GasFarm

Lightpaper

Get transaction on DeFi platforms, earn cashback ETH gas fees and farming rewards.

GasFarm Foundation

hello@gasfarm.org

Version 1.6.0 (December 2020)

ABSTRACT

GasFarm is a rewarding platform that pays back part of the Ethereum gas fees spent in a decentralized exchange/swap. In other words, it is an Ethereum gas token collector that will minimize high transaction fee loss. Users get cashback some of their ETH gas fees by using the advantages of GasFarm. GasFarm aims to simplify the process and help maximize returns and savings.

GasFarm realizes this reward system based on Proof of Stake (PoS) technology. The Proof of Stake technology allows to make network stronger and safer and get reward in return. Every staking pool offers its own daily/weekly/monthly income and payout frequency conditions.

It is the most practical way to experience traditional investment techniques on DeFi instruments.

CONTENT

1. BLOCKCHAIN AND ETHEREUM

A blockchain is best described as a public database that is updated and shared across many computers in a network.

"Block" refers to the fact that data and state is stored in sequential batches or "blocks". If you send ETH to someone else, the transaction data needs to be added to a block for it to be successful.

"Chain" refers to the fact that each block cryptographically references its parent. A block's data cannot be changed without changing all subsequent blocks, which would require the consensus of the entire network.

Each new block and the chain as a whole must be agreed upon by every node in the network. This is so everyone has the same data. For this to work, blockchains need a consensus mechanism.

Ethereum currently uses a proof-of-work consensus mechanism. This means that anyone who wants to add new blocks to the chain must solve a difficult puzzle that you need a lot of computing power to work on. Solving the puzzle "proves" that you have spent the computational resources. Doing this is known as mining. Mining can be trial and error but adding a block successfully is rewarded in ETH. On the other hand, submitting fraudulent blocks is not an attractive option considering the resources you've spent on producing the block.

New blocks are broadcast to the nodes in the network, checked and verified, updating the state for everyone.

So to summarise, when you send ETH to someone, the transaction must be mined and included in a new block. The updated state is then shared with the entire network. More on the details below.

1.1 WHAT IS ETHEREUM?

In the Ethereum universe, there is a single, canonical computer (called the Ethereum Virtual Machine, or EVM) whose state everyone on the Ethereum network agrees on. Everyone who participates in the Ethereum network (every Ethereum node) keeps a copy of the state of this computer. Additionally, any participant can broadcast a request for this computer to perform arbitrary computation. Whenever such a request is broadcast, other participants on the network verify, validate, and carry out ("execute") the computation. This causes a state change in the EVM, which is committed and propagated throughout the entire network.

Requests for computation are called transaction requests; the record of all transactions as well as the EVM's present state is stored in the blockchain, which in turn is stored and agreed upon by all nodes.

Cryptographic mechanisms ensure that once transactions are verified as valid and added to the blockchain, they can't be tampered with later; the same mechanisms also ensure that all transactions are signed and executed with appropriate "permissions" (no one should be able to send digital assets from Alice's account, except for Alice herself).

1.2 ETHEREUM VIRTUAL MACHINE (EVM)

The EVM's physical instantiation can't be described in the same way that one might point to a cloud or an ocean wave, but it does exist as one single entity maintained by thousands of connected computers running an Ethereum client.

The Ethereum protocol itself exists solely for the purpose of keeping the continuous, uninterrupted, and immutable operation of this special state machine; It's the environment in which all Ethereum accounts and smart contracts live. At any given block in the chain, Ethereum has one and only one 'canonical' state, and the EVM is what defines the rules for computing a new valid state from block to block.

1.2.1 FROM LEDGER TO STATE MACHINE

The analogy of a 'distributed ledger' is often used to describe blockchains like Bitcoin, which enable a decentralized currency using fundamental tools of cryptography.

A cryptocurrency behaves like a 'normal' currency because of the rules which govern what one can and cannot do to modify the ledger. For example, a Bitcoin address cannot spend more Bitcoin than it has previously received. These rules underpin all transactions on Bitcoin and many other blockchains.

While Ethereum has its own native cryptocurrency (Ether) that follows almost exactly the same intuitive rules, it also enables a much more powerful function: smart contracts. For this more complex feature, a more sophisticated analogy is required. Instead of a distributed ledger, Ethereum is a distributed state machine. Ethereum's state is a large data structure which holds not only all accounts and balances, but a machine state, which can change from block to block according to a pre-defined set of rules, and which can execute arbitrary machine code. The specific rules of changing state from block to block are defined by the EVM.
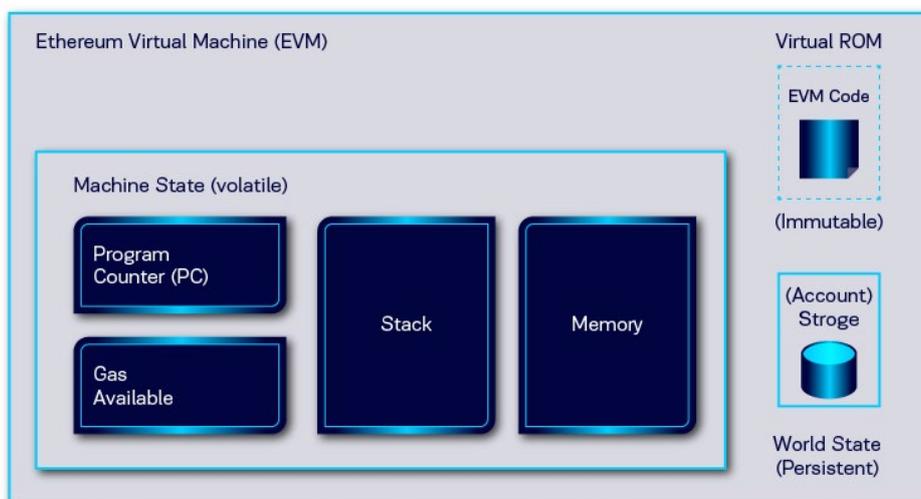

Diagram adapted from Ethereum EVM illustrated

1.2.2 THE ETHEREUM STATE TRANSITION FUNCTION

The EVM behaves as a mathematical function would: Given an input, it produces a deterministic output. It therefore is quite helpful to more formally describe Ethereum as having a state transition function:

$$- Y(S, T) = S' -$$

Given an old valid state (S) and a new set of valid transactions (T), the Ethereum state transition function Y(S, T) produces a new valid output state S'

1.2.3 EVM INSTRUCTIONS

The EVM executes as a stack machine with a depth of 1024 items. Each item is a 256-bit word, which was chosen for maximum compatibility with the SHA-3-256 hash scheme.

During execution, the EVM maintains a transient memory (as a word-addressed byte array), which does not persist between transactions.

Contracts, however, do contain a Merkle Patricia storage trie (as a word-addressable word array), associated with the account in question and part of the global state.

Compiled smart contract bytecode executes as a number of EVM opcodes, which perform standard stack operations like XOR, AND, ADD, SUB, etc. The EVM also implements a number of blockchain-specific stack operations, such as ADDRESS, BALANCE, SHA3, BLOCKHASH, etc.
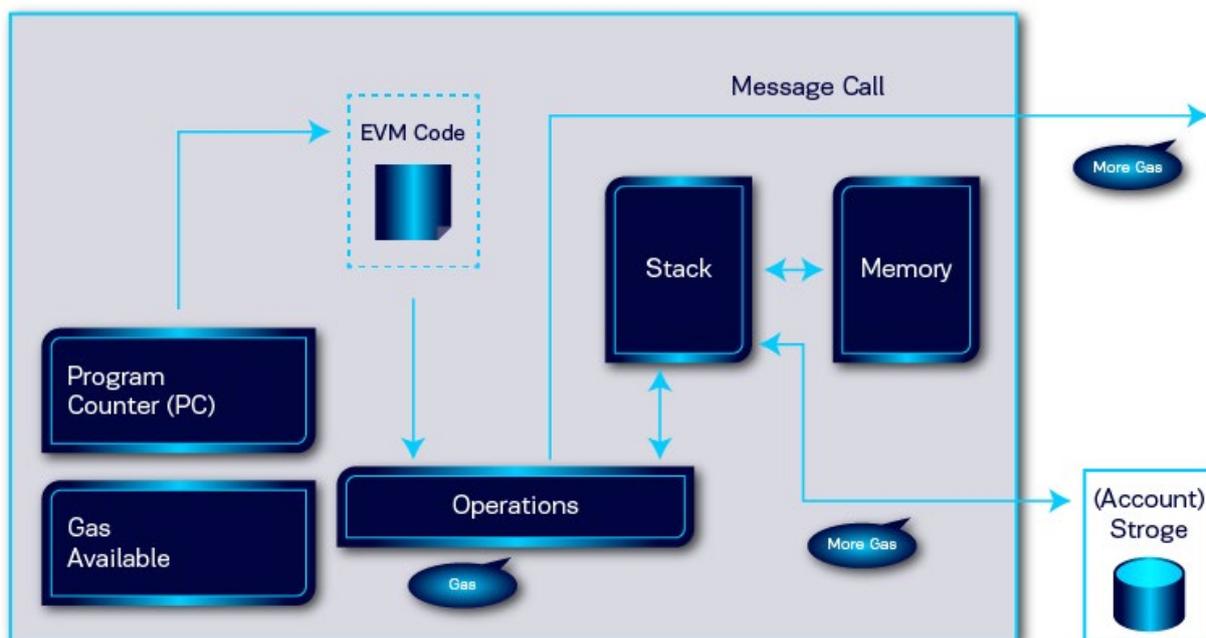
Diagrams adapted from Ethereum EVM illustrated

1.3 WHAT IS ETHER?

The purpose of Ether, the cryptocurrency, is to allow for the existence of a market for computation. Such a market provides an economic incentive for participants to verify/execute transaction requests and to provide computational resources to the network.

Any participant who broadcasts a transaction request must also offer some amount of ether to the network, as a bounty to be awarded to whoever eventually does the work of verifying the transaction, executing it, committing it to the blockchain, and broadcasting it to the network.

The amount of ether paid is a function of the length of the computation. This also prevents malicious participants from intentionally clogging the network by requesting execution of infinite loops or resource-intense scripts, as these actors will be continually charged.

1.3.1 GAS AND FEES

Gas is essential to the Ethereum network. It is the fuel that allows it to operate, in the same way that a car needs gasoline to run.

1.3.2 WHAT'S A TRANSACTION

An Ethereum transaction refers to an action initiated by an externally-owned account, in other words an account managed by a human, not a contract. For example, if Bob sends Alice 1 ETH, Bob's account must be debited and Alice's must be credited. This state-changing action takes place within a transaction.
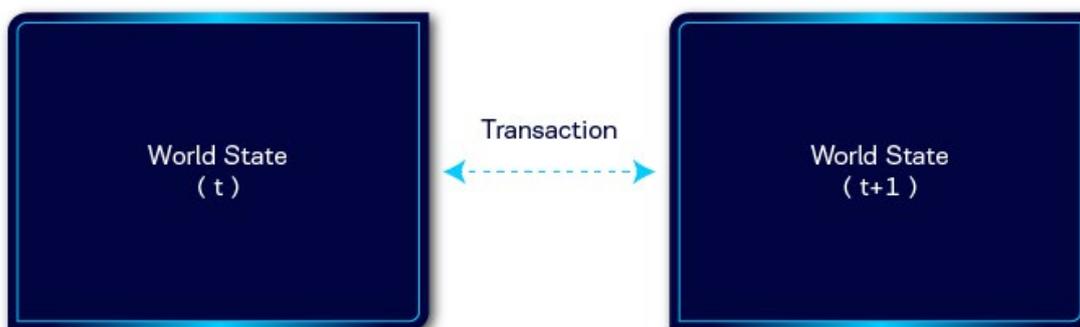
Diagrams adapted from Ethereum EVM illustrated

Transactions, which change the state of the EVM, need to be broadcast to the whole network. Any node can broadcast a request for a transaction to be executed on the EVM; after this happens, a miner will execute the transaction and propagate the resulting state change to the rest of the network.

Transactions require a fee and must be mined to become valid. To make this overview simpler we'll cover gas fees and mining elsewhere.

A submitted transaction includes the following information:

- recipient – the receiving address (if an externally-owned account, the transaction will transfer value. If a contract account, the transaction will execute the contract code)

- signature – the identifier of the sender. This is generated when the sender's private key signs the transaction and confirms the sender has authorised this transaction

- value – amount of ETH to transfer from sender to recipient (in WEI, a denomination of ETH)

- data – optional field to include arbitrary data

- gasLimit – the maximum amount of gas units that can be consumed by the transaction. Units of gas represent computational steps

- gasPrice – the fee the sender pays per unit of gas

Gas is a reference to the computation required to process the transaction by a miner. Users have to pay a fee for this computation. The gasLimit and gasPrice determine the maximum transaction fee paid to the miner. More on Gas.

The transaction object will look a little like this:

```
1     {
2        from: "0xEA663fbDe714fd799de3EdF0F56AA9716B898ec8",
3        to: "0xAc07ba73b6a9ee108530ff4df5077c2b3d481e5a",
4        gasLimit: "25000",
5        gasPrice: "540",
6        nonce: "0",
7        value: "10000000000",
8     }
```

Diagrams adapted from Ethereum EVM illustrated

But a transaction object needs to be signed using the sender's private key. This proves that the transaction could only have come from the sender and was not sent fraudulently.

1.3.3 WHAT IS GAS?

Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network.

Since each Ethereum transaction requires computational resources to execute, each transaction requires a fee. Gas refers to the fee required to successfully conduct a transaction on Ethereum.
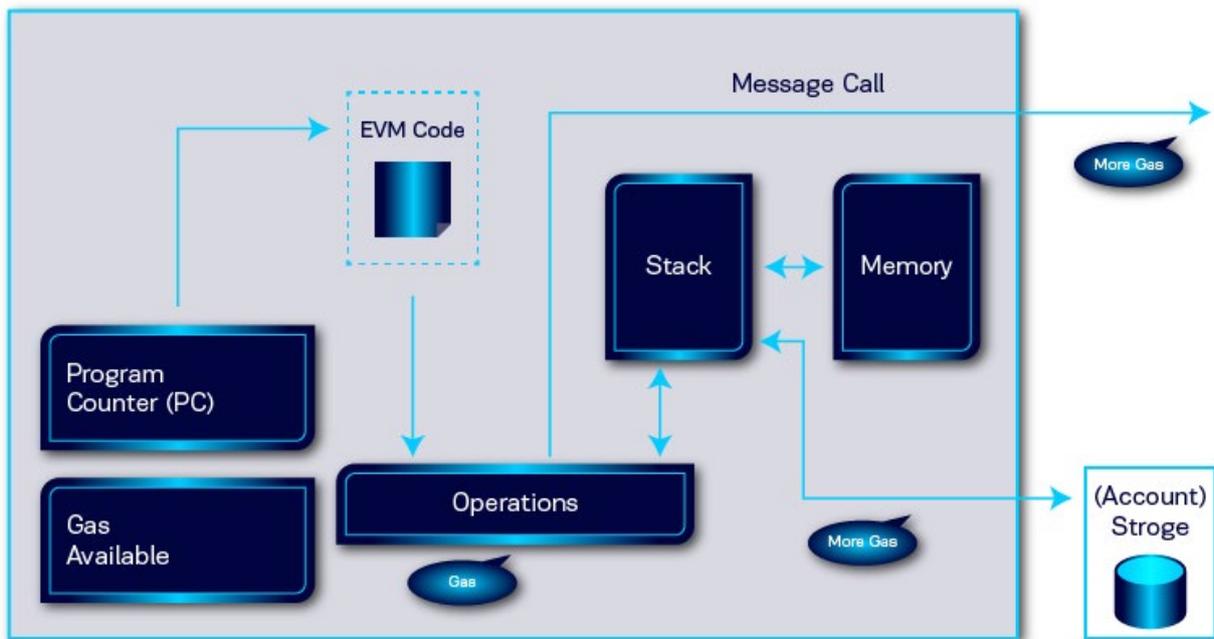

Diagram adapted from Ethereum EVM illustrated

In essence, gas fees are paid in Ethereum's native currency, ether (ETH). Gas prices are denoted in Gwei, which itself is a denomination of ETH - each Gwei is equal to 0.000000001 ETH (10-9 ETH). For example, instead of saying that your gas costs 0.000000001 Ether, you can say your gas costs 1 Gwei.

1.3.4 WHY DO GAS FEES EXIST?

In short, gas fees help keep the Ethereum network secure. By requiring a fee for every computation executed on the network, we prevent actors from spamming the network. In order to prevent accidental or hostile infinite loops or other computational wastage in code, each transaction is required to set a limit to how many computational steps of code execution it can use. The fundamental unit of computation is "gas".

Although a transaction includes a limit, any gas not used in a transaction is returned to the user.
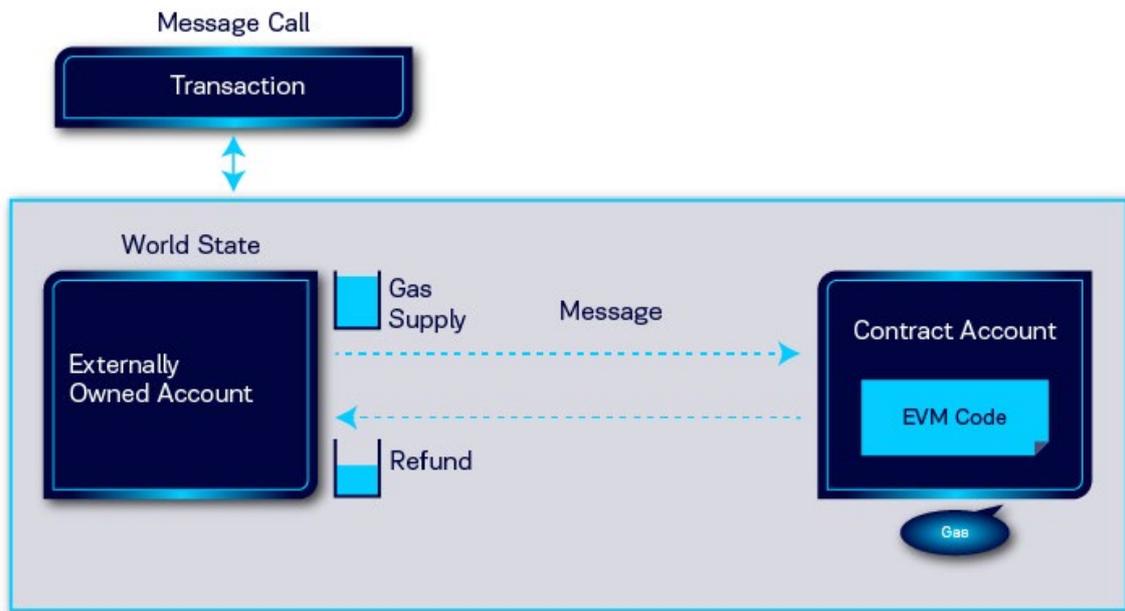

Diagram adapted from Ethereum EVM illustrated

1.4 WHAT ARE DAPPS?

In practice, participants don't write new code every time they want to request a computation on the EVM. Rather, application developers upload programs (reusable snippets of code) into EVM storage, and then users make requests for the execution of these code snippets with varying parameters. We call the programs uploaded to and executed by the network smart contracts.

At a very basic level, you can think of a smart contract like a sort of vending machine: a script which, when called with certain parameters, performs some actions or computation if certain conditions are satisfied. For example, a simple vendor smart contract could create and assign ownership of a digital asset if the caller sends ether to a specific recipient.

Any developer can create a smart contract and make it public to the network, using the blockchain as its data layer, for a fee paid to the network. Any user can then call the smart contract to execute its code, again for a fee paid to the network.

Thus, with smart contracts, developers can build and deploy arbitrarily complex user-facing apps and services: marketplaces, financial instruments, games, etc.
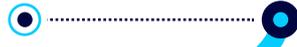
2. ROADMAP

GFT is planned to be unlocked and trade-able in April 2021. GasFarm is planning to launch cashback rewards and staking in May 2021. GasFarm App is scheduled to launch in May 2021.

2020 - Q3
GasFarm Concept,
Market Research

2020 - Q4
GasFarm Fundraising /
Team Building

2021 - Q1
GasFarm Lightpaper,
Business Development

2021 - Q2
Token Generation Event: GFT,
GasFarm Whitepaper,
Test SDK/APP Launch

2021 - Q3
Proof of Concept,
Product Development,
Partner Integration

2021 - Q4
GFT Market Development,
More Cex Listings

2022 - Q1
Cross-chain Launch,
Support for Multiple Assets

3 PLATFORM MECHANICS

3.1 EARN ETH GAS FEES

Get back the ETH gas fees you spent on the transfer.

GasFarm is platform to offer cashback rewards on spending.

Ethereum gas fees. The more one holds on to the GFT token, the more he is rewarded.

Cashback rewards are calculated on various percentages and parameters.

Rewards are distributed based on these percentages.

TRANSACTION FEES & CASHBACK RATES

	1001-5000 GFT	5001-10.000 GFT	10.001-50.000 GFT
3 DAY	UP TO 0,5%	UP TO 1,2%	UP TO 7%
7 DAY	UP TO 2%	UP TO 4,5%	UP TO 25%
15 DAY	UP TO 5%	UP TO 10%	UP TO 60%
1 MONTH	UP TO 13%	UP TO 23,5%	UP TO 100%

3.2 YIELD FARMING

Yield farming lets you lock up funds, providing rewards in the process.

It involves lending out cryptos via DeFi protocols in order to earn fixed or variable interest.

Earn cash rewards at the GFT token rate you locked.

GasFarm realizes this reward system based on Proof of Stake (PoS) technology. The Proof of Stake technology allows to make network stronger and safer and get reward in return. Every staking pool offers its own daily/weekly/monthly income and payout frequency conditions.

3.3 REFERRAL SYSTEM

Referral System is a program where you can earn passive income by inviting your friends. With just one click you can copy your unique referral link from the dashboard and share it on various digital platforms such as email, messenger, web browsers and more. You earn 5% passive income from the rewards of your friends using your referral link at GasFarm. Without forwarding and time limit, you can share your reference link with as many friends as you want.

3.4 FULL INTEGRATION TO DEFI PLATFORMS

Decentralized finance—often called DeFi—refers to the shift from traditional, centralized financial systems to peer-to-peer finance enabled by decentralized technologies built on the Ethereum blockchain. GasFarm works these Defi programs fully integrated.

Uniswap, Sushiswap, 1inch, Moonswap, Bancor etc. easier cashback your transaction fees on all ETH based decentralized exchanges.

3.5 WALLET VARIATION

It can be connected with wallets like MetaMask, Ledger, Portis, MEW, Authereum, Fortmatic, etc. You can easily connect to GasFarm App with Google Chrome, Mozilla Firefox etc,

METAMASK

Ledger

portis.io

MyEtherWallet

Authereum

Fortmatic

4. HOW IT WORKS?

4.1 LAUNCH APPLICATION

GasFarm App will work on mobile and web. You can manage, stake your gas token and avail gas cashback with extra rewards.

4.2 CONNECT WALLET

You have a wallet for you to collect your tokens.

You keep your account secure by using state of the art encryption and storing your keys locally in a secure vault on your device.

You may quickly connect any wallet you wish in our platform.

MetaMask, Ledger, Portis, MEW, Authereum, Fortmatic and etc. connect your wallet. Then get easy access to the GasFarm platform.

4.3 MANAGE TOKENS AND REWARDS

Earn maximum revenue yield farm rewards and ETH gas fees cashback with daily, weekly or monthly locks..

The rewards grow or decrease according to the amount of locked tokens on the farm.

At the same time, the reward amount increases in parallel with the lock times.

5. GASFARM TOKEN (GFT)

The native GFT token rewards participants who create value for the GasFarm ecosystem. GFT is fairly distributed, community-owned and self-governed.

GFT is an ERC-20 token secured by the Ethereum blockchain. 100,000,000 GFT tokens were minted at the Token Generation Event, after which no new tokens will be created.

The following details may be subject to change.

Token Utility:

GasFarm Token (GFT) allows users to receive cash rewards or cashback on Ethereum gas fees. Users can stake and collect their tokens for a specified period of time to earn reward tokens. This is a win-win situation as the user receives a cashback of gas fees in addition to the rewards of farm tokens.

5.1 TOKENOMICS

GasFarm Token (GFT) allows users to receive cash rewards or cashback on Ethereum gas fees. Users can stake and collect their tokens for a specified period of time to earn reward tokens.

This is a win-win situation as the user receives a cashback of gas fees in addition to the rewards of farm tokens.

| TYPE	% OF TOTAL	AMOUNT IN $	TOKEN AMOUNT	PRICE	UNLOCK
			GFT TOKENOMICS		
Private Sale	10%	$500K	10M	$0.05	Lockup for 1 month. Then 25% monthly is unlocked
Public Sale	30%	$3M	30M	$0.10	100% on initial listing
Rewards	35%		35M		From the start GasFarm app until 3 years
Foundation	5%		5M		Lockup for 2 years
Marketing	5%		5M		Lockup for 6 months.
Team	7%		7M		Lockup for 2 years
EcoSystem and Partnerships	5%		5M		Lockup for 1 year
Liquidity	3%		3M		$300K Total Uniswap liquidity will be locked for 1 year

5.2 GFT TOKEN DISTRIBUTION

At the Token Generation Event ("TGE"), 100,000,000 GFT tokens will be created by the issuer. This will be the final and fixed amount of GFT in existence, and it will not change.

GFT will be allocated as follows:

5.3 TOKEN SUMMARY

The table below provides the initial listing information of the GasFarm Token (GFT).
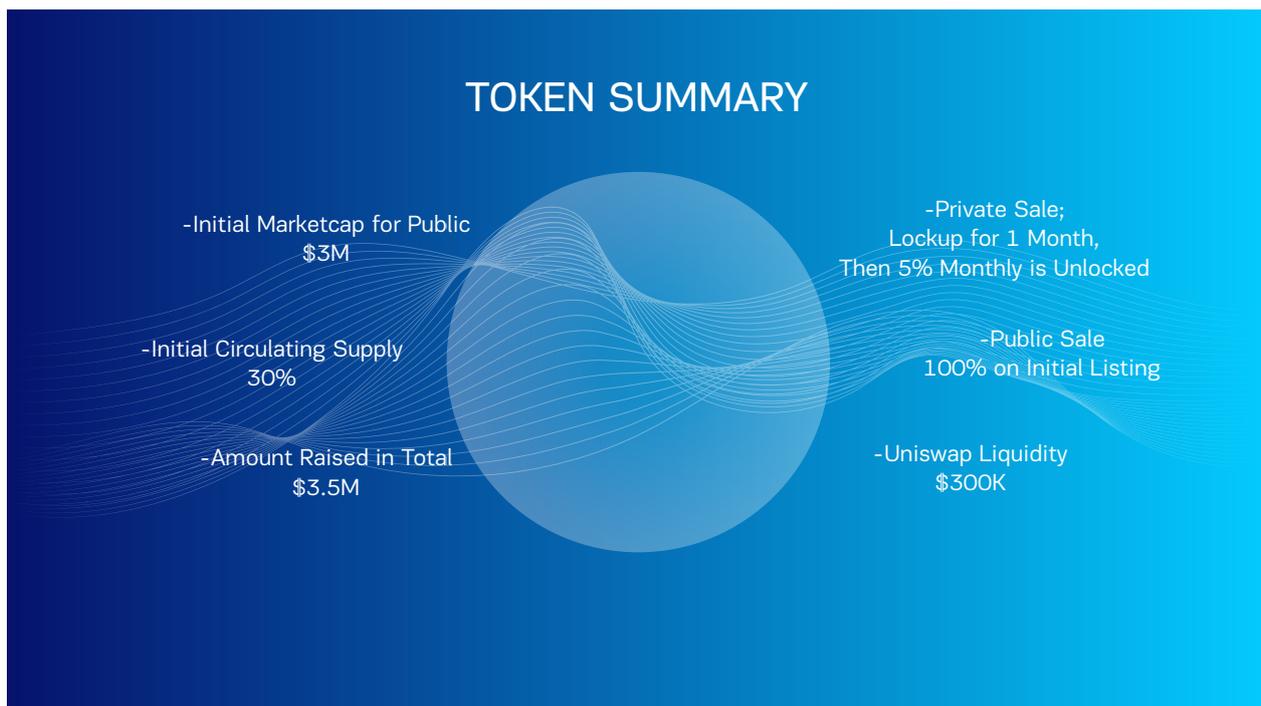
6 LEGAL DISCLAIMER

This lightpaper is for informational purposes only and does not constitute an offer or solicitation to sell securities or other investments. GasFarm does not guarantee the accuracy of statements made in (or in connection with) this lightpaper or the conclusions reached herein, and expressly disclaims any and all liability for any direct or consequential loss or damage of any kind whatsoever arising directly or indirectly from: (i) reliance on any statement contained in this lightpaper, (ii) any error, omission or inaccuracy in any such statement, and (iii) any other matter connected with or attributable to statements contained in this lightpaper.

hello@gasfarm.org