

# Serum - White paper

Serum Foundation

Июль 2020



<b>1 ВВЕДЕНИЕ</b>	<b>3</b>
Скорость и удобство использования	3
Централизация	3
Стейблкоины	3
Книга ордеров	3
Кросс-цепная поддержка	4
<b>Project Serum</b>	<b>4</b>
SRM	5
<b>Кросс-цепные свопы</b>	<b>6</b>
<b>Книга ордеров</b>	<b>7</b>
<b>Solana</b>	<b>8</b>
<b>Контракты</b>	<b>8</b>
<b>SerumBTC</b>	<b>8</b>
<b>SerumUSD</b>	<b>9</b>
<b>О нас</b>	<b>10</b>

# 1 ВВЕДЕНИЕ

Текущее лето посвящено DeFi-проектам. Мы видели запуск и рост сотен проектов в пространстве, которое в совокупности создало более мощную сеть децентрализованных финансов; чистые, интуитивно понятные интерфейсы и увеличение средств на депозитах. Также мы увидели введение ряда новых оригинальных проектов.

Но новые и хорошо продуманные – две большие разницы, и многие ключевые недостатки DeFi остаются нерешенными.

## 1.1 Скорость и удобство использования

Помимо всего прочего, DeFi-продукты медленные и дорогие. Проведение торговой сделки обходится в несколько долларов, а для её завершения иногда нужно несколько минут. Это хорошо в некоторых случаях, но многие клиенты предпочитают быстрое и дешёвое исполнение на централизованных биржах. Тяжело смотреть на свой кошелек Metamask в ожидании подтверждения сделки без использования централизованных бирж.

## 1.2 Централизация

Если Вы отследите весь процесс, то очевидно, что большинство протоколов DeFi приходят к централизованному оракулу ~ часто это самый критичный момент.

Иногда это оракулом ликвидационной цены, указывающий на API централизованной биржи. В других случаях это совет держателей токенов. Иногда это команда самого протокола.

Есть еще одна проблема: слишком многие децентрализованные протоколы требуют больших вычислительных ресурсов. Встраивание их в блокчейн ETH экономичным и быстрым способом в значительной степени не имеет места.

Это не значит, что централизация всегда плоха! USDT, USDC и подобные токены - отличные проекты, которые произвели революцию во всей криптоиндустрии. Они обеспечивают большую часть объема, и если Вам нужно что-то, что можно сконвертировать в доллар 24/7, это единственный способ и, вероятно, всегда так будет. Потому как фундаментальные долларовые купюры не в блокчейне, а на банковских счетах.

Но если вам нужен чистый DeFi, вариантов немного, среди них:

## 1.3 Стейблкоины

Банки не включены в блокчейн, как и физические долларовые банкноты. Итак, как Вы построите стабильную монету, которая всегда равна доллару, но также не полагается на банковский счет?

## 1.4 Книга ордеров

Uniswap незаметно произвел революцию в DeFi, позволив торговать без книги ордеров.

Но самое важное то, что необходим автоматизированный маркет-мейкинг. АММ является системой, в котором нет лимитных ордеров или офферов; в книге ордеров Вы можете определить цену, размер и направление, в котором хотите торговать. У АММ есть много недостатков. Вы не можете обеспечить ликвидность, если не предоставите ее на обе стороны; Вы не можете выбрать только конкретную цену; Вы не можете предоставить цену, отличающуюся от текущей рыночной цены; и Вы не можете выбрать объем средств для предоставления на рынок, без подкрепления его большей суммой.

Этому есть решение, что и делает остальная часть финансов. Но у DeFi нет книг ордеров, по большому счету, потому что сеть ETH слишком медленная и дорогая для их поддержки. Согласование заявок и предложений друг с другом включает в себя множество операций.

## 1.5 Кросс-цепная поддержка

Было сделано много попыток перекрестной поддержки. WBTC, вероятно, самая известная обертка BTC токеном ERC-20; Thorchain строит целый протокол, который позволяет обеспечить полную быструю перекрёстную поддержку между сетями.

Есть много способов осуществить это. Однако одна из общих черт всех нынешних решений - оракул, или группа держателей токенов, или какое-то другое место, где решение принимают люди, которые должны быть честными. Потому что, по сути, BTC не входит в Ethereum, так как же смарт-контракт может знать или влиять на его переводы?

Познакомьтесь, Project Serum.

Serum не идеален; как ничто не идеально. Есть фундаментальные компромиссы между скоростью и децентрализацией; между изысканностью и простотой использования.

Но Serum отличается от других, и в этом его сила. Его программное обеспечение позволяет осуществлять быстрые DEX-трейды; он имеет кросс-блокчейн поддержку, стейблкоины, монеты-обёртки (wgar), книги ордеров и возможность создавать собственные и новые финансовые продукты; и, имея всё это, *он полностью децентрализован*. Там нет оракулов с централизованными ценовыми каналами; никаких трибуналов, на честность которых Вы полагаетесь. Serum - чистый DeFi. В отличие от текущих DeFi-продуктов, он быстрый и дешёвый.

## 2 Project Serum

Project Serum представит полнофункциональную децентрализованную биржу с надежной кросс-цепной торговлей, со скоростью и ценой, которую хотят клиенты. И несмотря на то, что он построен на Solana, он будет совместим с Ethereum.

Serum включает в себя 7 основных составляющих:

- SRM - является токеном экосистемы Serum
  - SRM будет полностью интегрирован в Serum, а также будет получать выгоду от покупки / сжигания комиссий
- Кросс-цепные свопы: доверительный обмен активами между блокчейнами
  - Это важное отличие от большинства современных протоколов, которые полагаются на доверенные стороны при управлении свопом
- Книга ордеров: децентрализованная автоматизированная книга для лимит-ордеров
  - Это даст трейдерам полный контроль над своими ордерами, в отличие от автоматизированного маркет-мейкинга.
  - б) Книга ордеров и сделки полностью автоматизированы непосредственно на блокчейне и ордера устанавливаются конечными пользователями Serum
- Полная интеграция Ethereum и Solana
  - Это сделает Serum быстрой и эффективной – всё это при совместимости с экосистемой Ethereum и токенами ERC-20.
- Физически урегулированные кросс-цепные контракты
  - Это позволит легко осуществлять маржинальную торговлю в DeFi по синтетическим активам
- SerumBTC: модель для создания токенов BTC на ERC-20 или Solana
  - не требующий доверия токен BTC
- SerumUSD: модель для создания децентрализованного стейблкоина
  - Это будет децентрализованный стейблкоин, который не имеет единой точки

отказа

## 3 SRM

Ожидается, что SRM будет иметь следующее назначение:

- Все чистые сборы Serum идут на сжигание SRM
- Владение SRM дает скидку до 50% от всех сборов на Serum
  - Владение 1 MСРМ дает 60% скидку на сборы
- Сборы могут быть оплачены в SRM
- SRM и MSRM будут доступны на Serum
- SRM можно застейкать на ноду.
  - Каждый узел должен иметь не менее 10 000 000 SRM и из них как минимум один MSRM. Ожидается, что узлы будут играть следующую роль: каждый узел может быть вызван для обеспечения страхования транзакции между блокчейнами. Они получают часть комиссионных за любую транзакцию, в которой они таким образом участвуют. Такое обеспечение может быть подвержено определенным базовым рискам.
  - Будет создан фонд из SRM, которые будут распределяться как вознаграждения за стейкинг для каждого узла.

- У каждого узла есть лидер - тот, кто его создал. Часть всех наград за этот узел будет отдана лидеру.
- Узлы выполняют важные обязанности по оптимизации производительности и пропускной способности экосистемы Serum. Могут быть назначены награды или штрафы в зависимости от их результатов.
- Предполагается, что Serum будет включать ограниченную модель управления, основанную на токене SRM. Хотя большая часть экосистемы Serum будет неизменной, некоторые параметры без значительных рисков для безопасности (например, будущие сборы) могут быть изменены путем голосования токенами SRM.

Распределение SRM прогнозируется следующим образом:

- 20%: Команда и советники
- 23%: Участники проекта
- 3%: Заблокированные токены участников seed и аукционного раундов
- 27%: Фонд Партнеров и Сотрудников
- 27%: Фонд по развитию экосистемы

Некоторые из партнеров в экосистеме откладывают часть своего SRM для перераспределения среди владельцев своих собственных токенов или иным образом стимулируют распространение SRM. Ожидается, что это будет не менее 5% от общего объема поставок с течением времени.

Serum изначально функционирует на блокчейне Solana и доступен на блокчейне Ethereum (как токен ERC-20).

Циркулирующее предложение при запуске составит примерно 10% и увеличится примерно на 15% за год.

Все токены предпродажной подготовки, команды и участников будут разблокированы через 1 – 7 лет после листинга.

Всего выпущено 10,000,000,000 токенов SRM; больше эмиссии не будет.

Вышеуказанные суммы соответствуют ожидаемым и могут быть изменены.

## 4 Кросс-цепные свопы

Стандартная проблема в кросс-цепных DeFi: если у Алисы 10 ETH, а у Боба 1 BTC, как они обменивают их, не имея возможности украсть чужие деньги? Кто отправляет первым?

Большинство других протоколов выполняют различные вариации следующих шагов:

1. Алиса отправляет свой ETH на смарт-контракт
2. Боб отправляет BTC на мульти-сиг кошелёк
3. Некоторый набор нод, которые контролируют ключи от этих кошельков, отправляют BTC Алисе и ETH для Боба.

4. Определённая группа арбитров наблюдает за процессом. Они решают, была ли операция проведена как предназначалось; если нет, они наказывают ноды.

Есть много преимуществ для этого. Одним из недостатков является то, что протокол полагается на честность арбитров.

Но не Serum.

Вот как работает Serum:

1. Алиса отправляет свой ETH на смартконтракт (СК)
2. Алиса и Боб каждый посылают некоторое количество ETH в залог на СК
3. Боб должен отправить BTC Алисе
4. Если он это делает, то СК отправляет ETH Бобу и возвращает залог; все хорошо
5. Если он не делает, Алиса оспаривает сделку
6. Алиса и Боб отправляют историю блокчейна BTC в СК
7. СК решает, кто прав
8. Если права Алиса, СК возвращает ей ETH, её залог, а также часть залога Боба для компенсации неудобств.
9. Если прав Боб, СК отправляет ETH Алисы Бобу, часть ее залога для компенсации неудобств и возвращает Бобу его залог.

Это гарантирует следующие основные свойства:

- a) Если Алиса права и честна, СК решит ситуацию в ее пользу
- b) Если Боб прав и честен, СК решит ситуацию в его пользу
- c) Урегулирование не является чрезмерно дорогим или долгим
- d) Эффективное поведение поощряется, и люди получают компенсацию, если другие действуют злонамеренно

A и B верны, потому что, хоть блокчейн ETH не может прочитать или изменить сам блокчейн BTC, но он может его проверить. СК запрограммирован на анализ, является ли предложенная блок-схема BTC действительной; затем он может проверить, кто из пары Алисы и Боба отправит более длинный действительный блокчейн, и согласится в их пользу.

C - правда: процесс спора длительный, но не слишком; это займет примерно 100 долларов за газ.

D также верно: из-за наличия залога, Алиса проигрывает, если она нечестна, как и Боб, если он неправ; поэтому у Боба есть стимул отправить BTC, а у Алисы - не оспаривать его, если Боб это сделает. Это означает, что в подавляющем большинстве случаев посредничество не будет использоваться, и поэтому протокол будет быстрым и дешевым.

Этот протокол обобщает любую транзакцию, в которой целевой блокчейн (в данном случае BTC) это Proof of Work, и базовый протокол (ETH, в данном случае) намного быстрее, чем целевой блокчейн.

Кроме того, когда целевой блокчейн поддерживает смарт-контракты, модифицированная версия, подобная optimistic rollups может позволить размещать токенизированные активы: целевой блокчейн также может имитировать хэш блокчейна Solana, позволяя обеспечить полную кросс-цепную связь и, следовательно, вызывать функции создания и выкупа в смарт-контракте.

Это важный аспект Serum: несмотря на то, что он находится на Solana и обладает высокой скоростью и экономической эффективностью, он будет полностью применим к Ethereum. Это означает, что существующие проекты DeFi могут получить доступ к функциям и ликвидности Serum непосредственно из их собственных блокчейнов, создавая бесшовную интеграцию между текущей инфраструктурой и Serum.

## 5 Книга ордеров

Автоматизированные лимит-ордера непосредственно на блокчейне Serum позволяют пользователям отправлять ордера с указаниями, ценами и объемами, предоставляя им контроль над своей торговлей. Serum реализует книги ордеров между токенами; и благодаря своей кросс-цепной поддержке он также имеет книги ордеров ETH и BTC. Эти книги ордеров не контролируются централизованно, они полностью запрограммированы и автоматически сопоставляют ордера сторонних пользователей.

Книги ордеров являются одними из наиболее ресурсоемких продуктов в DeFi. Протокол Serum включает в себя большое количество оптимизаций для механизма сопоставления, чтобы сделать сопоставление заказов быстрее и дешевле.

Эти книги ордеров затем служат основным источником цен для Serum. С каждой сделки взимается комиссия. Все чистые сборы идут на покупку / сжигание SRM. Кроме того, владение SRM снижает Ваши сборы.

## 6 Solana

Solana — это блокчейн со значительно более высокой скоростью и более низкими затратами, чем более старые блокчейны. Он имеет несколько циклов расчета в секунду и стоит меньше копейки, чтобы отправить сообщение - это на два порядка выше существующих стандартов.

Основанный на Solana, Serum DEX будет иметь скорость, стоимость и UX, которые пользователи ожидают от централизованной биржи - и всё это при отсутствии необходимости доверия и внешнего хранилища. А благодаря полной кросс-цепной интеграции пользователи Serum смогут торговать на нём BTC, ETH, ERC-20, Solana и другими токенами.

Это, наконец, даст пользователям DeFi полностью децентрализованную биржу, имеющую опыт, которого они ожидают от CeFi (например, централизованные биржи).



## 7 Контракты

Serum предлагает пользователям возможность торговать индивидуальными контрактами на криптовалюту. Это позволяет пользователям размещать позиции с использованием заемных средств в любых продуктах, для которых у Serum есть рынки, включая кросс-цепные физически урегулированные контракты. Кроме того, эти контракты могут быть токенизированы и, таким образом, могут быть перемещены через блокчейн.

Serum предназначен для того, чтобы пользователи могли осуществлять торговлю с использованием кредитного плеча друг с другом (а не с любым сторонним обменным сервисом) в полностью публичной, полностью децентрализованной, полностью свободной системе, и всё это с разумной эффективностью.

## 8 SerumBTC

Как пример преимуществ экосистемы Serum, проект позволяет создать по-настоящему децентрализованный токен BTC на Ethereum или Solana следующим образом:

1. Создайте серию контрактов для BTC, срок действия которых истекает каждую неделю.
2. У каждого из них будет токен, представляющий длинную позицию, скажем, BTC-2020-07-22. Его можно использовать как токен ERC-20 или Solana, который 22 июля превратится в 1 BTC, но истечение срока действия делает его не идеальным, например, для Uniswap.
3. Создается еще один токен, SerumBTC. SerumBTC держит 1 BTC-2020-07-22 в смарт-контракте с функциями создания/выкупа. Каждую неделю SerumBTC автоматически переводит свои средства с фьючерса BTC этой недели на следующую. Таким образом, срок действия SerumBTC никогда не истекает, и его можно обменять на токен ERC-20 или Solana, который вскоре истечет и конвертируется в BTC.

## 9 SerumUSD

Еще один потенциальный проект для Serum - это SerumUSD, модель диверсифицированного стейблкоина в Serum.

SerumUSD может работать следующим образом:

1. Для SerumUSD\_BASK может быть создан ряд рынков, по одному на каждую неделю.
2. Тогда у каждого из них будет токен, представляющий продукт стейблкоина, скажем, SerumUSD-2020-07-22. Его можно использовать в качестве токена ERC-20 или Solana, который 22 июля превратится в 1 SerumUSD\_BASK - но это делает его не идеальным, например, для Uniswap.
3. Создается ещё один токен, SerumUSD. SerumUSD оборачивает 1 SerumUSD-2020-07-22 в смарт-контракт с функцией создания/конверсии. Каждую неделю SerumUSD программно

перемещает свои активы из фьючерса SerumUSD\_BASK этой недели на следующую. Таким образом, SerumUSD является постоянным токеном, и его можно использовать для выкупа токена ERC-20, который конвертируется в SerumUSD\_BASK.

Так что же такое SerumUSD\_BASK? И как это решает фундаментальную проблему стабильных монет DeFi - что проверка и отправка долларов централизована?

Эту задачу не выйдет *полностью* решить. Но может быть лучше, чем просто усреднение корзины стабильных монет - возьмем *медиану* монеты.

Предположим, что Алиса покупает 1 SerumUSD\_BASK у Боба. Это происходит следующим образом:

- SerumUSD\_BASK имеет корзину указанных стейблконов. Допустим, это USDC, TUSD, PAX, USDT, DAI, mUSD и sUSD.
- Алиса указывает 4 из этих стейблкоинов, которые она готова принять.
- Из этих 4 Боб выбирает 1 и отправляет его.

Таким образом, этот контракт рассчитывается по медиане из 7 монет - по крайней мере в той степени, в которой для Алисы и Боба он находится в верхней половине.

Это означает, что падение любой из семи монет не снизит цену SerumUSD на 14 % - фактически, она вообще не упадет, потому что большинство монет всё ещё стоит 1 доллар.

Эти два примера являются просто общими моделями, которые пользователи могут использовать для создания мощных продуктов на Serum. Скорость, гибкость и стабильность экосистемы позволяют пользователям создавать широкий спектр токенов и процессов.

## 10 О нас

Serum Project создан Serum Foundation. Мы являемся группой экспертов в области криптовалют, торговли и децентрализованного финансирования.

Несмотря на то, что мы создали протокол Serum, он не доступен нам - мы больше не обладаем особой силой в его управлении. Вам, криптосообществу, решать, как использовать его по своему усмотрению.