88MPH

SMART CONTRACT SECURITY ANALYSIS

Date of audit: 16.12.2020

Smart Contract Ownership	Team Reward	Total Supply	Minting Function	Migration Function	Funds Lock Period	Contract Pause	Suspicious Functions
Specific for each contract (check details below)	10% of the minted amount	Variable	Available	Available	None	Not possible	Not found

External Smart Contract Audit:

- The smart contracts were audited by Quantstamp

Ownership structure:

Smart contract	Owner	Description
MPH Token	MPHMinter	The following functions can be called by the owner: • **ownerMint(address account, uint256 amount)** • **transferOwnership(address newOwner)** • **renounceOwnership()** After the contract deploy, 229,842 MPH tokens were minted into the MerkleDistributor contract. The mint function is available. The burn function can be invoked by token holders.
MPHMinter	Timelock / GnosisSafe [1]	The contract holds 12.3% of MPH Token at the review time. The following functions can be called by the owner: • **renounceOwnership()** • **transferOwnership(address)** • **setPoolWhitelist(address, bool)** allows EOA owners to add any contract to the white list • **setGovTreasury(address)** is applied for receiving tokens minted as governance rewards • **setDevWallet(address)** is applied for receiving tokens minted as team rewards. The rewards rate is defined by the MPHIssuanceModel01 contract • **setMPHTokenOwner(address)** transfers ownership of the MPH Token contract to another contract • **setMPHTokenOwnerToZero()** makes MPH Token fully decentralized and totally blocks the ability to mint. This could break the staking part of the project, because it makes minting of the rewards impossible

		• **setIssuanceModel(address)** sets an address that will calculate the token amount that will be minted by MPHMinter. • **setVesting(address)**. The current address is set to the Vesting contract The following functions can be called by contracts from the onlyWhitelistedPool list: • **mintDepositorReward** • **takeBackDepositorReward** • **mintFunderReward**
Vesting	decentralized	The contract holds 2.89% of MPH Token and is used for creating vests and withdrawing them. The vest is a little token lock "pool" that unlocks a little portion of tokens to withdraw them each second. User rewards from the MPH Minter contract move here The contract allows to lock the MPH Token and select the period when holders could fully withdraw the token from the contract. The vest period is calculated by MPHIssuanceModel01 in the MPH Minter contract that creates these "vests" when users unstake tokens.
ClonedRewards	GnosisSafe [2]	The contract holds 4.6% of MPH Token at the review time. The owners could install a **rewardDistribution** address that could call the **notifyRewardAmount** function used for the reward system. The current address is MPH Minter. The following functions can be called by the owner: • **renounceOwnership()** • **transferOwnership(address)** • **setRewardDistribution(address)**
Rewards	Timelock / GnosisSafe [1]	The contract holds 7.13% of MPH Token at the review time. Functions that can be called by the owner are the same as in the Clone Reward contract.
MerkleDistributor	decentralized	The contract received 229 842 at the presale stage and holds 0.7% of MPH Token at review time. It was used for the initial token distribution.
MPHIssuanceModel01	GnosisSafe [1]	The following functions can be called by the owner: • **setDevRewardMultiplier** installs multiplier for the team rewards • **setPoolFunderRewardMultiplier** • **setPoolDepositorRewardTakeBackMultiplier** • **setPoolFunderRewardVestPeriod** • **setPoolDepositorRewardVestPeriod** • **setPoolDepositorRewardMintMultiplier**
Timelock	GnosisSafe [1]	The contract has a 48h delay and acts like a regular EOA address.

Total supply:
- Is variable as long as:
  - a) new tokens are minted when users gain rewards
  - b) the users can burn the tokens

Minting function:
- Available

Migration function:
- Available. Proxy patterns allow making migration

Team reward %:
- Additional 10% of the minted amount is minted and sent to the developer fund
- The risk of a quick token dump initiated by the team can be estimated as 2/10

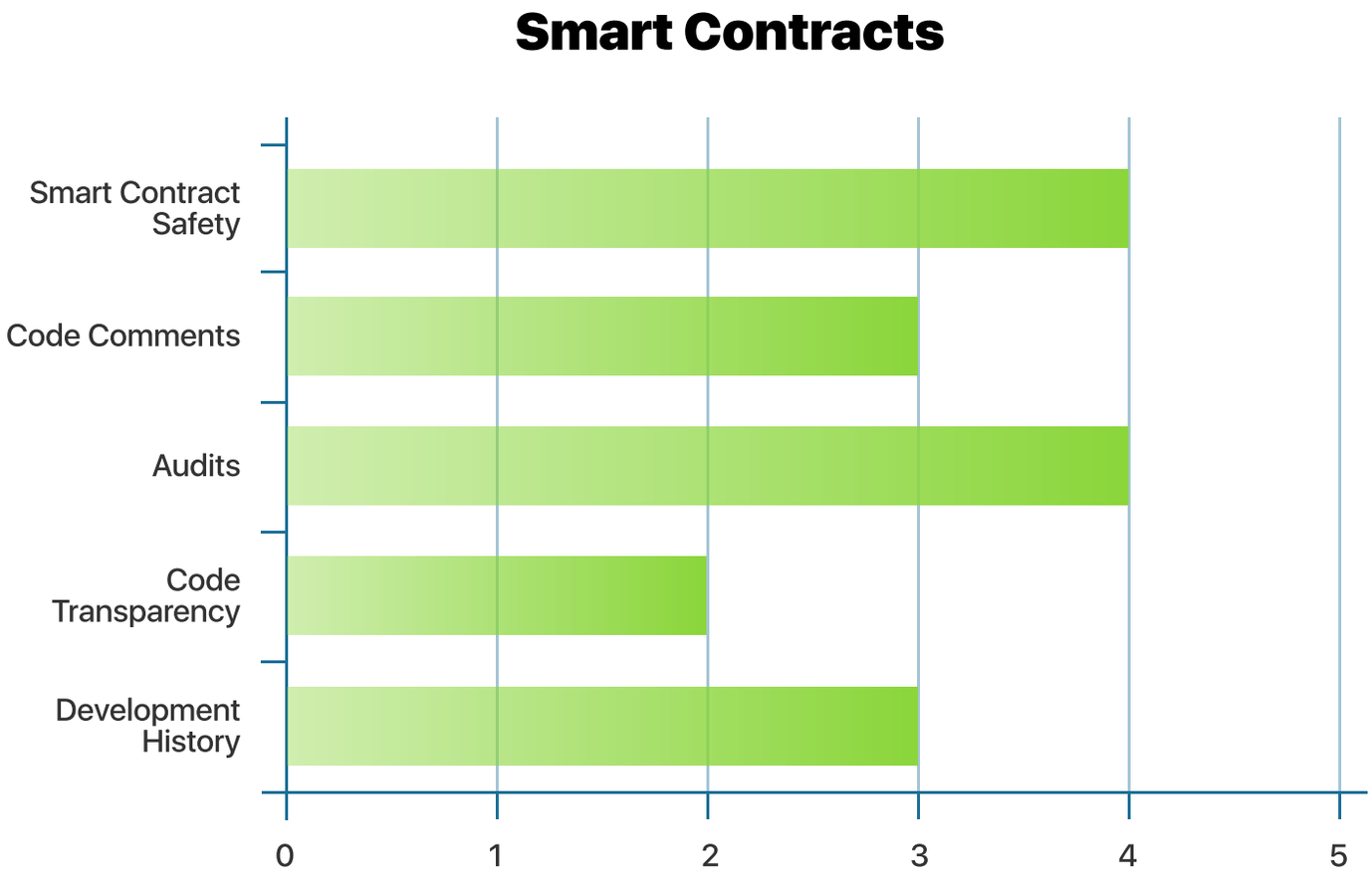
Funds lock period:
- None

Lock period for rewards withdrawal:
- Unlocking a little portion of tokens to withdraw them each second
- The lock period is implemented in the Vesting contract

Possibility to pause the Smart Contracts:
- Not available

List of suspicious functions:
- Not found

Risk Level LOW


Smart Contracts
Smart Contract Safety
Code Comments
Audits
Code Transparency
Development History
0
1
2
3
4
5

Conclusion

88mph is a DeFi lending protocol, which provides an opportunity to earn fixed interests and participate in liquidity mining.

The MPH token contract is owned by the MPH minter contract that allows calling a mint function after implementation of the 48h timelock contract. In turn, the timelock contract is owned by the Gnosis Safe wallet with 2 EOA owners. This fact doesn't make the project fully decentralized as it isn't managed by the community in this case. However, any implementations or changes in the code of the smart contracts could be tracked and users will be warned about them.

It's important to point out features of the MPHIssuanceModel01 contract. This contract is used for calculating and setting team and depositor rewards. Moreover, it allows setting a period during which the rewards will be gradually issued every second. Therefore, there is a lock period for the rewards withdrawal.

The total supply is variable as long as new tokens are minted when users gain rewards. There is no fund lock period defined in the smart contracts, meaning users can manage their funds immediately after the staking. Moreover, there is no possibility to pause the smart contracts: users have constant access to the functionality of the smart contracts.

The risk of a quick token dump, initiated by the team, can be estimated as low, because the EOA owners don't have a large share of the token distribution and can call the mint function only through the 48h timelock. But I would recommend users to monitor the timelock with a Telegram bot like @tracktxbot.

No suspicious functions were revealed during the auditing.

The risk level of the 88mph project can be estimated as low.