Monsoon Finance Whitepaper

Version 1.2

The Problem

The majority of today's blockchains are plagued by a single issue: Privacy. While the identities of users are preserved, the financial history is not. When cryptocurrencies are inevitably used as forms of payment for everyday goods and services, privacy is paramount, otherwise, anybody may readily discover the net worth of a platform’s users. The primary aim of self-sufficiency cannot be realized without privacy. Hence there are a few issues with existing blockchains regarding privacy.

Exposed Finance Records

Existing public blockchains have a significant privacy issue. By default, these blockchains share the exact details of all transactions including users’ wallet balances in plain view. Although the details of the transaction do not contain user identity, the availability of the wallet address and transaction history to anyone on the internet is still a legitimate privacy concern for most.

For example, if an individual goes to the grocery store now to buy some food, the grocery store cannot ask the individual's bank for their respective net worth or transaction history.

However, all this data is public with blockchains. Therefore businesses can make judgments about their customers, or worse, adjust their pricing, based on net worth.

In addition, when real estate deeds are represented as NFTs on blockchains, a public address can also reveal which properties an individual owns - potentially revealing where one lives.

Anyone with a particular user's wallet address may simply examine their address on block explorers like BSCScan, Etherscan, Polygonscan and evaluate their transaction history and holdings. This can have serious repercussions for crypto users as it makes private financial information public.

Lack of Multi-Chain Privacy

Existing blockchains have a large user base but fail to provide valuable services such as a multi-chain privacy bridge. This problem is more concerned with the flexibility provided to users and their overall experience with the platform. Hence

most blockchains fail to understand the needs of the users and without privacy tools are bound to fail in the long term.

Lack of Privacy on Cross-Chain DEXs

Most of the existing decentralized exchanges (DEXs) provide a plethora of features like removing third parties, offering unparalleled security, and so on, but fail to provide guaranteed privacy features. The swapping of assets between chains is made possible with existing DEXs but measures on privacy are ignored most of the time.

Solution: Monsoon Finance

Monsoon Finance, a multi-chain privacy protocol, overcomes existing blockchain challenges by providing private transactions to any and every smart contracts blockchain. It aims to solve privacy issues with tools like a Multi-chain Privacy Bridge and a Multi-chain Privacy DEX.

Multi-Chain Privacy Bridge

The Monsoon multi-chain decentralized privacy bridge will allow users to move assets from one chain to another in a completely trustless and private way. This is done through the use of zk-SNARK proofs that prevent the linkage of a deposit to a withdrawal. In addition, Monsoon nodes will stake MCASH to validate cross-chain transactions, and a majority consensus amongst staking nodes must be achieved for transactions to be processed, meaning the process is both decentralized and private.

The process is quite simple: a user will deposit a supported cryptocurrency into a smart contract and commit to withdrawing that asset on a supported chain. The user will then receive a ‘note’ that acts as a private key to that deposit. In the backend, Monsoon nodes listen for deposit events on all supported blockchains and aggregate them into blocks which they then construct into a blockchain. A majority of nodes must agree on the validity of the transactions in order for the blockchain to proceed and for the bridge to continue functioning.

After a certain number of signatures, the withdrawal smart contracts on every supported blockchain can be updated with new relevant deposits that can then be withdrawn. The user then uses the aforementioned ‘note’ to construct a zk-SNARK proof of the original deposit and submits the proof to the withdrawal

smart contract on the previously committed withdrawal chain. The proof is verified on-chain, and the withdrawal is processed to the user's requested withdrawal address. The zk-SNARK proof construction is done without revealing the original deposit, meaning the process is private - that is, an onlooker cannot link the withdrawal to the deposit.

Multi-Chain Privacy DEX

An interesting addition to the privacy bridge is a privacy DEX that can be automatically used when a user performs a private bridging transaction. This prevents an onlooker from understanding who originated the DEX trade. The process is again, quite simple: a user performs the same bridging process (deposit, wait, withdraw) and then requests the smart contract to convert (swap) the original asset to any other asset. The smart contract quickly converts the original asset to the requested asset and transfers it to the user's requested withdrawal address. This can be done as an integration with an already existent Uniswap-style decentralized exchange, or an alternative DEX can be constructed that is only used for private swaps.

To be clear, the privacy bridge is not a necessary precursor to the swap - instead, a user can simply perform a wallet-to-wallet private transaction (described

below) on the same chain, and the asset that has been ‘privatized’ can then be swapped immediately for another requested asset.

Wallet-To-Wallet Private Transactions

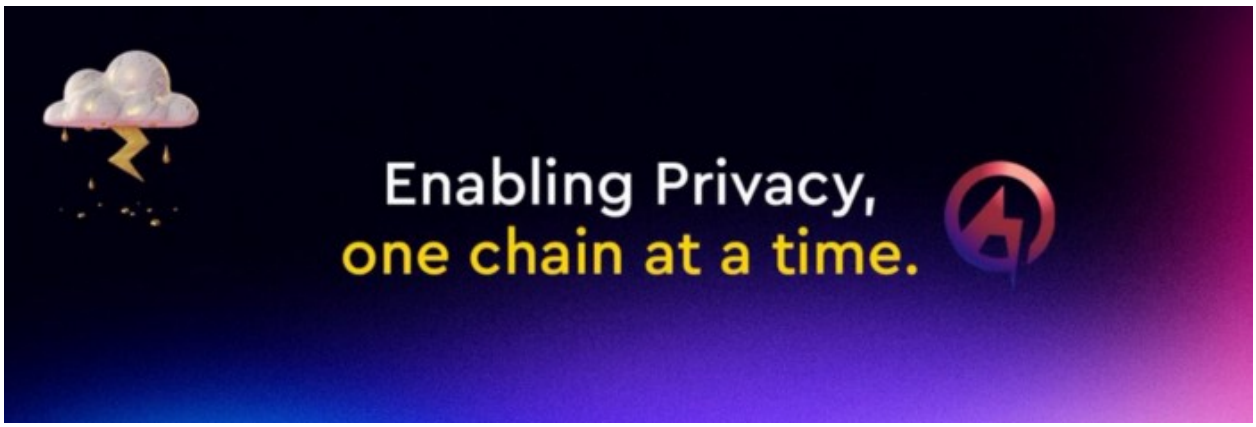
The final tool in the Monsoon privacy suite is a wallet-to-wallet privacy service that allows users to perform private transactions on any EVM-supported blockchain. The tool is a fork of Tornado Cash, with slight adjustments made to support different blockchains and the addition of a protocol fee. **This protocol fee, and all fees taken for the use of Monsoon privacy services, is used to buy back and burn MCASH from decentralized exchanges.**

The wallet-to-wallet privacy tool works similarly to the privacy bridge, just without the backend Monsoon node service. A user deposits cryptocurrency into a smart contract and is given a ‘note’ that acts as a private key for the deposit. If the note is lost, the deposit cannot be withdrawn. The user waits a certain period of time, depending on how many others are using the protocol and the degree of privacy they require - the longer the wait, the better the privacy.

After some time, say 15 minutes, the user uses the ‘note’ to construct a zk-SNARK proof that is then submitted to the smart contract. The proof is verified on-chain and the withdrawal is processed to the user’s requested withdrawal address. The

privacy tool uses a relayer service to submit the transaction on behalf of the user, further improving privacy.

This privacy tool is available now on Binance Smart Chain Mainnet at https://bsc.monsoon.finance and on Polygon Mumbai Testnet at htps://matic.monsoon.finance.



Product-Market Fit

Smart contracts are giving life to blockchain projects. The adaptability of smart contracts is necessary for blockchain platforms to perform smoothly. Similarly, adding privacy features within the smart contract world would prove to be very useful. But unfortunately, the vast majority of today's blockchains are missing privacy tools. This has led many people to assess each user's net worth and hence the overall decentralized self-sovereignty is not realized.

However, Monsoon Finance has created a method for enabling privacy on any smart contract blockchain. Monsoon Finance comes with features like a multi-chain privacy bridge and multi-chain decentralized exchange. The project, with its multi-chain privacy bridge, will enable the transfer of assets over any blockchain in a fully secure and decentralized manner while preserving privacy.

Monsoon nodes will stake MCASH to validate cross-chain transactions, and these transactions use zk-SNARKS to prevent nodes or any onlookers from linking deposits to withdrawals. A majority consensus amongst staking nodes must be achieved for transactions to be processed, meaning the process is both decentralized and private.

Monsoon's second major tool, a multi-chain privacy DEX, will allow users to deposit an asset on one chain and privately swap it for any asset on any other chain. The swap will use zk-SNARKs to obfuscate the identity of the party performing the swap. This addition to the suite of Monsoon privacy services will change the way assets are traded across all of DeFi. Institutions will no longer have to fear individuals tracking their wallets and copying their trades, for example.

Some of the competitors of Monsoon Finance include:

Tornado cash

Tornado Cash, or TORN as it is more often known, is a non-custodial, decentralized privacy solution built on Ethereum. It is known to increase transaction privacy by simply severing the on-chain link between the destination and source addresses. Despite having similarities with Monsoon Finance, it lacks the feature of a privacy bridge.

Secret Network

Secret Network is another blockchain that provides data privacy by default, allowing users to create and utilize permissionless and privacy-preserving apps. This one-of-a-kind feature protects users, secures apps, and enables hundreds of never-before-imagined Web3 use cases. Unlike Monsoon Finance, the Secret blockchain doesn't use zk-SNARKs for privacy preservation, instead of relying on TEEs (Trusted Execution Environment) which are hardware devices that can be tampered with.

Solbank

Solbank is the Solana ecosystem's lone privacy wallet. By severing the onchain link between transactions, consumers get complete financial security and anonymity. In other words, it functions similarly to a cash register. Despite the movement of money in this register, no one can know who previously possessed which bill. However, Solbank must compete with other platform wallets such as Phantom and Metamask for dominance, and the market is much more polarizing, meaning users are more likely to use only one wallet for all of the DeFi activities.

These are some of the close competitors for Monsoon Finance in the industry. But, with more advanced features like using zk-SNARKs, the multi-chain privacy bridge, and anonymity mining, Monsoon Finance stands apart from its competitors. It's a revolution to restore the fundamental right of privacy in a technological way.

Go-to-market Strategy

Multi-chain Privacy Bridge and Multi-chain DEX privacy

Multi-chain privacy is the prime feature provided by Monsoon Finance. It's already begun with wallet-to-wallet private transactions on Binance Smart Chain. You can view the Monsoon services available on BSC mainnet and Polygon testnet at monsoon.finance.

Monsoon plans to build community engagement with its services via partnerships with leading blockchain protocols. Three partnerships with large smart contract blockchains have already been attained, with more to come.

Moreover, Monsoon Finance is developing a Multi-chain privacy bridge where one can deposit assets on one chain and privately withdraw them on any other chain. This could revolutionize the industry in terms of privacy utility. Hence, Monsoon Finance is setting the bars high in terms of restoring the most fundamental right to privacy in the most technological way.

Recent developments

The recent months have been great for Monsoon Finance with Monsoon BSC being deployed on the BSC mainnet.

Monsoon Finance has also announced that it will be launching $MCASH IDO on Polystarter and BullPerks on 27th September 2021. Finally, Monsoon Finance is looking forward to collaborating with smart contract platforms and building the groundwork for its mining campaigns.

Upcoming announcements

Over the next few months, Monsoon Finance is set to make several major announcements and roll out new features starting with its upcoming IDO with Polystarter and Bullperks. This will be followed by deployments on Matic/Polygon, Fantom, and Avalanche.

Monsoon Finance will also include 2 additional instances on its blockchains, and the alpha implementation of the privacy bridge will be completed by EOY 2021. By 2022, they anticipate that their protocol will become self-sufficient through generated revenue and governance. This would go hand in hand with the implementation of Multi-chain privacy DEX functionality which is also scheduled for the end of Q2 2022.

Investors

Monsoon Finance's unique proposition and distinctive features have attracted massive attention from the industry. Monsoon's one-stop solution for DeFi with privacy is promising. As a result, multiple prominent investors like AU21 Capital, Polygon, NGC Ventures, Lotus Capital and more have offered it investment and strategic support. It not only proves the project's potential but also strengthens its mission and builds confidence in the community members.

Implementation Plan: Roadmap

Monsoon Finance's smart contracts and front end on Binance Smart Chain are live but still in beta. At the same time, they are aiming to complete liquidity farming programs before launching a token. In the close future, the project is looking to have BUSD mixer contracts up and running.

Despite being ready to start operations, the Monsoon team is taking extra precautions by examining their systems and addressing any minor or major issue to provide their users with nothing but the finest. After its completion, the next step would be to launch the Monsoon privacy service on several other chains and

create the cryptocurrency infrastructure required to expand Monsoon to millions of users.

Shortly after the launch of MCASH, Monsoon will set up its exclusive “Anonymity mining” feature to generate yield by depositing assets in the Monsoon privacy pools that come with advanced privacy features.

Last on the list is creating Monsoon NFTs on the Polygon network. This is the ultimate roadmap for Monsoon Finance for now, and it’s just a matter of time Monsoon expands into a huge network that makes privacy on blockchain mainstream.

Team & Advisors

Monsoon Finance has gained significant public attention quickly in the DeFi space, and the credit for such efficient growth undoubtedly goes to its expert & veteran team members and advisors.

A team of skilled and experienced professionals always delivers the best; the same is the case with Monsoon Finance. Each team member comes from a

different professional background, and everyone is the master at their craft, which has benefitted the project's growth remarkably.

Monsoon: Enabling Privacy, one chain at a time.

Appendix: Tokenomics

MONSOON

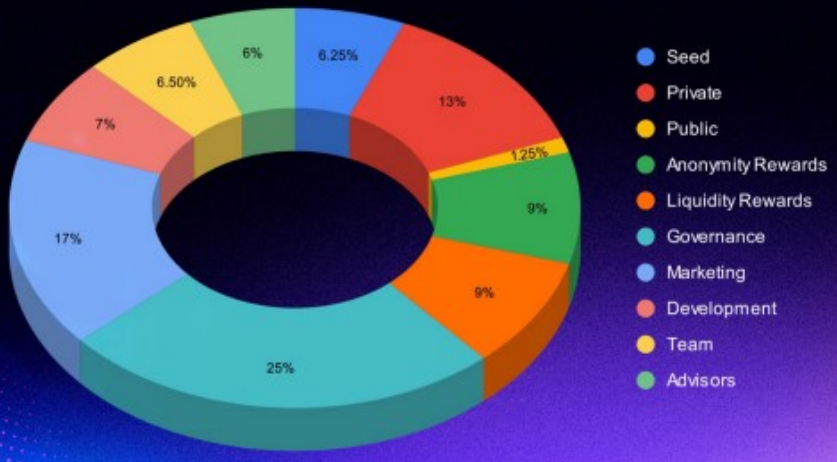
Tokenomics

Round	Token Allocation	% Total Supply	Price Per Token	Vesting
Public Sale	1,250,000	1.25%	$0.20	50% unlock at TGE, then 25% every month thereafter
Private Sale	13,000,000	13.00%	$0.153	8% unlock at TGE, then 10% every 30 days for 270 days
Seed Sale	6,250,000	6.25%	$0.08	5% unlock at TGE, then 10.55% every 30 days for 270 days
Governance Treasury	25,000,000	25.00%		5% unlock per month, after 3 months
Team	6,500,000	6.50%		5% unlock per month, after 3 months
Development	7,000,000	7.00%		5% unlock at TGE, then 5% every month
Advisors	6,000,000	6.00%		5% unlock per month, after 3 months
Marketing	17,000,000	17.00%		5% unlock at TGE, then 10% every month
Privacy Farming	9,000,000	9.00%		Linear distribution over 1 year
Liquidity Farming	9,000,000	9.00%		Linear distribution over 1 year

monsoon.finance @MonsoonFi @monsoonfinance @monsoonann

MONSOON

Token Distribution



monsoon.finance @MonsoonFi @monsoonfinance @monsoonann