Serum - White Paper

Serum Foundation

July 2020

For the most up to date information on Serum, visit our road map

Contents

1 Introduction

This is the summer of DeFi. We've seen the release and growth of hundreds of projects in the space, which together have created a more powerful DeFi network; clean, intuitive interfaces; and an explosion in locked value. We've also seen the introduction of a number of new, novel projects.

But novel and well-designed aren't the same thing, and many of the underlying weaknesses of DeFi remain.

1.1 Speed and Usability

Above all else, DeFi is slow and expensive. It costs dollars to do a trade, and minutes for it to clear. This is fine for some use cases–but many customers prefer the fast, cheap execution of centralized exchanges. It's hard to stare at your Metamask wallet waiting for a trade to be confirmed without missing centralized exchanges.

1.2 Centralization

When you trace all the way through, most DeFi protocols bottom out in a centralized oracle–often in the most crucial step.

Sometimes, this is a liquidation price oracle pointing to centralized exchange APIs. Other times it's a council of token holders. Sometimes it's the team of the protocol itself.

There's a further problem, too–most decentralizing protocols are computationally intensive. Fitting them into the ETH blockchain in a way that is cost efficient and fast has largely eluded the space.

That's not to say that centralization is always bad! USDT, USDC, and similar tokens are great projects which have revolutionized the entire crypto industry. They power much of the volume, and if you want something that can be turned into a dollar 24/7 that's the only game in town–and probably always will be. Because fundamentally dollar bills aren't on the blockchain, they're in bank accounts.

But if what you want is pure DeFi, the options are few and far between.

1.3 Stablecoins

Banks aren't on the blockchain, and neither are physical dollar bills. So how do you build a stablecoin that is always worth a dollar, but also doesn't rely on a bank account not getting shut down?

1.4 Orderbooks

Uniswap has quietly revolutionized DeFi by allowing trading without orderbooks.

But the more remarkable thing is that Automated Market Making is necessary. AMM is a system where there are no limit orders, or even bids or offers; in an orderbook, you can decide the price, size, and direction you want to trade. There are lots of disadvantages to AMM. You can't provide liquidity unless you provide both sides; you can't choose to only provide at a particular price; you can't provide at a price other than the current market price; and you can't choose the size to provide there without providing way more behind it.

There's a solution to this–it's what the rest of finance does. But DeFi doesn't have orderbooks, by and large, because the ETH network is too slow and expensive to support them. Matching bids and offers with each other involves a bunch of operations.

1.5 Cross-Chain Support

There have been many attempts at cross-chain support. WBTC is probably the most known, creating an ERC20 token wrapping BTC; Thorchain is building an entire protocol that allows for complete, fast cross-chain support.

There are lots of ways to attempt it. One thing all of the current versions have in common, though, is an oracle, or panel of token holders, or some other place where the truth is decided by people expected to be honest. Because, fundamentally, BTC isn't on Ethereum, so how can a smart contract know or impact its transfers?

Enter Project Serum.

Serum isn't perfect; nothing is. There are fundamental tradeoffs between speed and decentralization; between sophistication and ease of use.

But Serum is different, and it's powerful. Its software enables a fast DEX; it has cross-chain support, stablecoins, wrapped coins, orderbooks, and the ability to create custom and novel financial products; and while having all of those, it's fully decentralized. There are no oracles to centralized price feeds; no tribunals whose honesty you rely on. Serum is pure DeFi. And unlike current DeFi, it's fast and cheap.

2 Project Serum

Project Serum will unveil a fully functional decentralized exchange with trustless cross-chain trading, all at the speed and price that customers want. And despite living natively on Solana, it will be interoperable with Ethereum. Serum is made of seven main ingredients:

- SRM: the Serum token is the utility token of the Serum ecosystem
  - SRM will be fully integrated into Serum, and also benefit from a buy/burn of fees
- Cross-Chain Swaps: trustlessly exchange assets between chains
  - This is in contrast to most current protocols that rely on trusted parties to administer the swap
- Orderbook: a decentralized automated full limit orderbook
  - This will give traders full control over their orders, unlike automated market making.
  - Orderbook and matching is fully automated on-chain and orders are from Serum end users
- Full Ethereum and Solana integration
  - This will make Serum fast and efficient–all while being interoperable with the Ethereum ecosystem and ERC20 tokens
- Physically settled cross-chain contracts
  - These will allow easy margin positions in DeFi on synthetic assets
- SerumBTC: a model for creating an ERC20 or Solana tokenization of BTC
  - This would be a fully trustless BTC token
- SerumUSD: a model for creating a decentralized stablecoin
  - This would be a decentralized stablecoin that does not have a single point of failure

3 SRM

SRM is anticipated to hold the following utility:

- All of the net fees on Serum go to a SRM burn
- Holding SRM gives one up to 50% off of all fees on Serum
- Holding 1 MSRM gives a 60% discount on fees
- Fees may be made payable with SRM
- SRM and MSRM will be made available on Serum
- SRM can be staked on a node. Each node must have at least 10,000,000 SRM, and must include at least one MSRM. Nodes are expected to play the following role:
  - Each node may be called upon to provide insurance for a cross-chain transaction. They will receive a portion of the fees for any transaction in which they do this. Such collateral may be subject to certain default risks.
  - There will be a fund of SRM that will be distributed as staking rewards to each node.
  - Each node has a leader–the one who created it. A portion of all the rewards for that node will be given to the leader.
  - Nodes perform important duties to optimize the performance and throughput of the Serum ecosystem. Rewards or penalties can be paid based on their execution.
- Serum is anticipated to include a limited governance model based on the SRM token. While most of the Serum ecosystem will be immutable, some parameters without large security risks (e.g. future fees) may be modified via a governance vote of SRM tokens.

The SRM distribution is projected as follows:

- 20%: Team and Advisors
- 22%: Project Contributors
- 4%: Locked Seed and Auction Purchasers
- 27%: Partner and Collaborator Fund
- 27%: Ecosystem Incentive Fund

Some of the ecosystem partners have set aside a portion of their SRM to redistribute to holders of their native tokens or to otherwise spur SRM adoption. This is anticipated to be at least 5% of the total supply over time.

Serum is natively on the Solana blockchain (as an SPL token) and available on the Ethereum blockchain (as an ERC20 token).

The circulating supply at launch will be approximately 10%. This will grow by approximately 15% per year.

All presale, team, and contributor tokens will unlock between 1 and 7 years after listing.

10,000,000,000 SRM tokens have been minted; there will never be any more.

The amounts set forth above are as anticipated, and may be subject to modification.

4 Cross-Chain Swaps

The standard problem in cross-chain DeFi is: if Alice has 10 ETH and Bob has 1 BTC, how do they swap those without either being able to steal the others' money? Who delivers first?

Most other protocols do some version of the following:

- Alice sends her ETH to a smart contract
- Bob sends BTC to a multi-sig wallet
- Some set of nodes who control the keys to those wallets send the BTC to Alice and the ETH to Bob.
- Some set of arbitrators observe. They decide if the operation was carried out as intended; if not they punish the nodes.

There are a lot of advantages to this. One disadvantage is that it relies on those arbitrators to be honest.

Serum doesn't.

Here's how Serum works:

- Alice sends her ETH to a smart contract (SC)
- Alice and Bob each send some ETH collateral to SC
- Bob is supposed to send BTC to Alice
- If he does, then SC sends the ETH to Bob and returns collateral; all is good

- If he doesn't, Alice disputes
- Alice and Bob both send the BTC blockchain history to SC
- SC decides who's right
- If Alice is right, SC returns her ETH, her collateral, and gives her some of Bob's for the hassle
- If Bob is right, SC sends her ETH to Bob, some of her collateral to Bob for the hassle, and returns Bob his collateral

This guarantees the following core properties:

- If Alice is correct and honest, SC will settle in her favor
- If Bob is correct and honest, SC will settle in his favor
- Settlement isn't prohibitively expensive or long
- Efficient behavior is incentivized, and people are compensated if the other defects

A and B are true because, even though the ETH blockchain can't read or modify the BTC blockchain itself, it can verify it. SC is programmed to parse whether a proposed BTC blockchain is valid; it can then check which of Alice and Bob send the longer valid blockchain, and settle in their favor.

C is true: the dispute process is long but not prohibitively so; it takes roughly $100 of gas.

D is also true: because of the collateral, Alice loses if she's dishonest, as does Bob if he is; so Bob is incentivized to send the BTC, and Alice is incentivized not to dispute it if he does. This means that, the vast majority of the time, mediation will not be used, and so the protocol will be fast and cheap.

This protocol generalizes to any transaction where the target blockchain (BTC, in this case) is proof of work, and the base protocol (ETH, in this case) is much faster than the target blockchain.

Furthermore, when the target blockchain supports smart contracts, a modified version of this similar to optimistic rollups can allow for locked tokenized assets : the target blockchain can also simulate a hash of the Solana blockchain, allowing full cross-communication and thus smart-contract creations and redemptions.

This will allow users to seamlessly transfer assets between BTC, ERC20, and Solana, giving the current DeFi ecosystem easy access to the speed and efficiency of Solana.

This is a crucial aspect of Serum: despite being on Solana and having the speed and cost effectiveness that go along with that, it will be fully usable from Ethereum. This means that existing DeFi projects can access Serum's features and liquidity directly from their native blockchain, creating seamless integration between the current infrastructure and Serum.

5 Order Book

Serum's automated on-chain limit orderbooks allow users to submit orders with directions, prices and sizes, giving them control over their trading. Serum implements orderbooks between tokens; and because of its cross-chain support, it also has ETH and BTC orderbooks. These orderbooks are not centrally controlled– they are fully programmatic–and will automatically match orders between third party users.

Orderbooks are among the more computationally intensive products in DeFi. The Serum protocol includes a large number of optimizations to the matching engine in order to make the order matching faster and cheaper.

These orderbooks then serve as the core pricing source for Serum. There is a fee charged on each trade. All of those net fees go into a buy/burn of SRM. Furthermore, holding SRM decreases your fees paid.

6 Solana

Solana is a blockchain with significantly higher speed and lower costs than older blockchains. It has multiple settlement cycles per second and costs less than a penny to send a message–both orders of magnitude above existing standards.

The Solana-based Serum DEX will have the speed, cost and UX that users expect from a centralized exchange–all while being trustless and noncustodial. And because of Serum's full cross-chain integration, users will be able to trade BTC, ETH, ERC20s, SPL tokens (the token standard on the Solana blockchain), and more on it.

This will finally give DeFi users a fully decentralized exchange that has the experience they've come to expect from CeFi (e.g. centralized exchanges).

7 Contracts

Serum offers the ability for users to trade custom cryptocurrency contracts. These allow users to put on leveraged positions in any products that Serum has markets for – including cross-chain physically settled contracts. Further these contracts may be tokenized and can thus be moved across the blockchain.

Serum is intended to allow users to conduct leveraged trading between each other (and not any third party exchange facility) in a fully public, fully decentralized, fully non-custodial system, all with reasonable performance.

8 SerumBTC

As an example of the power of the Serum ecosystem, one could create a truly decentralized, permissionless BTC token on Ethereum and Solana as follows:

- Create a series of contracts for BTC, one to expire each week.
- Each of these, then, would have a token representing a long position–say, BTC-2020-07-22. This can be used as an ERC20 or Solana token that on July 22nd will turn into 1 BTC–but the expiration makes it not ideal for e.g. Uniswap.
- Another token, SerumBTC, is created. SerumBTC holds 1 BTC-2020-07-22 in a smart contract with creations/redemptions. Each week, SerumBTC automatically rolls its holdings from that week's BTC future to the next. Thus SerumBTC never expires, and can be redeemed for an ERC20 or Solana token that itself soon expires into BTC.

9 SerumUSD

Another potential project on Serum is SerumUSD, a model for a diversified stablecoin in Serum. SerumUSD could work as follows:

- A series of markets could be created for SerumUSD_BASK, one to settle each week.
- Each of these, then, would have a token representing the stablecoin product–say, SerumUSD-2020-07-22. This can be used as an ERC20 or Solana token that on July 22nd would turn into 1 SerumUSD_BASK–but that makes it not ideal for e.g. Uniswap.
- Another token, SerumUSD, would be created. SerumUSD wraps 1 SerumUSD-2020-07-22 in a smart contract with creations/conversions. Each week, SerumUSD programmatically moves its holdings from that week's SerumUSD_BASK future to the next. Thus SerumUSD is a persistent token, and could be redeemed for an ERC20 token that itself settles into SerumUSD_BASK.

So what is SerumUSD_BASK? And how does it solve the fundamental problem of DeFi stablecoins–that proof and sending of USD is centralized?

It can't fully solve it. But it can do better than just averaging a basket of stablecoins–it takes the median of one.

Say that Alice buys 1 SerumUSD_BASK from Bob. This settles as follows:

- SerumUSD_BASK has a basket of specified stablecoins. Say that's USDC, TUSD, PAX, USDT, DAI, mUSD, and sUSD.
- Alice specifies 4 of these stablecoins that she would be willing to accept.
- Of those 4, Bob chooses 1 and sends it.

So this contract settles to the median of the 7 coins–at least in as far as, for both Alice and Bob, it's in the top half.

This means that any one of the seven failing won't drop the price of SerumUSD by 14%–in fact it won't drop it at all, because the majority are still worth $1.

These two examples are just general models that users could use to build powerful products on Serum. The ecosystem's speed, flexibility, and stability allow for users to build a broad array of tokens and procedures.

10 About Us

Project Serum is built by the Serum Foundation. We are a group of experts in cryptocurrencies, trading, and decentralized finance.

While we have built the Serum protocol, it is permissionless–we do not hold special power anymore. It is up to you, the crypto community, to use it as you will.