PROJECT SERUM

- Serum 白皮书 -

Version 1

2020.07.25

此中文白皮书为英文版本译本，请以英文版本为准。此中文版白皮书后附英文版白皮书。

目录

1. 简介 3

1.1. 速度与实用性 3
1.2. 中心化 3
1.3. 稳定币 4
1.4. 订单簿 4
1.5. 跨链支持 4

2. PROJECT SERUM 5

2.1. SRM 通证 5
2.2. 跨链协议（CROSS-CHAIN SWAPS） 7
2.3. 订单簿（ORDER BOOK） 8
2.4. SOLANA 9
2.5. 合约（CONTRACTS） 9
2.6. SERUMBTC 9
2.7. SERUMUSD 10

3. 关于我们 11

1. INTRODUCTION 12

1.1. SPEED AND USABILITY 12
1.2. CENTRALIZATION 12
1.3. STABLECOINS 13
1.4. ORDERBOOKS 13
1.5. CROSS-CHAIN SUPPORT 13

2. PROJECT SERUM 14

2.1. SRM 14
2.2. CROSS-CHAIN SWAPS 16
2.3. ORDER BOOK 18
2.4. SOLANA 18
2.5. CONTRACTS 18
2.6. SERUMBTC 19
2.7. SERUMUSD 19

3. ABOUT US 20

1. 简介

这是一个属于 DeFi 的夏天——我们见证了数以百计的 DeFi 项目的出现以及发展，它们共同创建了一个更加强大的 DeFi 生态网，干净直观的交互页面，以及爆炸性的锁仓增长。同时我们也看到不少新颖的项目。

但是新颖和优异设计还是有本质区别的，大多 DeFi 底层的问题依然存在。

1.1. 速度与实用性

说到底，DeFi 处理速度非常缓慢同时也十分昂贵。完成一笔交易需要耗时几分钟，用户还得支付几美元费用。在某些场景，速度慢和高花费还可以忍受，但大多数用户一定更喜欢效率更高，并且手续费更低的中心化交易所。花几分钟去盯着你的 Metamask 钱包等待交易到账对很多人来说是一种折磨，而这个时候你会忍不住怀念起那些中心化的交易所。

1.2. 中心化

如果你要拍刨根究底去深挖的话，你会发现大多数 DeFi 协议在最关键的一步上用的却是一个中心化的预言机。

目前，一些 DeFi 协议遭遇中心化污染的关键步骤：可能是一个从中心化交易所 API 获取清算价格的预言机；或者可能是持币人组成的治理会；又或者可能是协议创始团队本身。

而更严重的一个问题则是大多数去中心化协议是计算密集型协议。而现在没人能找到一种把去中心化协议放在以太链上高效并且便宜的运行方式。

以上并不是要去说中心化总是不好的！USDT、USDC 和其他类似的项目都是数字货币行业革命性的产品。它们构成了区块链上大部分的交易量，如果你想要一个 24/7 能够转变成美元的产品，那他们可能是唯一的选择。因为本质上美元是不可能在区块链上的，它们永远只能在银行账户里。

如果你想要的是纯 DeFi，那么你的选择基本上是绝无仅有。

1.3. 稳定币

银行并没有在区块链上，同样美元现金也没有。那要如何创造一个永远与一美元等值的稳定币，同时又不需要依赖于银行的管控呢？

1.4. 订单簿

Uniswap 给 DeFi 带来了革命性的改变：交易无需订单簿。

更具里程碑意义的是自动化做市（AMM）必要性充分体现出来了。但同时，自动化做市也存在很多问题：你必须要给双边同时提供流动性；你不能给某个特定价格提供流动性；除了当前市价以外，你不能以其他价格去提供流动性；你没有办法根据自己的意愿去决定报价数量，实际提供的数量总是比计划的更多。

其实以上问题都是有解决办法的，其他金融行业也都是这么解决的——订单簿。但是 DeFi 没有订单簿，大部分原因是 ETH 网络太慢又太过昂贵。然而撮合买单和卖单确实需要大量的运算。

1.5. 跨链支持

已经有很多项目尝试过支持跨链。WBTC 可能是这些项目中最知名的，它创建了一个打包成 ERC20 通证的比特币；Thorchain 也正在建立一个完整的，快速的跨链支持协议。

同样，针对跨链支持也有不同的解决方法。大多数现存的解决办法都依赖同一个东西：预言机，或是一众持币者，或者是一帮大家相信会诚实并作出正确决定的人。本质上比特币并没有在以太坊上，所以一个智能合约应该如何知晓或者影响某一笔转账呢？

来到 Project Serum 的世界吧。

世上没有任何东西是完美的，Serum 也绝非完美。便捷高效与去中心化，精妙设计与普世易用之间的抉择，本身就是一个难题。

Serum 不一样的是它强大的兼容性。Serum 是一个运行起来非常快速的 DEX；它支持跨链，稳定币，打包通证，订单簿，以及期货交易；同时，它还做到了完全去中心化。Serum 里面不存在通过 API 从中心化交易所获取价格的预言机；它也不需要一个诚信的委员会。Serum 是一个纯正的 DeFi。不像现存的一些 DeFi 项目，Serum 高效、便捷、功能丰富、成本低。

2. Project Serum

Project Serum 将会是一个功能强大，并且完全去中心化的衍生品交易所。它能够进行完全去中心化的跨链交易，并非常高效准确地给用户提供可执行交易的价格。它是基于 Solana 搭建，同时之后也会与以太坊整合。Serum 的七大元素：

1. SRM：Serum 生态系统的功能型通证
    a) SRM 将会完全与 Serum 整合，同时从手续费回购/销毁中获益
2. 跨链协议：完全无需第三方信任监督的跨链资产交易
    a) 目前大部分跨链协议需要依靠可信的第三方来协助交易，但 Serum 不需要
3. 订单簿：完全去中心化的中央委托系统
    a) 与现有的自动化做市系统不同，Serum 中，交易员将完全能够掌控他们的委托
    b) 订单簿和撮合完全由用户掌握
2. 完整地整合以太坊链和 Solana 链
    a) 通过 Solana 链赋能，Serum 可以兼顾高效与低成本，同时整合以太坊链及 ERC20 代币
4. 期货：以实物交割的跨链合约
    a) 能够让用户轻松地在 DeFi 中进行合成资产的杠杆交易
5. SerumBTC：一种创建 ERC20 版本或者 Solana 版本 BTC 代币的方式
    a) 这种方式将能够创造处完全无需信任的 BTC 代币
6. SerumUSD：一种去中心话的稳定币
    a) 一个去中心化的不会出现单点故障的稳定币

2.1. SRM 通证

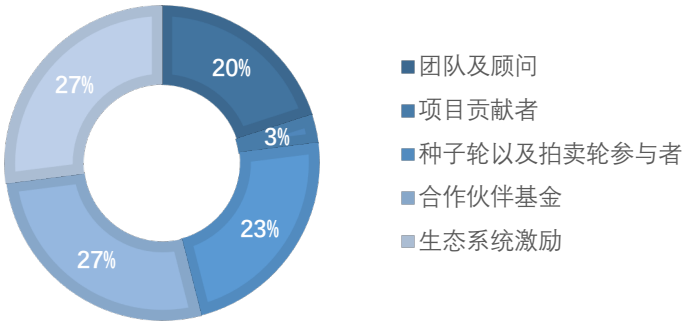
SRM 通证预计会有以下功能：

1. 所有的净手续费会用来每周回购/销毁 SRM
2. 持有 SRM 最高可以得到 Serum 生态系统 50%的手续费折扣
    a) 持有 MSRM 最高可以得到 Serum 生态系统 60%的手续费折扣
3. 有可能可以用 SRM 支付手续费
4. 用户可以在 Serum 上交易 SRM 和 MSRM
5. SRM 可以在节点上参与 Staking。每个节点至少需要 10,000,000 个 SRM，并至少需要一个 MSRM。每个节点将要扮演以下角色：

a) 每个节点会负责为跨链交易或者合约交易提供保险。每个节点会在为该交易提供完保险后获取该交易的一部分交易手续费。该保证金是可能有违约风险的。
b) 届时，SRM 基金将会设立，用于 Staking 的节点奖励发放。
c) 每个节点都会有一个领袖，也就是创立节点的那个人。有一部分的奖励会被分发给那个节点领袖。
d) 节点在 Serum 生态系统中将扮演重要角色以优化整体性能以及吞吐量。奖赏以及惩罚将根据每个节点的执行能力决定

6. Serum 预计会有小范围的基于 SRM 的治理计划。大部分 Serum 生态系统将不受此影响，但某些成分（比如费率）可能会收到 SRM 的治理投票更改。

SRM 分布如下：



作为激励，Serum 生态合作伙伴会把自己持有的部分 SRM，分发给持有他们自己原生通证的用户——这部分应用场景的 SRM，预计至少会占比 SRM 总发行量的 5%。

首发阶段，Serum 生态会以 Solana 链为底层技术支持，后续会以 ERC20 代币的形式整合在以太坊链上。

上线初期预计流通量大约为 10%，并会每年增长 15%的流通量。

所有的预售，团队，以及设计人员持有的代币都将在上线后 1 至 7 年内解锁。

SRM 总量为 10,000,000,000 ；未来也不会增发。

上述提及的数字均为白皮书成文时的预计数字，后续可能会有调整。

2.2. 跨链协议（Cross-Chain Swaps）

在跨链 DeFi 中通常都会遇到一个问题：如果小红有 10 个 ETH，小明有 1 个 BTC，两人如何互换资产，并且保证任何一方都没有可能盗取对方的资产？谁该先打币？

大多数预言机的做法和流程如下：

1. 小红把她的 ETH 打到智能合约上
2. 小明发送 BTC 到多层签名的钱包中
3. 一些控制这些钱包的节点将 BTC 打给小红，将 ETH 打给小明
4. 一些仲裁人在中间决定这个转换的过程是否合规，如果不合规，需要惩罚节点

这个方法有点很多，但有一个弊端是整个交易过程，极度依赖仲裁人自身是诚实守信的。

Serum 则完全无需依赖第三方的守信。

Serum 的运作机制：

1. 小红把她的 ETH 发送到一个智能合约
2. 小红和小明分别将一些 ETH 作为保证金打到智能合约里
3. 小明这时候要打 BTC 给小红
4. 如果小明打了 BTC，那智能合约会把小红的 ETH 自动打给小明，并退还小明的保证金；
5. 如果小明不打币，小红可以申诉
6. 小红和小明同时将 BTC 链上记录发送到智能合约中
7. 智能合约自动进行裁决
8. 如果小红申诉成功，智能合约将自动退回她的 ETH，她的 ETH 保证金，并将一部分小明的保证金分配给小红作为补偿
9. 如果小明正确，智能合约会把小红的 ETH 打给小明，并退回小明的保证金。小红的一部分 ETH 保证金也将作为补偿打给小明。

这种跨链协议保证了以下几个核心点：

a. 如果小红诚实且申诉正确，智能合约的裁决会对她有利
b. 如果小明正确且诚恳，智能合约的裁决会对他有利
c. 清算的成本不会过高，过程不需要等待过久
d. 机制本身鼓励高效行为，并且奖赏没有违约的一方

A 和 B 都是正确的：虽然以太坊自身无法直接读取或修改比特币链上信息，却可以验证该信息。智能合约编译后可以直接校验提案中比特币区块信息；可以检验是小红还是小明发送了更长的有效区块，并按照诚实那方提供的信息进行结算。

C 是正确的：申诉的过程比较长但不会长到无法执行，它大约会花费 100 美金的矿工费。

D 也是正确的：如果小红不诚实，那么她将失去保证金，同样如果小明不诚实他也将失去保证金。这样小明便有动力和信心先存入 BTC，小明存入 BTC 后，小红也就不会随便提起申诉。这意味着，大多数时间，仲裁流程都将无用武之地，自然整个协议效率将得到提升，成本也会降低。

Serum 预言机可以用于任何 POW 机制的目标区块链（例如上述中的 BTC 链）的跨链交换，且要求基础协议区块链（例如上述中的以太坊链）比目标区块链更快。

此外，如果目标区块链支持智能合约，一个类似于 Optimistic Rollups 的改进版本将允许锁定的通证跨链交换：目标区块链也可以模拟 Solana 区块链的哈希，这样一来就可以完全实现跨链沟通、创建/销毁智能合约。

这会让资产在 BTC 链, ERC20，和 Solana 链之间无缝划转，使得目前市面上的 DeFi 生态系统更加便捷高效地接入 Solana 链。

这是 Serum 非常重要的一个组成部分：尽管 Solana 链在速度和性价比上更有优势，DeFi 系统依旧可以在以太坊链上运行。这意味着现存的 DeFi 项目可以从他们当前运行的区块链上，直接接入 Serum 的功能和流动性，在其现有架构下与 Serum 间建立无缝衔接。

2.3. 订单簿（Order Book）

我们的中央订单簿允许用户提交不同交易方向，价格，数量的订单，让用户可以完全控制自己的订单。因为支持跨链，Serum 有不同币种的订单簿，包括 ETH 和 BTC 的订单簿。这些订单簿并不是中心化控制的，而是是全自动化、程序化地撮合第三方用户发出的订单。

订单簿本身在 DeFi 中消耗了比较多的计算资源。我们在搓单系统中加入了非常多的优化来确保订单撮合的效率、降低订单撮合的成本。

这些订单簿之后会成为 Serum 核心定价的根据。每一笔交易都将产生手续费。所有净交易手续费将回购/销毁 SRM。同时持有 SRM 将降低交易手续费。

2.4. Solana

Solana 是一个从速度和效率上完胜现有区块链的区块链协议。它有每秒多次结算的能力，能以低于一分钱的价格进行每次记账。效率上完胜现有任何协议标准。

基于 Solana 开发的 Serum DEX 分布式交易所，在保持无需信任第三方监管情况下，在速度，价格和用户交互上能完全与传统中心化交易所媲美。基于 Serum 整合性的跨链支持，用户可以在 Serum 上交易各式币种，包括 BTC、ETH、ERC20 代币、SOL 和更多其他代币。

在保证完全去中心化的前提下，Serum Dex 同时能给用户提供媲美中心化交易所的用户体验。

2.5. 合约（Contracts）

Serum 能提供在未来特定时间交割的数字资产合约。用户可以加杠杆，交易任何 Serum 上的交易对，包括需要跨链实物交割的合约产品。此外，这些合约产品可以被通证化，进而可以在跨链上。

Serum 旨在建立一个让用户直接与对手盘进行杠杆交易的(不需要经过中心化交易所），完全公开透明，完全去中心化，完全无托管系统，且性能优异的去中心化交易系统。

2.6. SerumBTC

运用 Serum 生态系统的强大能力，我们可以在以太坊区块链以及 Solana 区块链上建立完全去中心化，无需验证的比特币通证：

1. 创建一系列，以比特币为标的资产的期货合约，每周到期一个。
2. 然后每个期货合约会有一个对应的多头仓位的代币，比如合约代码为 BTC-2020-07-22——这个仓位可以币化为一个 ERC20 代币或者 Solana 代币，在 2020 年 7 月 22 日这天到期，以 1BTC 进行实物交割。但是在类似于 Uniswap 上却没有期货现货交割的可能性。
3. 另一个通证 SerumBTC 会被创造。SerumBTC 在智能合约上持有 1 个 BTC-2020-07-22 并支持申购/赎回。每周 SerumBTC 转仓持有仓位到下一周的比特币期货上。因此 SerumBTC 不会过期，并且可以赎回成 ERC20 上或 Solana 通证，并到期交割变成一个比特币现货。

2.7. SerumUSD

另一个有可能在 Serum 上的项目会是 SerumUSD，一个基于合约的 Serum 生态系统中的稳定币。SerumUSD 的运作机制如下：

1. 每周一系列期货仓位会创立并添加到 SerumUSD_BASK 中，每周到期一个。
2. 然后每个期货合约会有一个对应的多头仓位的代币，比如合约代码为 SerumUSD-2020-07-22——这个仓位可以币化为一个 ERC20 代币或者 Solana 代币，在 2020 年 7 月 22 日这天到期，以 1 SerumUSD_BASK 进行实物交割。但此类交割在类似于 Uniswap 上比较难以实现。
3. 另外一个通证 SerumUSD 会被创造。SerumUSD 在智能合约上持有一个 SerumUSD-2020-07-22 并支持申购/赎回。每周 SerumUSD 转仓持有仓位从当周 SerumUSD_BASK 期货到下周期货。因此 SerumUSD 不会过期。

所以 SerumUSD_BASK 是什么？它将如何从根本上解决 DeFi 稳定币的 USD 申购赎回的中心化问题？

虽然它并不能完美解决所有问题，它比一般的一篮子稳定币表现要更好。它不取稳定币篮子的平均值，而选取稳定币篮子的中位数。

比如小红从小明那里买了 1 个 SerumUSD_BASK。结算的步骤如下：

1. SerumUSD_BASK 由一篮子稳定币组成，其中比如有 USDC, TUSD, PAX, USDT, DAI, mUSD，和 sUSD。
2. 小红可以在上述稳定币中任意选择 4 种她乐意接受的稳定币。
3. 在小红选择的 4 种稳定币中，小明可以任意选择一种打币即可。

那么这个合约将按照 7 中稳定币的中位数进行结算。

如果七个稳定币中任意一个暴雷了，SerumUSD 的价值也不会跌超过 14%。实际上 SerumUSD 的价值并不会下跌，因为大部分的稳定币依旧值 1 美金，所以中位数将保持 1 美金。

以上仅为两个运用 Serum 强大功能就能创立的两种创新产品。Serum 生态系统的速度，灵活性，以及稳定性将允许用户创建一套完整的代币体系。

3. 关于我们

Project Serum 由 Serum Foundation 创立。我们是一群在加密资产，交易，以及去中心化金融等领域的专业人士，已与 Alameda Research Ltd 及其他全球顶级数字资产交易商和 DeFi 领域的专家达成战略合作。

我们创立 Serum 协议之后，它将没有任何权限限制，我们也不会在 Serum 生态系统中拥有任何特殊权利。整个 Serum 生态系统将完全交给用户，交给加密货币社区运行——完全去中心化。

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 futures; 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 derivatives 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:

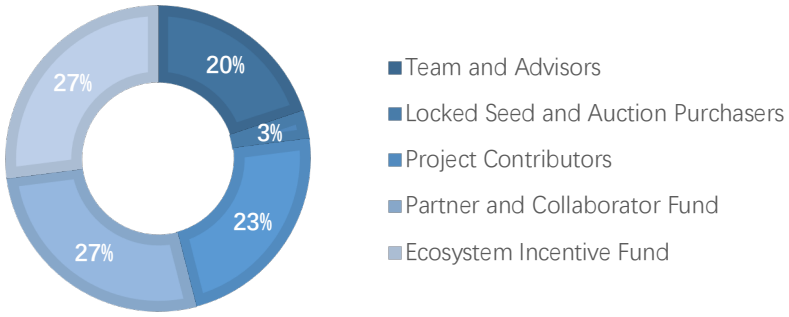
1. SRM: the Serum token is the utility token of the Serum ecosystem
    a) SRM will be fully integrated into Serum, and also benefit from a buy/burn of fees
2. Cross-Chain Swaps: trustlessly exchange assets between chains
    a) This is in contrast to most current protocols that rely on trusted parties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

2.1. SRM

SRM is anticipated to hold the following utility:

1. All of the net fees on Serum go to a SRM buy/burn
2. Holding SRM gives one up to 50% off of all fees on Serum
    a) Holding 1 MSRM gives a 60% discount on fees
3. Fees may be made payable with SRM
4. SRM and MSRM will be made available on Serum
5. 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:
    a) Each node may be called upon to provide insurance for a cross-chain swap or contract. 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.
    b) There will be a fund of SRM that will be distributed as staking rewards to each node.
    c) 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.
    d) Nodes perform important duties to optimize the performance and throughput of the Serum ecosystem. Rewards or penalties can be paid based on their execution.
6. 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.

SRM will be distributed as follows:



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 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 designes 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.

2.2. 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:

1. Alice sends her ETH to a smart contract
2. Bob sends BTC to a multi-sig wallet
3. Some set of nodes who control the keys to those wallets send the BTC to Alice and the ETH to Bob.
4. 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:

1. Alice sends her ETH to a smart contract (SC)
2. Alice and Bob each send some ETH collateral to SC
3. Bob is supposed to send BTC to Alice
4. If he does, then SC sends the ETH to Bob and returns collateral; all is good
5. If he doesn't, Alice disputes
6. Alice and Bob both send the BTC blockchain history to SC
7. SC decides who's right

8. If Alice is right, SC returns her ETH, her collateral, *and* gives her some of Bob's for the hassle
9. 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:

a. If Alice is correct and honest, SC will settle in her favor
b. If Bob is correct and honest, SC will settle in his favor
c. Settlement isn't prohibitively expensive or long
d. 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 swap 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 tonized assets in addition to swaps: 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 us 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.

2.3. Order Book

Our 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. We have implemented 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.

2.4. 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, Solana, and more on it.

This will finally give customers a fully decentralized exchange that has the experience they've come to expect from CeFi.

2.5. Contracts

Serum offers the ability for users to trade cryptocurrency contracts that are settled at specified dates in the future. 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.

2.6. 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:

1. Create a series of contracts for BTC, one to expire each week.
2. 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.
3. 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.

2.7. SerumUSD

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

1. A series of contracts could be created for SerumUSD_BASK, one to expire each week.
2. Each of these, then, would have a token representing a long position--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 the expiration makes it not ideal for e.g. Uniswap.
3. Another token, SerumUSD, would be created. SerumUSD holds 1 SerumUSD -2020-07-22 in a smart contract with creations/redemptions. Each week, SerumUSD rolls its holdings from that week's SerumUSD_BASK future to the next. Thus SerumUSD never expires, and could be redeemed for an ERC20 token that itself soon expires 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:

1. SerumUSD_BASK has a basket of allowed stablecoins. Say that's USDC, TUSD, PAX, USDT, DAI, mUSD, and sUSD.
2. Alice specifies 4 of these stablecoins that she would be willing to accept.
3. 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.

3. About Us

Project Serum is built by the Serum Foundation. We are a group of experts in cryptocurrencies, trading, and decentralized finance collaborating with Alameda Research LTD, one of the industry's top liquidity providers.

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.