uint16",

          "name": "observationCardinalityNextOld",

          "type": "uint16"

        },

        {

          "indexed": false,

          "internalType": "uint16",

          "name": "observationCardinalityNextNew",

          "type": "uint16"

        }

      ],

      "name": "IncreaseObservationCardinalityNext",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": false,

          "internalType": "uint160",

          "name": "sqrtPriceX96",

          "type": "uint160"

        },

        {

          "indexed": false,

          "internalType": "int24",

          "name": "tick",

          "type": "int24"

        }

      ],

      "name": "Initialize",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": false,

          "internalType": "address",

          "name": "sender",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "address",

          "name": "owner",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "int24",

          "name": "tickLower",

          "type": "int24"

        },

        {

          "indexed": true,

          "internalType": "int24",

          "name": "tickUpper",

          "type": "int24"

        },

        {

          "indexed": false,

          "internalType": "uint128",

          "name": "amount",

          "type": "uint128"

        },

        {

          "indexed": false,

          "internalType": "uint256",

          "name": "amount0",

          "type": "uint256"

        },

        {

          "indexed": false,

          "internalType": "uint256",

          "name": "amount1",

          "type": "uint256"

        }

      ],

      "name": "Mint",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": false,

          "internalType": "uint8",

          "name": "feeProtocol0Old",

          "type": "uint8"

        },

        {

          "indexed": false,

          "internalType": "uint8",

          "name": "feeProtocol1Old",

          "type": "uint8"

        },

        {

          "indexed": false,

          "internalType": "uint8",

          "name": "feeProtocol0New",

          "type": "uint8"

        },

        {

          "indexed": false,

          "internalType": "uint8",

          "name": "feeProtocol1New",

          "type": "uint8"

        }

      ],

      "name": "SetFeeProtocol",

      "type": "event"

    },

    {

      "anonymous": false,

      "inputs": [

        {

          "indexed": true,

          "internalType": "address",

          "name": "sender",

          "type": "address"

        },

        {

          "indexed": true,

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "indexed": false,

          "internalType": "int256",

          "name": "amount0",

          "type": "int256"

        },

        {

          "indexed": false,

          "internalType": "int256",

          "name": "amount1",

          "type": "int256"

        },

        {

          "indexed": false,

          "internalType": "uint160",

          "name": "sqrtPriceX96",

          "type": "uint160"

        },

        {

          "indexed": false,

          "internalType": "uint128",

          "name": "liquidity",

          "type": "uint128"

        },

        {

          "indexed": false,

          "internalType": "int24",

          "name": "tick",

          "type": "int24"

        }

      ],

      "name": "Swap",

      "type": "event"

    },

    {

      "inputs": [

        {

          "internalType": "int24",

          "name": "tickLower",

          "type": "int24"

        },

        {

          "internalType": "int24",

          "name": "tickUpper",

          "type": "int24"

        },

        {

          "internalType": "uint128",

          "name": "amount",

          "type": "uint128"

        }

      ],

      "name": "burn",

      "outputs": [

        {

          "internalType": "uint256",

          "name": "amount0",

          "type": "uint256"

        },

        {

          "internalType": "uint256",

          "name": "amount1",

          "type": "uint256"

        }

      ],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "internalType": "int24",

          "name": "tickLower",

          "type": "int24"

        },

        {

          "internalType": "int24",

          "name": "tickUpper",

          "type": "int24"

        },

        {

          "internalType": "uint128",

          "name": "amount0Requested",

          "type": "uint128"

        },

        {

          "internalType": "uint128",

          "name": "amount1Requested",

          "type": "uint128"

        }

      ],

      "name": "collect",

      "outputs": [

        {

          "internalType": "uint128",

          "name": "amount0",

          "type": "uint128"

        },

        {

          "internalType": "uint128",

          "name": "amount1",

          "type": "uint128"

        }

      ],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "internalType": "uint128",

          "name": "amount0Requested",

          "type": "uint128"

        },

        {

          "internalType": "uint128",

          "name": "amount1Requested",

          "type": "uint128"

        }

      ],

      "name": "collectProtocol",

      "outputs": [

        {

          "internalType": "uint128",

          "name": "amount0",

          "type": "uint128"

        },

        {

          "internalType": "uint128",

          "name": "amount1",

          "type": "uint128"

        }

      ],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "factory",

      "outputs": [

        {

          "internalType": "address",

          "name": "",

          "type": "address"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "fee",

      "outputs": [

        {

          "internalType": "uint24",

          "name": "",

          "type": "uint24"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "feeGrowthGlobal0X128",

      "outputs": [

        {

          "internalType": "uint256",

          "name": "",

          "type": "uint256"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "feeGrowthGlobal1X128",

      "outputs": [

        {

          "internalType": "uint256",

          "name": "",

          "type": "uint256"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "internalType": "uint256",

          "name": "amount0",

          "type": "uint256"

        },

        {

          "internalType": "uint256",

          "name": "amount1",

          "type": "uint256"

        },

        {

          "internalType": "bytes",

          "name": "data",

          "type": "bytes"

        }

      ],

      "name": "flash",

      "outputs": [],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "uint16",

          "name": "observationCardinalityNext",

          "type": "uint16"

        }

      ],

      "name": "increaseObservationCardinalityNext",

      "outputs": [],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "uint160",

          "name": "sqrtPriceX96",

          "type": "uint160"

        }

      ],

      "name": "initialize",

      "outputs": [],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "liquidity",

      "outputs": [

        {

          "internalType": "uint128",

          "name": "",

          "type": "uint128"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "maxLiquidityPerTick",

      "outputs": [

        {

          "internalType": "uint128",

          "name": "",

          "type": "uint128"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "internalType": "int24",

          "name": "tickLower",

          "type": "int24"

        },

        {

          "internalType": "int24",

          "name": "tickUpper",

          "type": "int24"

        },

        {

          "internalType": "uint128",

          "name": "amount",

          "type": "uint128"

        },

        {

          "internalType": "bytes",

          "name": "data",

          "type": "bytes"

        }

      ],

      "name": "mint",

      "outputs": [

        {

          "internalType": "uint256",

          "name": "amount0",

          "type": "uint256"

        },

        {

          "internalType": "uint256",

          "name": "amount1",

          "type": "uint256"

        }

      ],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "uint256",

          "name": "",

          "type": "uint256"

        }

      ],

      "name": "observations",

      "outputs": [

        {

          "internalType": "uint32",

          "name": "blockTimestamp",

          "type": "uint32"

        },

        {

          "internalType": "int56",

          "name": "tickCumulative",

          "type": "int56"

        },

        {

          "internalType": "uint160",

          "name": "secondsPerLiquidityCumulativeX128",

          "type": "uint160"

        },

        {

          "internalType": "bool",

          "name": "initialized",

          "type": "bool"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "uint32[]",

          "name": "secondsAgos",

          "type": "uint32[]"

        }

      ],

      "name": "observe",

      "outputs": [

        {

          "internalType": "int56[]",

          "name": "tickCumulatives",

          "type": "int56[]"

        },

        {

          "internalType": "uint160[]",

          "name": "secondsPerLiquidityCumulativeX128s",

          "type": "uint160[]"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "bytes32",

          "name": "",

          "type": "bytes32"

        }

      ],

      "name": "positions",

      "outputs": [

        {

          "internalType": "uint128",

          "name": "liquidity",

          "type": "uint128"

        },

        {

          "internalType": "uint256",

          "name": "feeGrowthInside0LastX128",

          "type": "uint256"

        },

        {

          "internalType": "uint256",

          "name": "feeGrowthInside1LastX128",

          "type": "uint256"

        },

        {

          "internalType": "uint128",

          "name": "tokensOwed0",

          "type": "uint128"

        },

        {

          "internalType": "uint128",

          "name": "tokensOwed1",

          "type": "uint128"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "protocolFees",

      "outputs": [

        {

          "internalType": "uint128",

          "name": "token0",

          "type": "uint128"

        },

        {

          "internalType": "uint128",

          "name": "token1",

          "type": "uint128"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "uint8",

          "name": "feeProtocol0",

          "type": "uint8"

        },

        {

          "internalType": "uint8",

          "name": "feeProtocol1",

          "type": "uint8"

        }

      ],

      "name": "setFeeProtocol",

      "outputs": [],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "slot0",

      "outputs": [

        {

          "internalType": "uint160",

          "name": "sqrtPriceX96",

          "type": "uint160"

        },

        {

          "internalType": "int24",

          "name": "tick",

          "type": "int24"

        },

        {

          "internalType": "uint16",

          "name": "observationIndex",

          "type": "uint16"

        },

        {

          "internalType": "uint16",

          "name": "observationCardinality",

          "type": "uint16"

        },

        {

          "internalType": "uint16",

          "name": "observationCardinalityNext",

          "type": "uint16"

        },

        {

          "internalType": "uint8",

          "name": "feeProtocol",

          "type": "uint8"

        },

        {

          "internalType": "bool",

          "name": "unlocked",

          "type": "bool"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "int24",

          "name": "tickLower",

          "type": "int24"

        },

        {

          "internalType": "int24",

          "name": "tickUpper",

          "type": "int24"

        }

      ],

      "name": "snapshotCumulativesInside",

      "outputs": [

        {

          "internalType": "int56",

          "name": "tickCumulativeInside",

          "type": "int56"

        },

        {

          "internalType": "uint160",

          "name": "secondsPerLiquidityInsideX128",

          "type": "uint160"

        },

        {

          "internalType": "uint32",

          "name": "secondsInside",

          "type": "uint32"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "address",

          "name": "recipient",

          "type": "address"

        },

        {

          "internalType": "bool",

          "name": "zeroForOne",

          "type": "bool"

        },

        {

          "internalType": "int256",

          "name": "amountSpecified",

          "type": "int256"

        },

        {

          "internalType": "uint160",

          "name": "sqrtPriceLimitX96",

          "type": "uint160"

        },

        {

          "internalType": "bytes",

          "name": "data",

          "type": "bytes"

        }

      ],

      "name": "swap",

      "outputs": [

        {

          "internalType": "int256",

          "name": "amount0",

          "type": "int256"

        },

        {

          "internalType": "int256",

          "name": "amount1",

          "type": "int256"

        }

      ],

      "stateMutability": "nonpayable",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "int16",

          "name": "",

          "type": "int16"

        }

      ],

      "name": "tickBitmap",

      "outputs": [

        {

          "internalType": "uint256",

          "name": "",

          "type": "uint256"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "tickSpacing",

      "outputs": [

        {

          "internalType": "int24",

          "name": "",

          "type": "int24"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [

        {

          "internalType": "int24",

          "name": "",

          "type": "int24"

        }

      ],

      "name": "ticks",

      "outputs": [

        {

          "internalType": "uint128",

          "name": "liquidityGross",

          "type": "uint128"

        },

        {

          "internalType": "int128",

          "name": "liquidityNet",

          "type": "int128"

        },

        {

          "internalType": "uint256",

          "name": "feeGrowthOutside0X128",

          "type": "uint256"

        },

        {

          "internalType": "uint256",

          "name": "feeGrowthOutside1X128",

          "type": "uint256"

        },

        {

          "internalType": "int56",

          "name": "tickCumulativeOutside",

          "type": "int56"

        },

        {

          "internalType": "uint160",

          "name": "secondsPerLiquidityOutsideX128",

          "type": "uint160"

        },

        {

          "internalType": "uint32",

          "name": "secondsOutside",

          "type": "uint32"

        },

        {

          "internalType": "bool",

          "name": "initialized",

          "type": "bool"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "token0",

      "outputs": [

        {

          "internalType": "address",

          "name": "",

          "type": "address"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    },

    {

      "inputs": [],

      "name": "token1",

      "outputs": [

        {

          "internalType": "address",

          "name": "",

          "type": "address"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    }

  ],

Appendix D (UniswapV3PoolDeployer ABI without bytecode):

{

  "\_format": "hh-sol-artifact-1",

  "contractName": "UniswapV3PoolDeployer",

  "sourceName": "contracts/UniswapV3PoolDeployer.sol",

  "abi": [

    {

      "inputs": [],

      "name": "parameters",

      "outputs": [

        {

          "internalType": "address",

          "name": "factory",

          "type": "address"

        },

        {

          "internalType": "address",

          "name": "token0",

          "type": "address"

        },

        {

          "internalType": "address",

          "name": "token1",

          "type": "address"

        },

        {

          "internalType": "uint24",

          "name": "fee",

          "type": "uint24"

        },

        {

          "internalType": "int24",

          "name": "tickSpacing",

          "type": "int24"

        }

      ],

      "stateMutability": "view",

      "type": "function"

    }

  ],

}