FlashSwap: a protocol for the decentralised crypto derivative market trading

Whitepaper 1.0

Abstract

This document presents a brief summary about the collection of protocols that facilitate the creation of different financial products to be created, issued, and traded for any pair of underlying ER20 tokens. Our approach uses off-chain order books with on-chain settlement to allow creation of efficient markets. Our protocols are entirely secure and trustless, creating a truly distributed market with no central management. All of our protocols are open and extendable by anyone, requiring no special permissions to be used with other smart contracts.

Contents

1 Introduction

The blockchain revolution brings with it the ability for anyone to own and transfer their assets across an open network without the need for any third-party intervention, removing the need for trust and ensuring consistency and correctness of all movements as well as providing an open, public ledger that provides indelible tracing of these transactions. This concept has led to a rapidly growing uptake and the number of assets is growing at a tremendous rate. There are many centralised platforms offering the facilitation of exchange across this estate, and these systems currently generally offer the ability for traders to take long positions in assets, however there are very few systems that allow engagement with more complex financial positions.

FlashSwap aims to utilise the ERC20 asset class to provide a facility that offers classes of products such as derivatives and margin trades, which in turn allows the more sophisticated investor to manage their portfolios more efficiently and effectively as well as opening up further routes for speculation. The decentralised, trustless nature of our offerings means that individuals will always retain complete control over their assets throughout the trade. The more traditional blockchain based trading systems currently cater predominantly to the less experienced trader, but opening up these more sophisticated financial products opens up a vastly lucrative market: Derivatives alone account for a market that is estimated to be greater than 10 times the global GDP, and as blockchain becomes more popular and with the onset of security tokens offering the capability to tokenise real-world assets, this market can be opened up to blockchain. Our aim is to capture part of this market and to be early to market with this concept on blockchain. Our intention is to utilise ERC20 tokens for trading, which are generated from the Ethereum platform because we feel this offers the greatest room for growth as well as significant performance advantages which will become essential as this market expands. To succeed, FlashSwap must meet three key criteria:

- **Security and correctness:** FlashSwap must be designed with security and testability in mind.
- **Blockchain performance:** FlashSwap will be and will remain at the cutting edge of public blockchain performance in terms of latency and throughput.
- **Application performance:** The application layer must perform on par with professional non-blockchain-based trading must perform on a par with professional non-blockchain trading systems.

However, there are other things we also need to address and to understand this, we first need to take a look at the two types of exchange which will be presented in the next section.

2 CEX vs DEX

Today, most financial exchanges are centralised. This means that money deposited by users is often held in one location. For hackers, that location is known as a 'honey pot' - the sweet spot they aim to attack.

Centralised exchanges have a history of poor security, and they have not performed particu- larly well in recent years. We have seen many hacks over the past year - and this is not unique to crypto exchanges; we see many examples in the 'real world' of attacks taking place on large organisations, which are made possible purely because of centralisation. As a consequence of this, centralised exchanges are becoming more of a structural risk to the global financial infras- tructure. A decentralised exchange would disseminates funds, leaving no single honey pot to be targeted by hackers.

The other issue is that a centralised exchange is effectively a ’middleman’ in the transaction and the issues here are that of performance, availability and cost. System downtime is also an issue because when this happens, user funds become locked during this time whilst with a decentralised exchange, though it may require maintenance and downtime, during this period user funds remain available to them throughout. However, generally, centralised exchanges are great. Yet, they have fundamental flaws which result from having everything in one place. These issues are addressed by disintermediating and automating the process. However, if decentralised exchanges are so great, why does nobody use them?

Despite their benefits, decentralised exchanges remain underutilised. It has been estimated that trading on centralised exchanges vs on decentralised is in the region of 500:1. This is because despite seeing decentralised exchanges introduce useful new features, they are forgetting to combine with what competitors are offering (that is the spirit of open-source after all) and what incumbents already offer (how else do you expect people to move from their trusted service providers).With this in mind, decentralised exchanges currently face two fundamental issues preventing institutional adoption: insufficient infrastructure and the lack ofa user-focused, progressive interface (UX/UI). FlashSwap aims to address both of these issues and we will discuss this later in the document, however first, we would like to explain the fundamental components ofthe platform itself.

3 The FlashSwap blockchain

In this section, we present the key characteristics of the FlashSwap blockchain.

3.1 Smart contracts

Fortunately the Ethereum platform already implements Smart Contracts extremely well, so the FlashSwap system will not need to implement its own Smart Contract system, though it will need to enhance the existing contract system to implement features specifically designed to facilitate secure handshaking between all parties involved in a financial transaction such that funds are contractually transferred appropriately based on the agreed parameters ofthe agreement. In order to provide this, FlashSwap will implement its own ERC20- based blockchain utilizing token (FlashSwap Token).

3.2 Blockchain layer

The FlashSwap blockchain will be ’proof of stake’ in order to provide sufficient performance, scalability and flexibility. It will use Tendermint for consensus, which provides a 1-second block time, latency between 015-1.5 seconds and can process up to 4,000 transactions a second. This is required in order to support high trade volumes on the network. All transactions undergo initial validation by the system and are then processed by the FlashSwap application only after each block is finalised. This is required in order to support high trade volumes on the network. All transactions undergo initial validation by the system and are then processed by the FlashSwap application only after each block is finalised.

3.3 Abstracted pairing

In order to arbitrate financial transactions between trustless parties, we need common ground and smart contracts. The FlashSwap blockchain will utilise its own token (FlashSwap Token) to act as this common ground, through a concept we call ’Abstracted pairing’. This is essentially a way to converting all other tokens in the transaction to FlashSwap Token using a “stablecoin” mechanic.

Once all currencies are converted to FlashSwap, the management of any transfers and transactions are vastly simplified. The ’pairing’ refers to the process of how every tradeable ERC20 token in FlashSwap will be internally paired with the FlashSwap token.

Conversion to FlashSwap Token will then capture with that transaction the value ofthe FlashSwap Token/targetcoin pairing at that point, to avoid value drift during the lifetime of the transaction. Note that this conversion process all happens within wallets owned by the trustless parties. At no point do individuals lose ownership or control over their currencies outside of the smart contract agreement. To illustrate this, consider the case where a seller wants to sell token XYZ, which is an ERC20 token. They submit their sell order which immediately converts XYZ to FlashSwap token using the current XYZ/FlashSwap Token pricing and records the price at this point. The FlashSwap token is deposited in our sellers FlashSwap wallet.

A buyer wishes to purchase XYZ, and therefore submits a bid using their own currency (ABC). This is again converted to FlashSwap Token in the same way, and then a smart contract is generated to allow the exchange of the seller’s and buyers’ FlashSwap Token tokens. After contract resolution, the seller receives the buyer’s FlashSwap Token and vice- versa. The seller then has their FlashSwap Token automatically converted to ABC at the buyer’s recorded rate and the buyer receives XYZ at the sellers recorded rate. This simple example serves to illustrate the basic mechanics here, which are required in order to introduce Smart Contracts to a ERC20-based transaction.

4 Trading Protocols

With FlashSwap, we aim to deliver a number of different financial products, starting with those we perceive to attract the greatest interest, in order that we can build trade volumes up as quickly as possible.

Our initial suite of products will include (but will not be limited to) Margins and Option trading. Both of these trades require the use of the following subsections.

4.1 Collateral/escrow

In some cases, transactions require some tokens to be held in escrow as collateral for the transaction. When this happens, the tokens will be effectively frozen from use while the Smart Contract is in force.

Collateral will be locked in FlashSwap Token tokens, which takes them out of circulation for the duration of the trade. This will decrease selling pressure for FlashSwap Token tokens and add value to the token price.

4.2 Margin trading protocol

Margin trading allows a trader to open a position with leverage. For example, if we opened a margin position with 2x leverage and our base assets had increased by 10%. Our position would have yielded 20% because of the 2X leverage. Standard trades are traded with a leverage of 1:1.

In FlashSwap, due to its decentralised nature, margin trading will be possible only via the existence of the lending market.

Lenders are other users on the exchange that provide loans to traders so they can invest in larger amounts of coins, and lenders benefit from the interest on the loans. The lending and borrowing between the lender and borrower will be managed via a smart-contract mechanism, ensuring complete transparency.

4.3 Margin trading mechanics

The Margin Trading protocol uses the FlashSwap Smart Contract system in order to facilitate decentralized margin trading, along with the FlashSwap Allowance functionality which permits the contract to manage the transaction between the respective parties. Basically a contract will be defined between the lender, the borrower and the buyer. These contracts will be open and indisputable, but handled entirely without third party involvement.

4.4 Opening a position

Opening a position through the Smart Contract requires the following transaction packet from a trader:

- The amount of tokens the trader wishes to borrow.
- The buy order offering to buy the token to be borrowed from the lender, in return for their converted FlashSwap Token held in escrow.
- The amount of token the trader wishes to deposit.
- The address that will own the position after opening.

When the contract receives the transaction the following happens:

1. Transfers of the offered deposit from the trader to the escrow vault (tokens controlled by the Smart Contract and frozen using Ethereum contractual mechanics).
2. Transfers of the requested amount of the owed token from the lender to the borrower.
3. A record is maintained to show that the requested amount of the loan has been used.
4. Contract handles the exchange of the owed token for the amount of held token offered by the buy order. The contract will then verify the validity of all elements of the transaction and then execute the trade.
5. Transfer of the held token received from the sell to the secure vault. The held token remains locked in Vault for the duration of the position.
6. The details of the position are stored in the contract, mapped by a unique public identifier. This identifier can then be utilised by the trader and/or lender to manage the position.

All steps happen in parallel, either succeeding or failing as a ’packet’. There will be no outcome where anything partially succeeds or fails. At the conclusion of the trade, the secure vault contains an amount of held token for the position. This remains in the vault until the position is closed, after which they are released.

4.5 Closing a position

The trader has the right to close any part of the position, at any time by raising a sell order that offers to sell at least the amount of token owned to the lender (including any interest charges incurred) for an amount of the vault-held token.

4.6 Calling in the loan

The final way a margin trade can be settled is by the lender calling in the loan from the trader. This can happen at any time during the trade and is achieved by the lender sending a request to call in, along with the amount of lent token that must be deposited into the position by the trader to cancel the margin call. The trader is then given a fixed time to either pay back the loan or put up additional tokens into escrow.

If the trader fails to meet the deadline, the lender is entitled to the entire escrow-held balance locked in to the position. This is generally raised as a transaction when the price of the owed token relative to the escrow token rises to the point where the escrow token in the position may no longer be sufficient to buy back the owned amount. This, along with the fact that in order to settle within the time limit, means that both trader and lender need to be online continually in order to manage the trades. This clearly is not practical, therefore FlashSwap offers functionality to manage this automatically:

4.7 Automatic management

In order to address this issue of both trader and lender needing to continually monitor trades in order to respond at the right times, FlashSwap will implement the ability for users to define actions to execute automatically based on specific criteria being met:

- Calling in of a position if escrow token is within *x*% of payback amount
- Automatically pay back or increase deposit amount if loan called in, based on projected price movement (using TA indicators or simple calculations)

The automatic management will require the user to grant delegation of position management to a FlashSwap management module, however ownership of all tokens within the transaction will continue to remain with the original actors.

4.8 Options trading protocol

Options are derivative instruments that give the holder the right to buy or sell a cryptocurrency at a predetermined price (Strike price) sometime in the future (expiry time).

Options are a great way to hedge financial risk from unforeseen events. They are also used regularly by options traders in order to make a profit on very volatile financial assets. This is why they would be ideal for cryptocurrency trading.

Before we can take an in-depth look at cryptocurrency options, we have to cover some basic option theory. There are two types of options that one can buy. These are a CALL and a PUT option. A CALL option gives the holder the right to buy an asset at the strike price. A PUT gives the holder the right to sell an asset at a predetermined price.

The cost of buying an option is called the option premium and this price is determined by a number of factors. These include such variables as the strike price, the current price, the time to expiry and the volatility. A full overview of these factors is beyond the scope of this text but you can read more about option pricing here.

What is important to understand is that someone who is buying a CALL option is hoping that the price of the cryptocurrency asset will increase in price and will be above the price of the Strike price at expiry of the option. The opposite can be said for the buyer of a PUT option.

4.9 Options trading mechanics

FlashSwap will use three actors in the creation of an Options trade: Creator, Contract, and the OptionCover. We also will assume for the purposes of this explanation that all currencies have already been converted to FlashSwap Token so that the transaction can utilize smart contracts.

4.10 Issuance

Issuance of options can occur at any time before the option expiry date and this therefore means that each option can be publicly traded individually. The following mechanics facilitate the issuance process:

The Creator is responsible for creating an instance of an Option Cover Cover. A valid instance requires the following information:

- The address of the FlashSwap Token token the option is for (referred to as base token).
- The address of the FlashSwap Token token the strike price and premium are to be paid in (referred to as the quote token).
- The strike price (broken into two parts to form an exchange rate between base token and quote token).
- The option expiration date.

5 Liquidity

The simplest solution is for the protocol to include a fee, payable to some organisation that is tasked with attracting liquidity. This has several disadvantages that:

- it introduces unacceptable centralisation around the organisation in question, allowing it to favour some markets and effectively censor others by controlling the provision of liquidity;
- the organisation would be a bottleneck for the launch of new markets, which could severely compromise the ideal of permissionless market creation; and
- it would eventually give rise to a large and bureaucratic operation that would be liable to misallocate resources and lose out to more nimble ecosystem based alternatives.

To achieve our design goals therefore requires that incentivisation of market making be built into the protocol, and that this caters for markets with different trading volumes, and at different points in their lifecycle. This is achieved through facilitation at the protocol level of dynamically priced liquidity, which recognises that market making is capital intensive and thus aims for a market-driven solution that efficiently balances the need for order book depth on the one hand with a preference for low fees on the other.

5.1 Mechanics of the liquidity

FlashSwap is in essence a peer-to-peer liquidity facilitation protocol with liquidity able to be priced individually for each market. The liquidity fee is incurred — in a quantity determined by the volume and price of the potential trade, as well as the market's current liquidity price — by an aggressive, or price-taking order when it trades. In situations such as auctions where there is no maker-taker relationship between the counterparties, the cost of liquidity is shared equally. The liquidity cost is later credited during settlement to the participants responsible for the provision of liquidity in the market: the price maker, the market's infrastructure operators, and the market makers. The price maker and infrastructure operators will receive appropriate amounts, with the remainder divided between the instrument's market makers, with relative allocations based on individual contributions to the order book liquidity. Market making volume is more valuable to the market when it is more competitively priced and consequently, the relative allocations between market makers of the liquidity reward takes their historical pricing into account. Since market makers have a choice of where they deploy their capital, they will rationally select markets that offer the highest potential liquidity returns over their investment horizon. Their liquidity returns depend on: trading volume, their share of the liquidity rewards, and the liquidity price, which is always calculated in terms of the base currency of a market. Liquidity pricing is the protocol's mechanism to ensure liquidity is being attracted to markets that have the greatest need and that all markets operate at the most efficient costs for participants.

6 Token economics

6.1 Staking and voting

The primary on-chain governance mechanic in FlashSwap is voting by network participants based on their stake within the scope of the poll, for example: i) for network governance issues, like the creation of a new market or determination of network parameters, stake would be measured in terms of a participant's holding of the network's native crypto-asset; whereas ii) for market governance decisions, stake may be measured by the notional value of a participant's net position, their market making stake or a combination of both. Where a crypto-asset is allocated to a risk universe, either as fees or as trading collateral, it is considered to be held by the network rather than the participant and so will not be counted against the participant's votes. In some cases, the network may 'vote' for a default option with the weight of any such assets. However, assets held by a FlashSwap network but not allocated to a risk universe will be included in a participant's stake for any votes. A participant can only vote one way in any given poll, and will always be deemed to have voted with their full available stake. The required majority for a decision and minimum participation will be defined for each type of poll, with a 2/3 majority and 0% minimum participation36 being standard. For votes requiring a certain (non-zero) participation level, the proposer will forfeit some of their staking asset if the minimum required participation level is not reached. This measure is in place to ensure that 'proposal spam' has a cost and that governance proposals do not create a vector for liveness attacks. In order to remove the incentive for various malicious behaviours such as voter bribery, there is the potential to introduce secret ballots for on-chain governance voting using principles from homomorphic encryption and secure electronic elections technologies.

6.2 Market proposal and new market creation

A proposal must specify the tradable instrument, including product, product parameters, risk model, risk parameters, trading mode, and market parameters, and the size of the participant's market making commitment, which will become their market making stake . Proposals will be visible to all participants, and must successfully complete the process described below before a market becomes tradable. If a market creation proposal gets through, market creators will need to pay for a listing fee which is in forms of platform tokens. 50% of fees will be allocated into a fee collection pool and rewarded to stakers and governance, and the rest of the fees will be burned permanently.

6.3 Liquidity incentive mechanism

Liquidity mining is a community-based, data-driven approach to market making, in which a token issuer or exchange can reward a pool of miners to provide liquidity for a specified token. You earn rewards by running a market making bot that maintains orders on exchange order books. A large percentage of the token allocations is for liquidity providers since this is the most important factor to boost our platform. Unlike most financial platforms which give out equal amounts of tokens weekly, we introduce first comers advantage schemes, which first comers (early liquidity providers) will get on average more token rewards than others. The weighted percentages of early liquidity contributors are higher. Liquidity token rewards will be distributed on a weekly basis.

6.4 Transaction fees

All transaction fees from all markets will be gathered into the fee pool. 50% of the fee pool will be burned on a weekly basis and the rest of 50% will be evenly distributed stakers and governance based on their staking power.

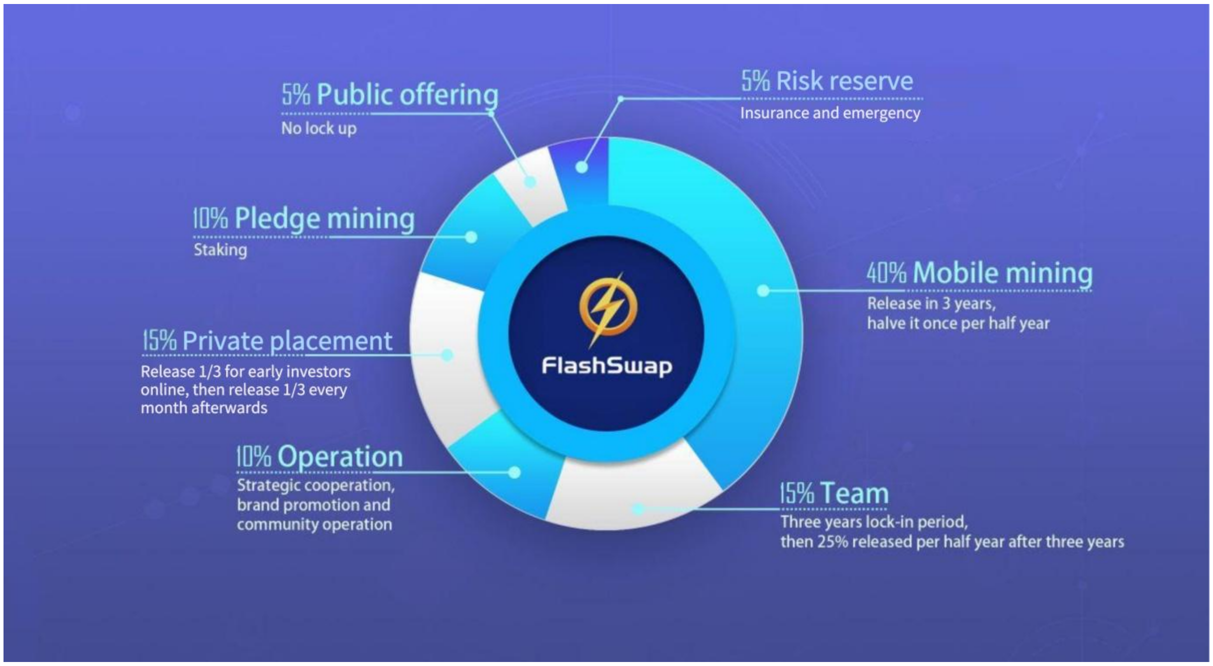
6.5 Token distribution

Token name：FSP

Total Token：40,000,000 FSP

Token distribution:

1.	Mobile mining：	16,000,000	FSP	40%
2.	Team：	6,000,000	FSP	15%
3.	Operation：	4,000,000	FSP	10%
4.	Risk reserve：	2,000,000	FSP	5%
5.	Pledge mining：	4,000,000	FSP	10%
6.	Private placement：	6,000,000	FSP	15%
7.	Public offering：	2,000,000	FSP	5%



6.6 The use and release rules of Token

1. Mobile mining: In order to provide a better environment for the growth of the project and to provide a better liquidity for Token, the feedback will be given back to the community through AMM in a deceasing way within 3 years, halve it once per half year.

2. Team: The portion of incentive for team will be locked in for three years, then release 25% every half year after three years.

3. Operation: For early strategic cooperation, the entire upstream and downstream industries and cooperation, brand promotion, media placement and community publicity.

4. Risk reserve: For purchasing NXM insurance and responding to emergencies.

5. Pledge mining: For long-term investors and holders who accompany the growth of the project, staking will be carried out with a period of 3 months to 1 year.

6. Private placement: Release 1/3 for early investors online, then release 1/3 every month afterwards.

7. Public offering: Public sale of FSP in circulation.

7 Our Team

Kamram Reynolds: Over 6 years of experience in fintech and data product strategy, data science products, and technology architecture, building successful SAAS, PAAS, and blockchain data services platforms in multi languages.

Steven Stankovic: 5+ years experience in software development, Senior Java / J2EE / Web / Android Developer and Architect with more than 5 years experience of full time work.

Peirre Richard: Network full-stack engineer, specializing in automated operation and maintenance, and has extensive experience in development and product shaping

Adam Taylor: With a PhD in computer science, he is an experienced infrastructure analyst.