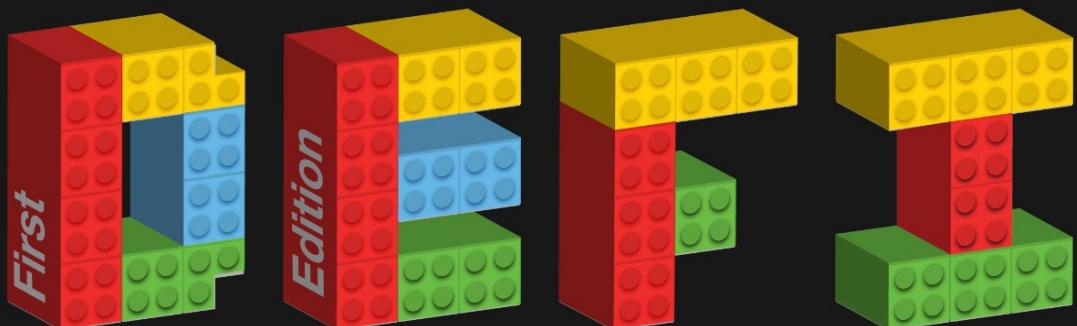
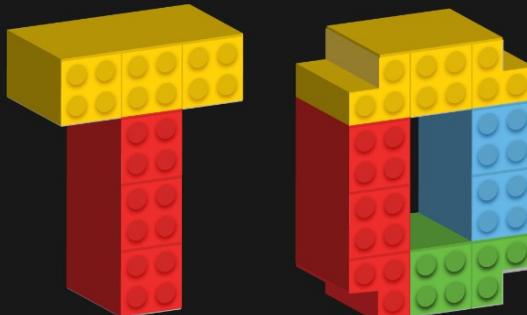
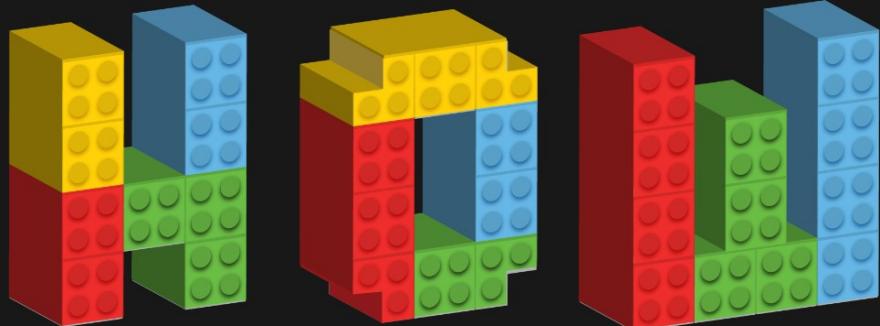


"Probably the most comprehensive DeFi manual out there,
a must-read."

Hugh Karp, Founder of Nexus Mutual



ADVANCED

Decentralized Finance is taking over the world.
Learn how to get started and join the revolution.



CoinGecko

Что такое DeFi: Продвинутый курс

Первая редакция, Май 2021 года

Под авторством:

Lucius Fang, Benjamin Hor, Erina Azmi, Khor Win Win

Переведено энтузиастами с форума cp0x.com



Оригинал

<https://landing.coingecko.com/how-to-defi/>

Авторские права © 2021 CoinGecko

1-е издание, май 2021 года

Макет: Анна Тан

teaspoonpublishing.com.my

Все права защищены. Никакая часть этой публикации не может быть воспроизведена, сохранена в поисковой системе или передана в любой форме или любыми средствами, электронными, механическими, копировальными, записывающими или иными, за исключением кратких выдержек для целей обзора, без предварительного письменного разрешения издателя и владельцев авторских прав. Также рекомендуется проконсультироваться с издателем, если у вас есть какие-либо сомнения относительно законности любого копирования, которое должно быть предпринято.

«Вероятно, это самое полное руководство по DeFi, которое необходимо прочитать».

– Хью Карп, основатель Nexus Mutual

«Образование имеет первостепенное значение в DeFi, и такие ресурсы, как «Что такое DeFi», очень важны. Это не только отличное продолжение, но и еще раз команда CoinGecko смогла предоставить всесторонний и глубокий обзор постоянно меняющегося пространства».

– Ганеш Свами, генеральный директор Covalent

«Это самое полное руководство по DeFi по любому, без исключения. Вы должны прочитать это от корки до корки».

– Лео Ченг, соучредитель CREAM Finance

«Если вы хотите узнать о последних тенденциях в DeFi, эта книга-лучшая из лучших на рынке».

– Янвэнь Фэн, соучредитель Perpetual Protocol

«Эта книга является отличным продолжением их первой книги и обеспечивает более глубокое погружение в DeFi и в то, как ориентироваться в нюансах пространства».

– Джослин Чанг, руководитель отдела развития APAC в основном подразделении MakerDAO по развитию

«Читать «Что такое DeFi» в 2021 году - это все равно, что случайно встретиться с Виталиком Бутериным в кафе в Цуге в 2015 году и открыть для себя Ethereum из первых рук. «Что такое DeFi» поможет вам принимать жизненно важные решения при создании и использовании протоколов и приложений DeFi этого десятилетия».

– Молли Уинтермут, основательница Hegic

«DeFi нелегкодается новичкам, пока. Но с помощью этого лучшего руководства CoinGecko читатели очень быстро поймут, что DeFi – это не просто будущее. DeFi есть сейчас, и скоро он станет неотъемлемой частью повседневной жизни многих людей по всему миру. Это, вероятно, лучший путеводитель прямо сейчас, чтобы осветить путь любому человеку в его путешествии на любом этапе».

– Азим Ахмед, соучредитель Armor

«Эта книга представляет собой экскурс во все важные концепции и платформы, которые вам необходимо знать, чтобы эффективно взаимодействовать с DeFi. Я буду использовать это в качестве ориентира как для себя, так и для новичков в криптопространстве в течение довольно долгого времени».

– Лоуренс Э. Дэй, Основная команда Indexed Finance

«Самое глубокое и актуальное руководство по пониманию DeFi и всех его возможностей»

– DeFi Тед, советник в COVER Protocol

ВВЕДЕНИЕ.....	14
ЧАСТЬ ПЕРВАЯ: СОСТОЯНИЕ DEFI.....	15
ГЛАВА 1. ОБЗОР DEFI	16
Лето DeFi 2020 года.....	16
Экосистема DeFi.....	18
Повышение стоимости газа (Gas – комиссия).....	19
DeFi становится мейнстримом	21
Рекомендуемая литература	22
ГЛАВА 2: ДЕЯТЕЛЬНОСТЬ DEFI.....	23
Фарминг.....	23
Майнинг ликвидности.....	24
Раздачи токенов (Airdrops).....	25
Первоначальное предложение DEX (IDO)	26
Первоначальное предложение по кривой спроса (IBCO – Initial Bonding Curve Offering)	27
Самонастраивающийся пул ликвидности (LBP – Liquidity Bootstrapping Pool).....	27
Первоначальное предложение фарминга (IFO – Initial Farm Offering).....	27
Фарминг: пошаговая инструкция	27
Сопутствующие риски	33
Вывод.....	33
Рекомендуемая литература	34
ЧАСТЬ ВТОРАЯ: ОЦЕНКА СЕКТОРОВ DEFI.....	35
ГЛАВА 3: ДЕЦЕНТРАЛИЗОВАННЫЕ БИРЖИ.....	36
Типы децентрализованных бирж (DEX)	37
Автоматизированные маркетмейкеры (AMM).....	38
Какие существуют типы AMM?.....	39
Как определяются цены в формуле AMM на основе постоянного значения произведения? ..	41
Различные автоматизированные маркетмейкеры (AMM).....	42
Uniswap.....	42
SushiSwap	44
Balancer	47
Curve Finance	48
Bancor	49
Каковы различия между AMM?	50
I. Комиссии пула.....	50
II. Майнинг ликвидностью.....	51
III. Веса активов в пуле	52
Риски, связанных с использованием AMM.....	53
I. Ценовое проскальзывание	53

II.	Фронтраннинг	55
III.	Непостоянные потери	56
Децентрализованные биржи, заслуживающие упоминания		58
Вывод		59
Рекомендуемая литература		59
ГЛАВА 4: АГРЕГАТОРЫ DEX		60
Протоколы агрегаторов DEX		60
1inch Network	60	
Matcha	62	
Paraswap	63	
Факторы производительности агрегаторов DEX		63
Какой агрегатор DEX представляет наибольшую ценность?		65
Сопутствующие риски		66
Агрегаторы, заслуживающие упоминания		67
Вывод		67
Рекомендуемая литература		68
ГЛАВА 5: ДЕЦЕНТРАЛИЗОВАННОЕ КРЕДИТОВАНИЕ		69
Обзор протоколов кредитования		70
Compound	70	
Maker	71	
Aave	72	
Cream Finance	72	
Подробное сравнение протоколов		73
Количество поддерживаемых активов	74	
Доход	74	
Объем заблокированных средств (TVL)	75	
Коэффициент использования (BV/TVL)	76	
Ставки по кредитам и займам		77
Кредиторы	77	
Заемщики	78	
Сопутствующие риски		79
Протоколы кредитования, заслуживающие упоминания		80
Вывод		81
Рекомендуемая литература		81
ГЛАВА 6: ДЕЦЕНТРАЛИЗОВАННЫЕ СТЕЙБЛКОИНЫ И СТАБИЛЬНЫЕ АКТИВЫ		82
Централизованный стейблкоин		82
Tether (USDT)	82	
Децентрализованный стейблкоин		83

DAI.....	83
Как мы решаем задачу стейблкоинов?	84
Что такое алгоритмические стейблкоины и стабильные активы?.....	84
Модель ребейза	86
Ampleforth.....	86
Модель сеньоража.....	86
Empty Set Dollar.....	87
Basis Cash.....	88
Frax Finance.....	88
Как ранее обстояли дела с алгоритмическими стейблкоинами?.....	89
Почему FRAX стал успешным?.....	91
Следующее поколение алгоритмических стейблкоинов и стабильных активов.....	91
Fei Protocol	92
Reflexer.....	93
Float Protocol.....	94
Какое будущее у новых алгоритмических стейблкоинов и стабильных активов?.....	95
1. Обеспечение	95
2. Стимулы и сдерживающие факторы для трейдеров.....	96
3. Полномочия в чрезвычайных ситуациях.....	97
Сопутствующие риски.....	97
Стейблкоины, заслуживающие упоминания	98
Вывод.....	99
Рекомендуемая литература	99
ГЛАВА 7: ДЕЦЕНТРАЛИЗОВАННЫЕ ПРОИЗВОДНЫЕ ФИНАНСОВЫЕ ИНСТРУМЕНТЫ (ДЕРИВАТИВЫ).....	100
Децентрализованные бессрочные деривативы.....	100
Perpetual Protocol	100
dYdX	102
Сравнение Perpetual Protocol и dYdX (уровень 1).....	103
Бессрочные деривативы, заслуживающие упоминания.....	104
Децентрализованные опционы	104
Hegic.....	105
Orup.....	106
Сравнение Hegic и Orup.....	107
Децентрализованные опционы, заслуживающие упоминания.....	107
Синтетические активы	108
Synthetix	109
UMA	110
Сравнение Synthetix и UMA.....	112
Синтетические активы, заслуживающие внимания	113
Сопутствующие риски	113

Вывод.....	114
Рекомендуемая литература	114
ГЛАВА 8: ДЕЦЕНТРАЛИЗОВАННОЕ СТРАХОВАНИЕ	116
Что такое страхование?.....	116
Как работает страхование?.....	117
Нужно ли страхование в криптоиндустрии?.....	117
Протоколы страхования DeFi.....	117
Nexus Mutual	118
Типы страховок	118
Покупка страховки	119
Оценка страхового случая	119
Оценка рисков	120
Токеномика	121
Доходы от протокола	122
Armor Protocol	123
arNXM	123
arNFT	124
arCORE	124
arSHIELD	124
Заявки на страховой случай	125
Доходы от протокола	125
Cover Protocol.....	126
Типы страховок	126
Покупка страховки	127
Оценка страхового случая	127
Оценка рисков	127
Доходы протокола	128
Сравнение Nexus Mutual и Cover Protocol.....	128
Эффективность использования капитала	129
Доступные страховки	129
Процент выплат по страховым полисам	130
Сопутствующие риски	130
Страховые продукты, заслуживающие упоминания	131
Вывод.....	132
Рекомендуемая литература	133
ЧАСТЬ ТРЕТЬЯ: РАЗВИВАЮЩИЕСЯ КАТЕГОРИИ DEFI.....	134
ГЛАВА 9: ДЕЦЕНТРАЛИЗОВАННЫЕ ИНДЕКСЫ.....	135
Распределение ETF DeFi.....	136
Index Cooperative (INDEX)	137
Indexed Finance (NDX).....	137
PowerPool Concentrated Voting Power (CVP).....	138
Сравнение протоколов индексов	138

Комиссии протокола.....	139
Стратегии протоколов.....	140
Вес фондов.....	141
Сопутствующие риски.....	142
Децентрализованные индексы, заслуживающие упоминания.....	143
Вывод.....	143
Рекомендуемая литература	144
ГЛАВА 10: ДЕЦЕНТРАЛИЗОВАННЫЕ РЫНКИ ПРОГНОЗИРОВАНИЯ.....	145
Как работают протоколы прогнозирования?.....	145
Маркетмейкинг.....	145
Решение	147
Протоколы рынков прогнозирования.....	147
Augur	147
Omen.....	148
Каковы еще ключевые различия между Augur и Omen?	149
Сопутствующие риски.....	152
Протоколы рынков прогнозирования, заслуживающие упоминания.....	152
Вывод.....	152
Рекомендуемая литература	153
ГЛАВА 11: ДЕЦЕНТРАЛИЗОВАННЫЕ ПРОТОКОЛЫ С ФИКСИРОВАННОЙ ПРОЦЕНТНОЙ СТАВКОЙ	154
Обзор Протоколов с фиксированными процентными ставками	155
Yield.....	155
Saffron.Finance.....	157
Horizon Finance	158
Какой FIRP лучше использовать?.....	160
Сопутствующие риски	161
Протоколы с фиксированной ставкой, заслуживающие упоминания.....	161
Вывод.....	162
Рекомендуемая литература	163
ГЛАВА 12: ДЕЦЕНТРАЛИЗОВАННЫЕ АГРЕГАТОРЫ ДОХОДНОСТИ	164
Протоколы агрегаторов доходности.....	164
Yearn Finance	164
Хранилища	165
Стратегии	166
Партнерства Yearn Finance	167
Alpha Finance	167
Badger Finance	169

Harvest Finance.....	170
Сравнения агрегаторов доходности.....	171
Сопутствующие риски	172
Агрегаторы доходности, заслуживающие упоминания.....	172
Вывод.....	172
Рекомендуемая литература.....	173
ЧАСТЬ ЧЕТВЕРТАЯ: ТЕХНОЛОГИИ, ОПРЕДЕЛЯЮЩИЕ DEFI.....	174
ГЛАВА 13: ОРАКУЛЫ И АГРЕГАТОРЫ ДАННЫХ.....	175
Протоколы оракулов.....	175
Chainlink	176
Band Protocol	178
Агрегаторы данных.....	180
Graph Protocol.....	180
Covalent.....	182
Оракулы и агрегаторы данных, заслуживающие упоминания	183
Сопутствующие риски	184
Вывод.....	184
Рекомендуемая литература	185
ГЛАВА 14: МУЛЬТИЧЕЙН ПРОТОКОЛЫ И КРОССЧЕЙН МОСТЫ	186
Обзоры протоколов и мостов.....	186
Ren Project	186
Блокировка и формирование актива.....	187
Сжигание и высвобождение актива	188
Сжигание и формирование актива.....	188
ThorChain	188
Binance Bridge.....	191
Anyswap.....	192
Terra Bridge	193
Мультичейн и кросчейн платформы, заслуживающие упоминания	194
Сопутствующие риски	194
Вывод.....	195
Рекомендуемая литература	195
ГЛАВА 15: ВЗЛОМЫ DEFI	196
Причины взломов.....	197
1. Экономические взломы/флэш-займы.....	197
2. Культура использования кода.....	197
3. Небрежное кодирование и недостаточный аудит.....	197
4. Выдергивание ковра (инсайдерская работа).....	198
5. Атака оракула	198

6. Атака на Metamask	198
Флэш-займы	199
Что такое флэш-займы?	199
Использование флэш-займа.....	200
Протокол флэш-займов: Furucombo	201
Тематическое исследование: Взлом флэш-займов bZx.....	202
Заключение по флэш-займам.....	204
Решения	205
Фонд внутреннего страхования.....	205
Страхование	205
Вознаграждения за выявление ошибок	205
Другие возможные решения.....	206
Советы для частных лиц.....	206
Не предоставляйте смарт-контрактам неограниченное одобрение.....	206
Не предоставляйте смарт-контрактам неограниченное одобрение: Руководство.....	207
Отзыв неограниченных разрешений от смарт-контрактов.....	210
Использование аппаратного кошелька	211
Использование отдельного профиля браузера.....	211
Отдельный профиль браузера: Пошаговое руководство.....	212
Вывод.....	214
Рекомендуемая литература	214
ГЛАВА 16: БУДУЩЕЕ ФИНАНСОВ	215
Сколько времени пройдет до того, как институты будут опираться на эти сети?.....	216
К чему это приведет нас в ближайшие 5-10 лет?.....	216
ЗАКЛЮЧЕНИЕ	218
ПРИЛОЖЕНИЯ.....	219
Рекомендации CoinGecko.....	219
Аналитика	219
Новые сайты.....	219
Почтовые рассылки	219
Подкасты	220
Youtube.....	220
Руководство по Bankless	220
Понравившиеся проекты.....	220
Панели управления.....	220
Децентрализованные обмены.....	220
Агрегаторы обмена	221
Кредитование и заимствование	221
Оракулы и агрегаторы данных	221
Рынки прогнозирования.....	221
Налоги	221
Кошельки	221
Оптимизаторы дохода.....	221

Введение

Когда мы впервые написали книгу «Что такое DeFi: Курс для начинающих» (первое издание) в марте 2020 года, мы намеренно опустили много информации, чтобы начинающим было легче начать работу с DeFi. Мы знали, что книга лишь представляет поверхностную информацию о том, что может предложить DeFi. Конечно, новичкам так не покажется – многие просто пытаются понять быстро растущую отрасль, требующую ускоренного обучения.

По мере того как наши читатели знакомились с основами DeFi, последовал спрос на более глубокие знания. Мы знали, что нам нужно написать продолжение для читателей, заинтересованных в дальнейшем изучении DeFi, поэтому мы написали продвинутую книгу с этой целью.

Мы понимаем, как легко заблудиться в DeFi. Каждую неделю появляются инновации в протоколах, повышающие эффективность DeFi и расширяющие возможности их использования. Полностью устраниТЬ этот пробел в знаниях невозможно, тем не менее, в этой книге мы надеемся преодолеть этот пробел с помощью наших исследований и анализа ключевых сегментов DeFi.

В этом издании мы кратко расскажем о текущем состоянии DeFi и о том, чего мы можем ожидать в ближайшие годы. Мы сравним существующие протоколы в соответствующих секторах и предложим некоторый сравнительный анализ.

На протяжении всей книги у нас также будут представлены ссылки на **рекомендуемую литературу** в конце каждой главы. В этих разделах мы поделимся дополнительными материалами, которые, по нашему мнению, будут полезны, когда вы глубже погрузитесь в экосистему DeFi. Благодаря авторам этих материалов DeFi стал более доступным!

Эта книга лучше всего подходит для читателей, которые уже обладают некоторым базовым пониманием DeFi и намерены стать активными пользователями DeFi. Поэтому мы рекомендуем новичкам начать с нашей книги «Что такое DeFi: Курс для начинающих», прежде чем продолжить с «Что такое DeFi: Продвинутый курс».

Мы надеемся, что, поделившись нашими знаниями, вы получите более глубокое понимание DeFi и сможете решить, какие протоколы DeFi лучше всего соответствуют вашим потребностям.

CoinGecko

Lucius Fang, Benjamin Hor, Erina Azmi, Khor Win Win

1 мая 2021 года

ЧАСТЬ ПЕРВАЯ: СОСТОЯНИЕ DEFI

Глава 1. Обзор DeFi

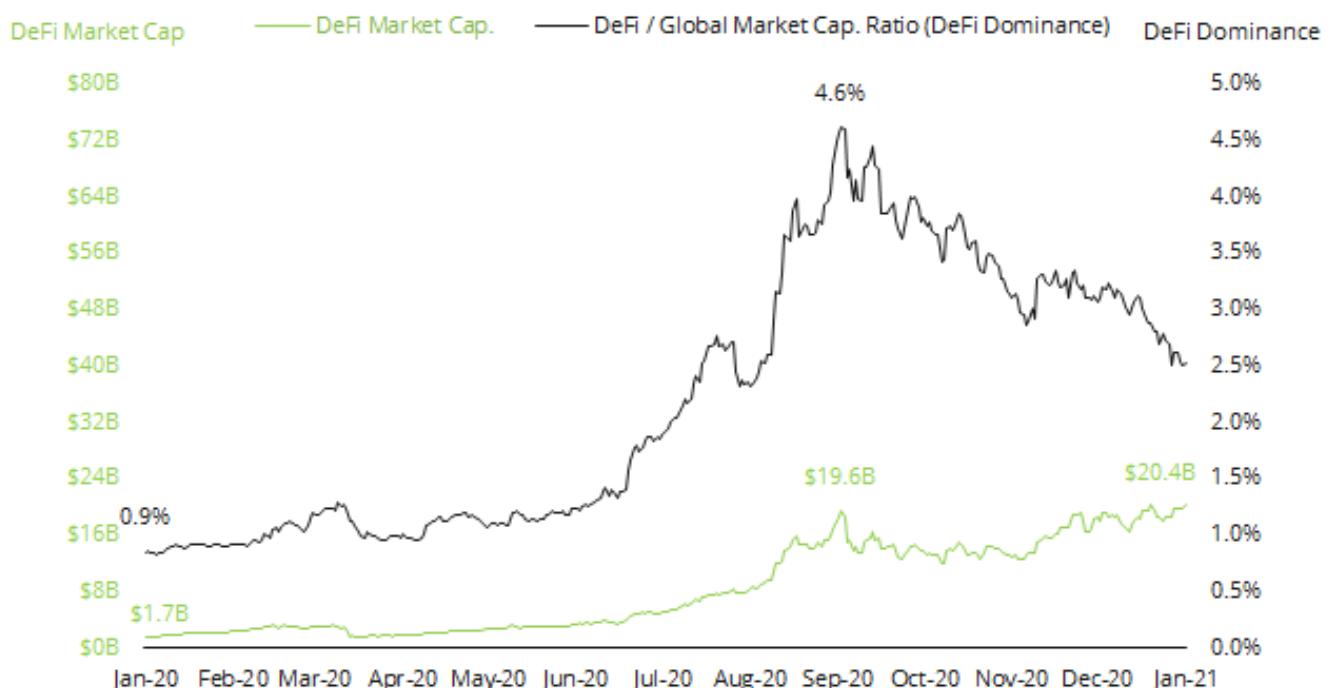
Рост децентрализованных финанс (DeFi) застал криптомир врасплох летом 2020 года настолько, что мы называем этот период летом DeFi 2020 года. Общая заблокированная стоимость (TVL), показатель объема капитала, заблокированного в протоколах DeFi, рос с головокружительной скоростью, превысив волшебное значение в 1 миллиард долларов в мае 2020 года и завершив год с 15,7 миллиардами долларов в TVL.

С тех пор DeFi непрерывно растет, расширяясь в другие блокчейны, не связанные с Ethereum. TVL DeFi достигла поразительной цифры в 86,05 миллиарда долларов в апреле 2021 года, демонстрируя экспоненциальный рост криptoиндустрии.

В этой главе мы рассмотрим ключевые события лета 2020 года DeFi, рассмотрим текущую экосистему DeFi, рост комиссий на газ в Ethereum и поделимся своими мыслями о том, как DeFi становится мейнстримом.

Лето DeFi 2020 года

Криптопространство стало свидетелем стремительного роста сектора DeFi в 2020 году, особенно с июня по август. Рыночная капитализация протоколов DeFi увеличилась в 12 раз до 19,6 миллиарда долларов в разгар лета, которое назвали Летом DeFi 2020. Доминирование DeFi, рассчитанное путем соотношения рыночной капитализации проектов DeFi к общей капитализации крипторынка, быстро выросло с 0,9% до 4,6%.

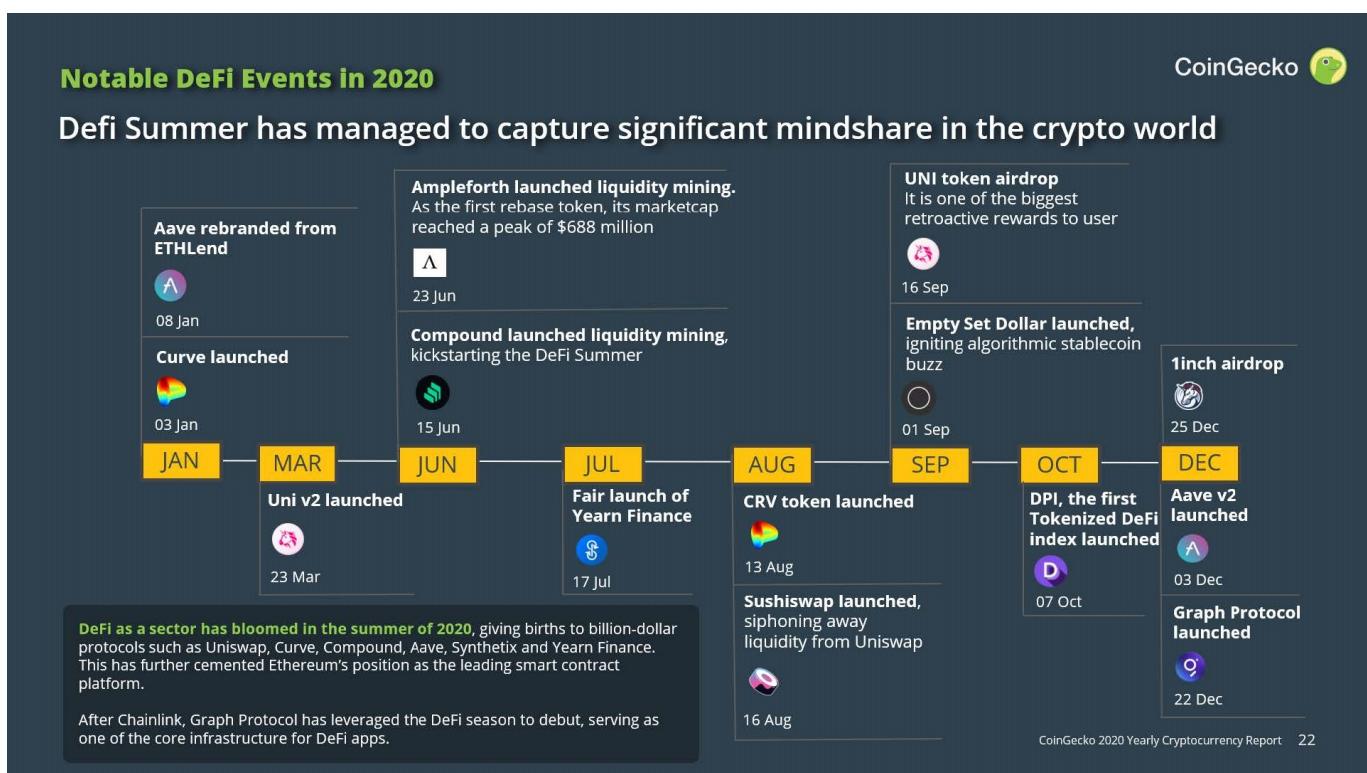


Для тех из вас, кто не был связан с DeFi в 2020 году, мы подготовили краткий обзор ключевых событий DeFi в 2020 году.

2020 год характеризовался запуском протоколов и токенов многих ключевых проектов DeFi. Многие из этих протоколов DeFi внедрили программы майнинга ликвидности с высокой доходностью, чтобы привлечь пользователей к своим протоколам.

Майнинг ликвидности – это программа вознаграждения, которая выдает собственные токены протокола пользователям, предоставляющим ликвидность протоколу DeFi. Майнинг ликвидности не является какой-то новой концепцией в DeFi. Он был впервые представлен компанией Synthetix еще в июле 2019 года, а позже был популяризирован компанией Compound в июне 2020 года.

Популярность этих программ майнинга ликвидности привела к тому, что летом 2020 года было запущено множество проектов, многие из которых включали названия продуктов питания и овощей, такие как Yam (сладкая картошечка) и Pickle (соленый огурчик). Пользователи провели напряженное лето, будучи «майнерами доходности», активно вкладывая свой капитал в различные протоколы DeFi в поисках самых высоких доходов.



Агрегатор доходности Yearn Finance создал ажиотаж «честного запуска» в июле 2020 года. Токены YFI были справедливо распределены среди всех, кто хотел принять участие, без каких-либо частных продаж ранним инвесторам. История продолжилась «случайным» запуском токена CRV компанией Curve Finance в августе 2020 года.

В том же месяце был запущен SushiSwap, форк Uniswap. SushiSwap провел так называемую атаку «вампирского майнинга», чтобы переманить ликвидность из Uniswap, введя токен SUSHI для стимулирования пользователей.

Чтобы не отстать от конкурента, Uniswap в сентябре 2020 года осуществила раздачу токена UNI, что привело к неожиданной прибыли для всех пользователей, которые взаимодействовали с протоколом Uniswap. (Примечание: если бы вы прочитали нашу книгу «Что такое DeFi: Курс для начинающих» в 2020 году и использовали Uniswap перед выпуском токена UNI, вы бы тоже получили UNI!)

Это положило начало еще одной волне крипто-безумия, когда многие проекты решили запустить свои токены, чтобы привлечь больше пользователей для развития. Проекты без токенов вскоре оказались вынуждены рассмотреть возможность выпуска токенов для эффективной конкурентоспособности.

Экосистема DeFi

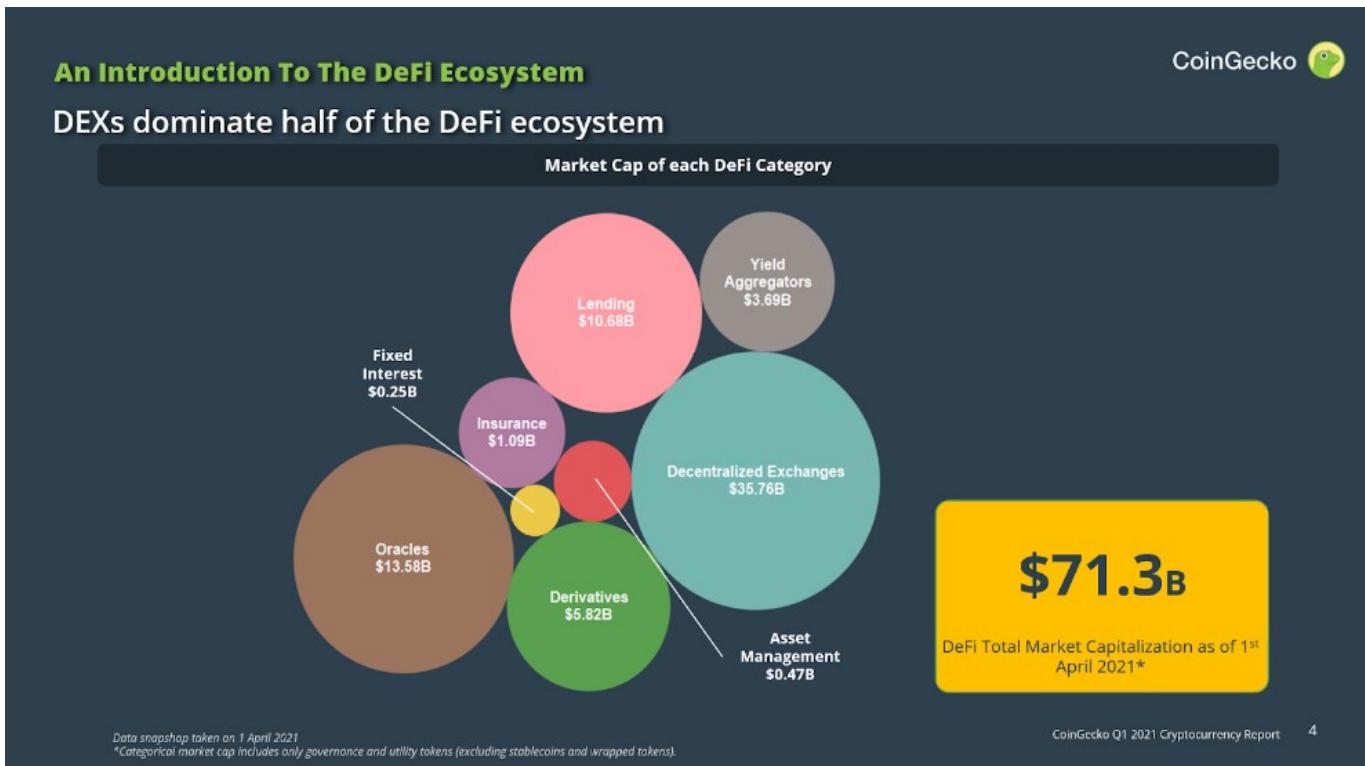
Общая заблокированная стоимость DeFi (TVL) в апреле 2021 года превысила впечатляющие 86,05 миллиарда долларов. TVL является одним из наиболее широко используемых показателей в DeFi, поскольку он представляет общую сумму активов, удерживаемых каждым протоколом. Как правило, чем больше значений зафиксировано в протоколе, тем лучше для протокола.

В большинстве случаев заблокированный капитал используется для предоставления таких услуг, как маркетмейкинг (market making - ММ), кредитование, управление активами и арбитраж со всей экосистемой, принося доход провайдерам капитала.

Однако TVL не всегда является надежным показателем, поскольку его уровни могут быть нестабильными, так как капитал может быть ограничен временными стимулами, такими как программы майнинга ликвидности или внешние катализаторы, такие как ошибки в смарт-контрактах. Следовательно, важно смотреть на TVL с течением времени, чтобы измерить удержание капитала и лояльность пользователей.

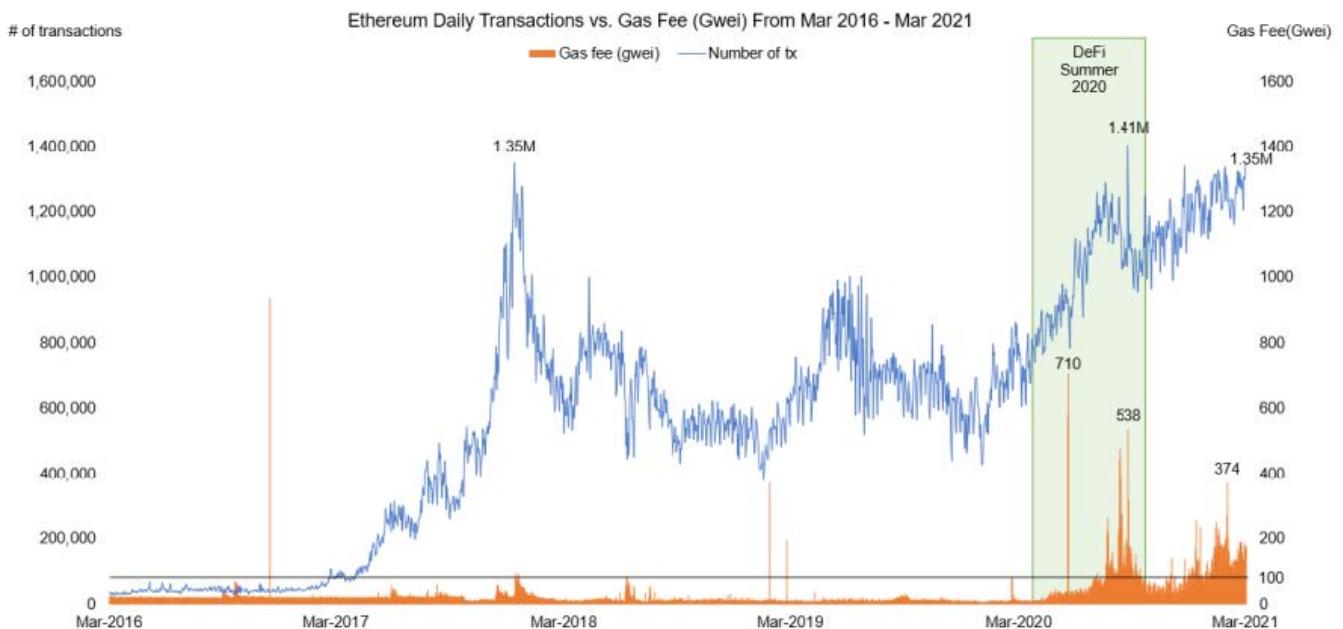
С таким большим объемом капитала, «заблокированным» внутри пространства, появились различные приложения DeFi, бросающие вызов нормам финансовых теорий и их границам. Новые финансовые эксперименты происходят ежедневно, порождая новые категории, такие как алгоритмические стейблкоины (stablecoin).

Ниже приведен обзор развивающейся экосистемы DeFi, основанной на рыночной капитализации. Категория децентрализованной биржи (DEX) является самой крупной, за которой следуют категории оракулов (oracles) и кредитов (lending).



Повышение стоимости газа (Gas – комиссия)

С начала 2020 года количество транзакций на Ethereum непрерывно росло и превысило миллион транзакций в день. Уровень транзакций, похоже, находится на пути к преодолению пиковых уровней транзакций 2018 года.



Большое количество сделок привело к росту цен на газ, которые к августу 2020 года достигли колоссальных 700 gwei за сделку (для наглядности – это порядка 100\$ за простую операцию при курсе 2000\$ за 1 ETH). Хотя цена на газ в 2021 году ниже по сравнению с летом 2020 года, цена эфира в 2021 году намного выше, что

приводит к росту общих комиссий за транзакции. Ethereum побил свой предыдущий рекордный максимум в январе 2021 года и зафиксировал новый пик в размере 4 357 \$ 12 мая 2021 года.

From Dec 29, 2018 To May 14, 2021



Высокая цена на газ и рост цен на Ethereum сделали использование многих приложений DeFi на Ethereum экономически нецелесообразным для пользователей без значительного капитала. Выполнение простого обмена токенов на Uniswap в 1 квартале 2021 года могло стоить до 100 долларов за транзакцию, что делало его возможным только для крупных обменов. Комиссии за транзакции становятся еще выше для более сложных транзакций, таких как транзакции по фармингу.

Высокие комиссии за транзакции заставили многих пользователей Ethereum DeFi искать более дешевые альтернативы. Такими стали решения второго уровня (Layer-2, такие как Optimism, Arbitrum, zkRollups), сайдчейны (например, xDai и Polygon) или конкурирующие блокчейны уровня 1 (например, Binance Smart Chain, Solana и Terra). Мы рассмотрим их более подробно в Главе 14.

DeFi становится мейнстримом

Криptoиндустрия привлекла большое внимание в первой половине 2021 года. Значимые события, происходящие во всем мире, привели к появлению захватывающих внимание заголовков, таких как:

1. Первоначальные инвестиции Tesla в биткоин в размере 1,5 миллиарда долларов (примечание: Илон Маск отказался позже от биткоина и вернул обратно деньги, разумеется с прибылью, а сейчас строит ферму для майнинга).
2. Продажа неизменяемого токена (NFT, НФТ) Beeple за 69 миллионов долларов (коллаж «Everydays: The First 5000 Days» художника Майка Винкельманна) на аукционе Christie's.
3. Visa, поддерживающая USDC (долларовый стейблкоин) в качестве варианта расчетов в Ethereum.
4. Планы Fidelity по созданию биржевого фонда биткоинов.
5. Листинг Coinbase на бирже NASDAQ.
6. Позитивное восприятие Китаем биткоина и других криптоактивов в качестве альтернативных инвестиций (примечание переводчика: на данный момент власти Китая рекомендуют не использовать криптовалюты основным банкам страны, а также запрещает рекламировать их в сети TikTok).

Повышенное внимание средств массовой информации к более широкому крипторынку также привело к тому, что все больше внимания уделяется DeFi. В частности, институциональные инвесторы начали обращать на это внимание. Например, в отчете Citibank «Глобальная перспектива и решения» (Citi GPS), озаглавленном «Будущее денег: криптовалюта, CBDC (*Central Bank Digital Currency, цифровая валюта центрального банка*) и наличные деньги 21 века», банк с 209-летней историей рассказал о преимуществах DeFi, включая устранение посредников и повышение финансовой прозрачности.

Примечательно, что в том же докладе также были рассмотрены различные протоколы DeFi, такие как Maker, Compound, Uniswap и UMA. Подробный отчет Федерального резервного банка Сент-Луиса также подчеркивает потенциал DeFi, способный вызвать «изменение парадигмы в финансовой индустрии и потенциально способствовать созданию более надежной, открытой и прозрачной финансовой инфраструктуры».

Также видно, как инвестиционные институты пробуют использовать DeFi. Grayscale, один из наиболее известных цифровых инвестиционных фондов, активно предлагает доступ к определенным активам (например, Chainlink) через трасты на основе акций. Фонд управления активами Bitwise также имеет фонд индекса DeFi, который предлагает доступ к более чем 10 активам DeFi, таким как Aave и Compound. Когда фонд открылся в марте 2021 года, он собрал 32,5 миллиона долларов всего за две недели.

DeFi также не останавливается на виртуальном пространстве. Предполагаемые случаи использования DeFi в «реальном мире» уже материализовались, так как протоколы DeFi признаны подходящими альтернативами традиционным банковским инструментам.

Centrifuge, одна из первых компаний «реального мира», которая интегрировалась с MakerDAO, использует нецифровые активы в качестве залога через свое приложение Tinlake. 21 апреля 2021 года компания успешно оформила свой первый кредит на базе MakerDAO на сумму 181 тыс. долларов с домом в качестве залога, фактически создав одну из первых заладных на основе блокчейна.

Рекомендуемая литература

1. Отчет CoinGecko за 1 квартал 2021 года

<https://assets.coingecko.com/reports/2021-Q1-Report/CoinGecko-2021-Q1-Report.pdf>

2. Понять Эфириум, уровень 2.

<https://ethereum.org/en/eth2/>

3. За пределами Ethereum: Убийцы или усилители Ethereum?

<https://peeman34.medium.com/ethereum-enhancers-or-ethereum-killers-a-new-ecosystem-dd7aeed3d440>

ГЛАВА 2: ДЕЯТЕЛЬНОСТЬ DEFI

В этой главе мы рассмотрим различные способы участия в экосистеме DeFi. Протоколы DeFi предоставляют доступ и беспрецедентную свободу провайдерам капитала в финансовой сфере.

Такие виды деятельности, как маркетмейкеры (ММ), страхование и создание структурированных продуктов, ранее были доступны только институционалам с большой базой капитала и специализированными знаниями. DeFi значительно снизила эти барьеры и предоставила эти виды деятельности широким массам.

Мы расскажем далее о некоторых ключевых областях и видах деятельности DeFi, таких как фарминг, майнинг ликвидности, раздача токенов (airdrop) и первоначальные предложения DEX (IDO).

Фарминг

Фарминг, пожалуй, является одной из самых инновационных особенностей DeFi. Это относится к деятельности по выделению капитала протоколам DeFi для получения прибыли.

Большинство протоколов DeFi являются peer-to-peer (P2P) финансовыми приложениями, в которых выделенный капитал используется для предоставления услуг конечным пользователям. Сборы, взимаемые с пользователей, затем распределяются между провайдерами капитала и протоколом. Сборы, которые получают провайдеры капитала, являются внутренней доходностью.

На криpto-сленге мы называем этих инвесторов «фермерами», а возможности получения дохода – «фармингом». Многие фермеры, постоянно меняют свои места заработка в поисках возможностей для получения наивысшей прибыли.

Ниже приведены некоторые примеры фарминга, где предоставленный капитал будет использоваться для различных целей:

- Биржи – предоставление капитала для создания рынка на децентрализованных биржах, получая взамен комиссионные за транзакции.
- Кредитование – предоставление кредитов заемщикам, получая проценты.
- Страхование – использование страхования, получая страховые взносы и принимая на себя риск выплаты страховки в случае наступления определенного события.
- Опционы – использование опционов на продажу или покупку («колл», «пут»), чтобы получить прибыль.
- Синтетические активы – формирование стейблкоинов или других синтетических активов, получая взамен комиссионные.

Майнинг ликвидности

Финансовые услуги являются капиталоемкой отраслью и, как правило, выигрывают от экономии за счет масштаба. Это означает, что чем больше капитала у фирм, тем лучше. Протоколы DeFi не являются исключением - получение значительного капитала станет существенным конкурентным преимуществом для протоколов DeFi.

В криptoиндустрии протоколы DeFi стимулируют предоставление ликвидности с помощью программ майнинга ликвидности. Майнинг ликвидности относится к программе вознаграждения собственными токенами протокола в обмен на предоставление капитала. Эти токены обычно поставляются с правами управления и могут иметь возможность получения денежных потоков от протоколов DeFi.

При правильном проектировании программы майнинга ликвидности являются быстрым способом получения больших объемов ликвидности за короткий промежуток времени, хотя и с уменьшением владения токенами. Эти программы также могут быть использованы для стимулирования новых пользователей к опробованию новых протоколов DeFi. Вы, возможно, подумали об аналогичных стимулах в Uber (хотя вряд ли вы это вспомнили), который субсидировал поездки в первые дни с использованием венчурного капитала.

Программы майнинга ликвидности также являются новым способом привлечения участия сообщества в протоколах DeFi. Поскольку протоколы DeFi по своей природе являются открытыми, они опираются на добровольное участие сообщества. Распределение токенов поощряет участие сообщества в определении будущего направления протокола.

Хотя может показаться, что программы майнинга ликвидности предлагают бесплатные вознаграждения, участвуя в них, вы на некоторое время блокируете свой капитал, и у вашего капитала есть издержки неполучения более высокой прибыли в другом месте. Кроме того, во многих случаях блокировка вашего капитала не является безрисковой. Деятельность фарминга, как правило, сопряжена с различными рисками, которые могут привести к потере денег.

Наиболее распространенной формой программы майнинга ликвидности является предоставление собственной ликвидности токенов на децентрализованных биржах с использованием базовых токенов, таких как ETH, WBTC (биткоин) или стейблкоины в долларах США. Такие программы стимулируют создание ликвидности вокруг собственных токенов протокола и позволяют пользователям легко торговать этими токенами на децентрализованных биржах.

Пример

В августе 2020 года децентрализованная биржа SushiSwap запустила свой токен управления под названием SUSHI и хотела увеличить ликвидность между SUSHI и ETH. Команда предложила вознаградить бесплатными токенами SUSHI любого, кто предоставит ликвидность в торговой паре SUSHI/ETH на SushiSwap.

Пользователи должны были предоставлять как SUSHI, так и ETH в равном соотношении. Давайте предположим, что у пользователя есть ETH на сумму 1000 долларов и он хотел бы принять участие в этой программе майнинга ликвидности, чтобы заработать токены SUSHI. Пользователь сначала обменивает половину своего ETH на SUSHI. Затем он предоставляет SUSHI на 500 долларов и ETH на 500 долларов в пул ликвидности SUSHI/ETH. Ему будут предоставлены токены провайдера ликвидности SUSHI/ETH (LP - Liquidity Provider), представляющие его долю в пуле ликвидности, которую затем можно будет разместить на платформе SushiSwap для получения поощрения за токен SUSHI.

Другие типы программ майнинга ликвидности имеют различные названия, основанные на протоколе, в котором используется заблокированный капитал. Например, Compound, децентрализованный протокол кредитования и заимствования, выдает токены COMP кредиторам и заемщикам для стимулирования протокольной деятельности. Nexus Mutual, децентрализованный протокол страхования, имеет программу майнинга Shield, которая выдает токены NXM держателям токенов NXM, которые вкладывают свой капитал в определенные протоколы, чтобы увеличить возможности страхования. Hegic, децентрализованный протокол опционов, предоставляет токены rHEGIC продавцам и покупателям опционов для стимулирования активности протокола.

Существует несколько веб-сайтов для мониторинга возможностей фарминга и майнинга ликвидности:

- <https://www.coingecko.com/en/yield-farming>
- <https://vfat.tools/>
- <https://zapper.fi/farm>

Раздачи токенов (Airdrops)

Раздачи токенов – это, по сути, бесплатное распределение токенов. Проекты обычно проводят раздачу в рамках своей маркетинговой стратегии, чтобы привлечь внимание и шумиху вокруг запуска своих токенов, хотя и с компромиссом в виде уменьшения доли владения токенами.

Некоторые проекты также проводят раздачу, чтобы вознаградить ранних пользователей, которые взаимодействовали с их протоколами. В каждом протоколе будут указаны критерии для определения получателей раздачи, такие как время взаимодействия и минимальное используемое количество.

Некоторые заметные раздачи показаны ниже:

Protocol	Token symbol	Date Airdrop	Initial Price	Price as of 1st April 2021	Return
 Uniswap	UNI	16 September 2020	\$3.44	\$28.71	734.59%
	1INCH	25 December 2020	\$2.36	\$4.46	88.98%
	POOL	17 February 2021	\$11.98	\$23.11	92.90%

Одной из наиболее заметных раздач была проведена Uniswap. Ранние пользователи получили минимум 400 UNI. По состоянию на 1 апреля 2021 года, раздача стоила 11 484 доллара. (Примечание: если бы вы прочитали нашу книгу «Что такое DeFi: Для новичков» в 2020 году и использовали Uniswap до раздачи, вы бы тоже получили токен UNI)

Первоначальное предложение DEX (IDO)

Криптовоинтакты вынуждены проявлять творческий подход к стратегиям запуска и распространения токенов. С ростом популярности децентрализованных бирж (DEX) у проектов теперь есть реальная возможность напрямую обращаться к пользователям, не платя заоблачные комиссии за размещение на централизованных биржах. Команды криптовоинтактов теперь могут размещать свои токены без необходимости получения разрешения на DEX.

Однако справедливое распределение токенов среди широкой группы пользователей по справедливой цене по-прежнему является сложной задачей. Существуют различные типы доступных IDO, и мы рассмотрим несколько популярных типов.

Первоначальное предложение по кривой спроса (IBCO – Initial Bonding Curve Offering)

Первоначальное предложение по кривой спроса, или IBCO – это довольно новая концепция, предназначенная для предотвращения практики фронтраннинга. По сути, по мере того, как все больше инвесторов вкладывают капитал в кривую спроса, цена токена будет увеличиваться по сравнению с его первоначальной стоимостью.

Однако не имеет значения, когда вы решите внести свой вклад, так как все инвесторы будут платить на основе одной и той же окончательной расчетной цены. Основываясь на цене в конце IBCO, каждый инвестор получит часть токенов в зависимости от их доли в общем инвестированном капитале. Такие проекты, как Hegic и Aavegotchi, с большим успехом использовали этот метод распространения при первоначальных запусках токенов.

Самонастраивающийся пул ликвидности (LBP – Liquidity Bootstrapping Pool)

Размещенные с использованием «умных» пулов Balancer, самонастраивающихся пулов ликвидности (LBP) – это способ для проектов продавать токены с помощью настраиваемого автоматизированного маркетмейкера (AMM). Обычно эти пулы будут содержать токен проекта и залоговый токен, обычно номинированный в стейблкоинах. Создатели «умного» пула могут изменять его параметры и вводить в правила продажи различные функции, такие как снижение цены с течением времени, а также приостановка любых дальнейших обменов из-за высокого спроса или внешних уязвимостей.

Первоначальное предложение фарминга (IFO – Initial Farm Offering)

Впервые представленное PancakeSwap, первоначальное предложение фарминга (IFO) позволяет пользователям размещать свои токены провайдера ликвидности (LP) в обмен на токены проекта. Используя механизм контроля переполнения, пользователи могут вкладывать любое количество LP-токенов в проект. Благодаря схеме с возвратом лишних инвестиций (схема овербукинга. *пояснение переводчика: в этом случае PancakeSwap не может обеспечить токенами всех провайдеров ликвидности при их слишком большом количестве*), все неиспользованные средства возвращаются пользователю. IFO на PancakeSwap используют токены провайдера ликвидности CAKE-BNB, таким образом проект получает токены BNB в обмен на токены их недавно созданного токена протокола, в то время как оставшиеся токены CAKE сжигаются.

Фарминг: пошаговая инструкция

В этом разделе мы рассмотрим пошаговое руководство по фармингу. Используя предыдущий пример SUSHI/ETH в этой главе, мы покажем, как фармить с помощью Zapper.

Net Worth
\$2,700.46
Assets: \$2,761.73 Debt: \$61.27

Account Overview [Don't see your assets?](#)

Wallet	\$2,151.42	Deposits	\$281.84	Staked	\$328.48
Debt	\$61.27				

Шаг 1

- Подключите кошелек Ethereum по адресу <https://zapper.fi/dashboard>
- Выберите вкладку «Pool».

Explore Opportunities

Filter by token, protocol

#	Available Pools	Liquidity	ROI	
1	3Pool Curve Curve	\$1,513,530,625	0.98% (1y) 0.02% (1w)	<button>Invest</button>
2	stETH Curve Curve	\$1,169,379,047	0.04% (1y) 0.00% (1w)	<button>Invest</button>
3	WBTC / ETH SushiSwap	\$948,974,159	12.82% (1y) 0.25% (1w)	<button>Invest</button>
4	sETH Curve Curve	\$934,333,647	0.45% (1y) 0.01% (1w)	<button>Invest</button>
5	FEI / ETH Uniswap V2	\$906,697,368	5.32% (1y) 0.10% (1w)	<button>Invest</button>
6	SUSHI / ETH SushiSwap	\$756,612,959	8.56% (1y) 0.16% (1w)	<button>Invest</button>

Шаг 2

- В этом руководстве мы собираемся фармить SUSHI/ETH, чтобы получить токен SUSHI.
- Нажмите «Invest».

3

Add liquidity

Connected

From: ETH MAX

To: SUSHI / ETH (Sushiswap)

Est. Pool Allocation: 11.97 SUSHI, 0.05015 WETH

Pool Share: 0.00004327%

Est. Daily Fee Income: \$0.08

Transaction Settings: Slippage Tolerance: 3.00%, Minimum Received: 0.646934, Transaction Speed: Fast

Confirm

Ethereum Mainnet

Account 1 → 0xcff6...6bC2

https://zapper.fi

CONTRACT INTERACTION

♦ 0.1

DETAILS DATA

GAS FEE: ♦ 0.013817 (\$45.39)

TOTAL: ♦ 0.113817 (\$373.94)

CUSTOM NONCE: 25

Reject Confirm

Шаг 3

- В Zapper мы можем обменять любой отдельный актив на любой токен LP. Здесь мы поменяем ETH на SUSHI/ETH.
- Подтвердите транзакцию.

4

Dashboard Exchange Pool Farm Bridge History

Current Investments

Pool	Value	Earning (Fees)
SUSHI / ETH (SushiSwap)	\$325.92 11.91 SUSHI / 0.05 ETH	\$27.87 / y \$0.54 / w

Шаг 4

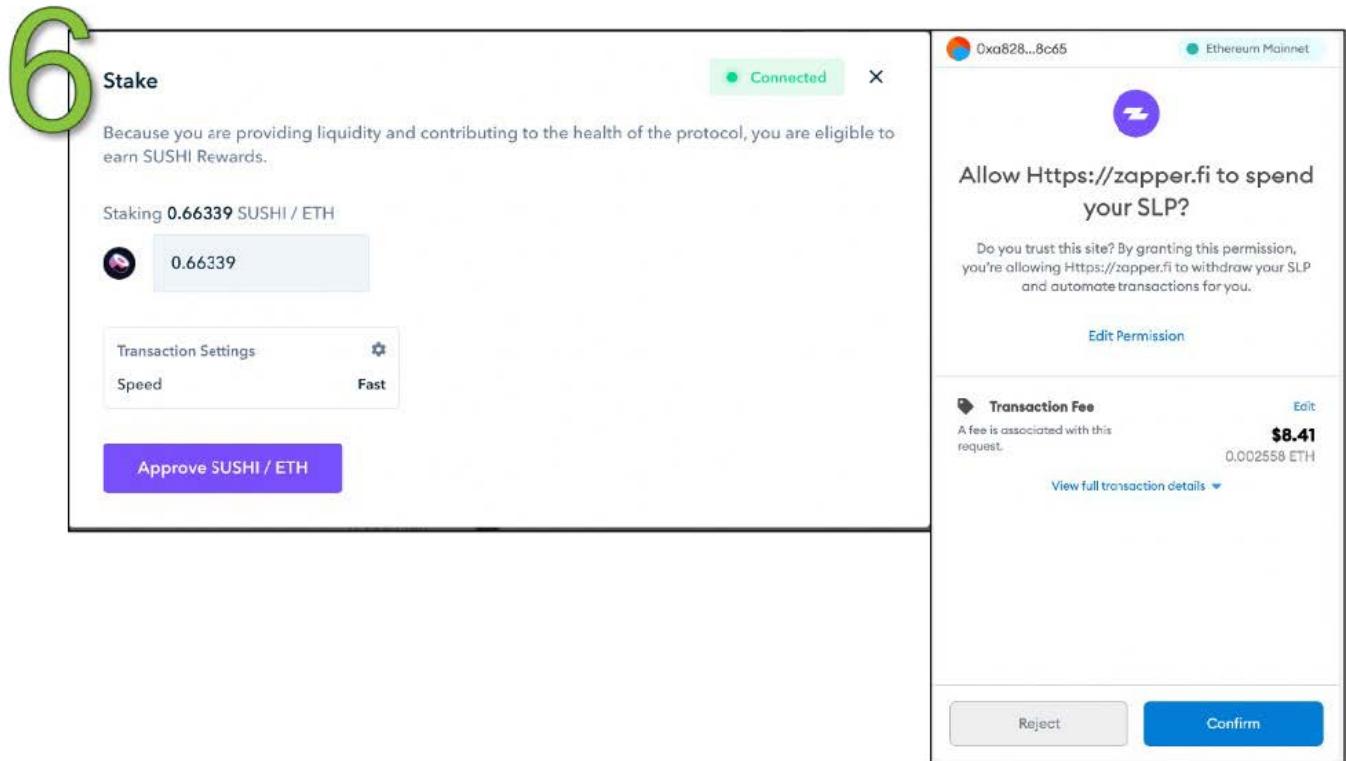
- Пул SUSHI/ETH появится в разделе «Current Investments»

5

#	Assets	Liquidity	ROI ①	Rewards
1	stETH Curve Curve	\$1,169,379,046.99	2.86% (1y) 0.05% (1w)	
2	sETH Curve Curve	\$931,818,683.80	8.28% (1y) 0.15% (1w)	
3	WBTC / ETH SushiSwap	\$887,201,167.16	13.22% (1y) 0.25% (1w)	
4	3Pool Curve Curve	\$746,131,297.57	6.49% (1y) 0.12% (1w)	
5	SUSHI / ETH SushiSwap	\$739,208,532.84	22.75% (1y) 0.43% (1w)	
6	HBTC Curve Curve	\$528,552,733.45	6.54% (1y) 0.12% (1w)	

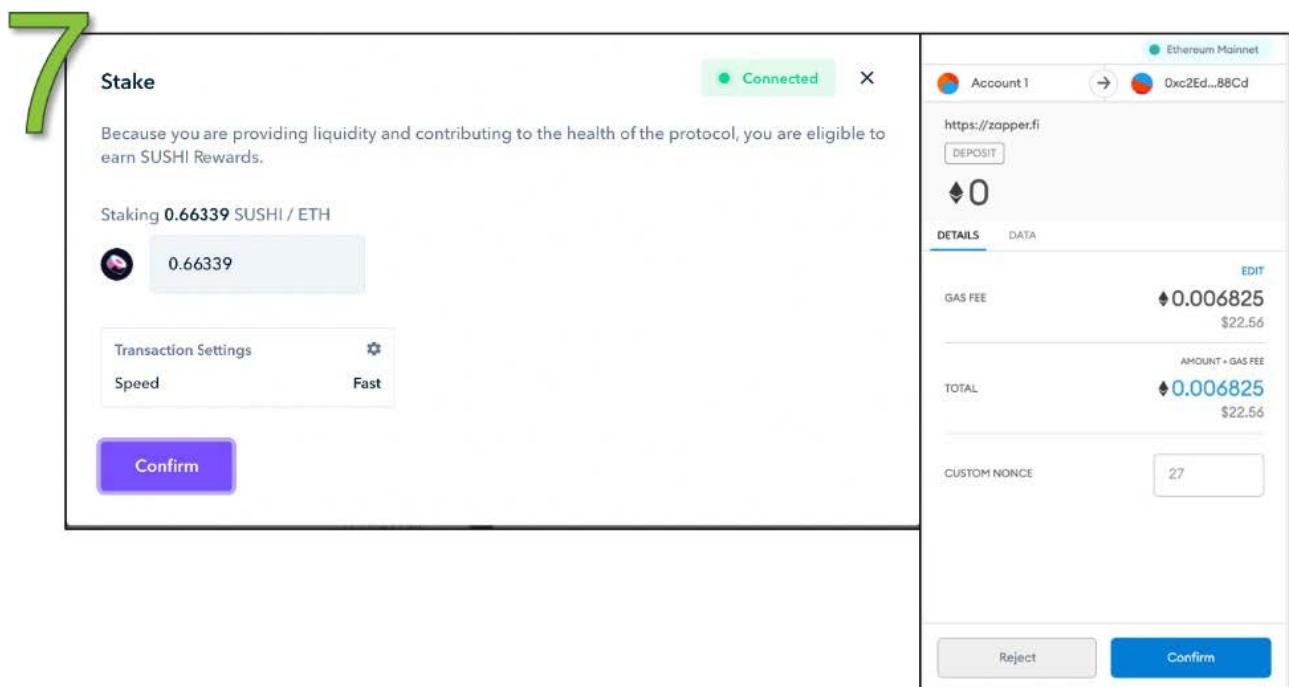
Шаг 5

- На вкладке «Farm» перечислены возможности ведения фарминга и соответствующие ожидаемые доходы.
- Появится зеленая кнопка «Stake», если у нас есть базовый актив для возможности выращивания урожая.
- Нажмите «Stake».



Шаг 6

- Одобрите транзакцию. Это позволяет Zapper получить доступ к нашему LP-токену SUSHI/ETH.



Шаг 7

- Подтвердите транзакцию

8

Active Farms

Assets	Value	Earning
SUSHI / ETH SushiSwap	\$327.62 0.6633 tokens	\$27.91 / yr \$0.54 / w

Claim Unstake

Шаг 8

- Теперь мы сможем получать комиссию за торговлю SUSHI/ETH и вознаграждение за майнинг ликвидности.
- Нажмите «Claim», чтобы забрать вознаграждение.

9

Claim your rewards

Connected X

Claiming 0.000190368 SUSHI Rewards

0.000190368

Transaction Settings Speed Fast

Confirm

Шаг 9

- Награды можно получить, нажав «Confirm».
- Мы можем выйти из позиции, нажав «Unstake», соответствующая кнопка показана на рисунке 8.

Сопутствующие риски

Как только вы познакомитесь с экосистемой DeFi, вы неизбежно увидите различные протоколы, предлагающие сногсшибательную доходность, иногда превышающую 1000% годовой процентной доходности (APY)! Хотя заманчиво вкладывать свои деньги, такие APY, как правило, являются временными и, в конечном итоге, стабилизируются до более низких показателей с приходом других фермеров.

Учитывая быстро развивающийся мир DeFi, инвесторы также должны быстро принимать решения о том, стоит ли инвестировать в проект. Синдром упущененной выгоды (FOMO – Fear of Missing Out) реален и к нему не следует относиться легкомысленно.

Независимо от того, являетесь ли вы трейдером, инвестором или фермером, всегда следует обращать внимание на риски, такие как риск уязвимостей смарт-контрактов, риск непостоянных потерь (IL – impermanent loss) и соответствующий системный риск (риск краха финансового рынка криптовалют). Независимо от того, насколько технически обоснованным может быть проект, эксплойты (использование различных уязвимостей для кражи денег) всегда возможны со стороны злоумышленников.

Пользователи должны понимать, что экосистема DeFi все еще находится в зачаточном состоянии, и большинство мероприятий DeFi все еще являются экспериментальными. Мы рассмотрим различные типы рисков, связанных с каждой категорией DeFi, на протяжении всей этой книги и посвятим всю главу 15 рискам, связанным с использованием смарт-контрактов.

Вывод

DeFi – это прорыв. Мы являемся свидетелями финансовой революции, происходящей прямо перед нами, которая демократизирует доступ к финансам, способствует расширению доступа к финансовым услугам и обещает финансовую прозрачность. Хотя DeFi в своей текущей итерации не идеален, он дает нам представление о том, как может выглядеть будущее.

Любой человек в мире, имеющий доступ к Интернету, теперь может принять участие в этом грандиозном финансовом эксперименте. Криптофинансовые операции, такие как предоставление ликвидности и токенизация собственности, позволяют создавать новые формы организаций. Пройдет совсем немного времени, и мы увидим, что протоколы DeFi более ценные, чем крупнейшие компании в мире.

Рекомендуемая литература

1. Токены управления: Инвестиции в фундаментальные блоки новой экономики

<https://thedefiant.io/governance-tokens-investing-in-the-building-blocks-of-a-new-economy/>

2. Новые модели служебных токенов

<https://multicoin.capital/2018/02/13/new-models-utility-tokens/>

3. Вопросы и ответы по раскрутке ликвидности

<https://docs.balancer.finance/smart-contracts/smart-pools/liquidity-bootstrapping-faq>

4. Что такое фарминг

<https://learn.zapper.fi/articles/what-is-yield-farming>

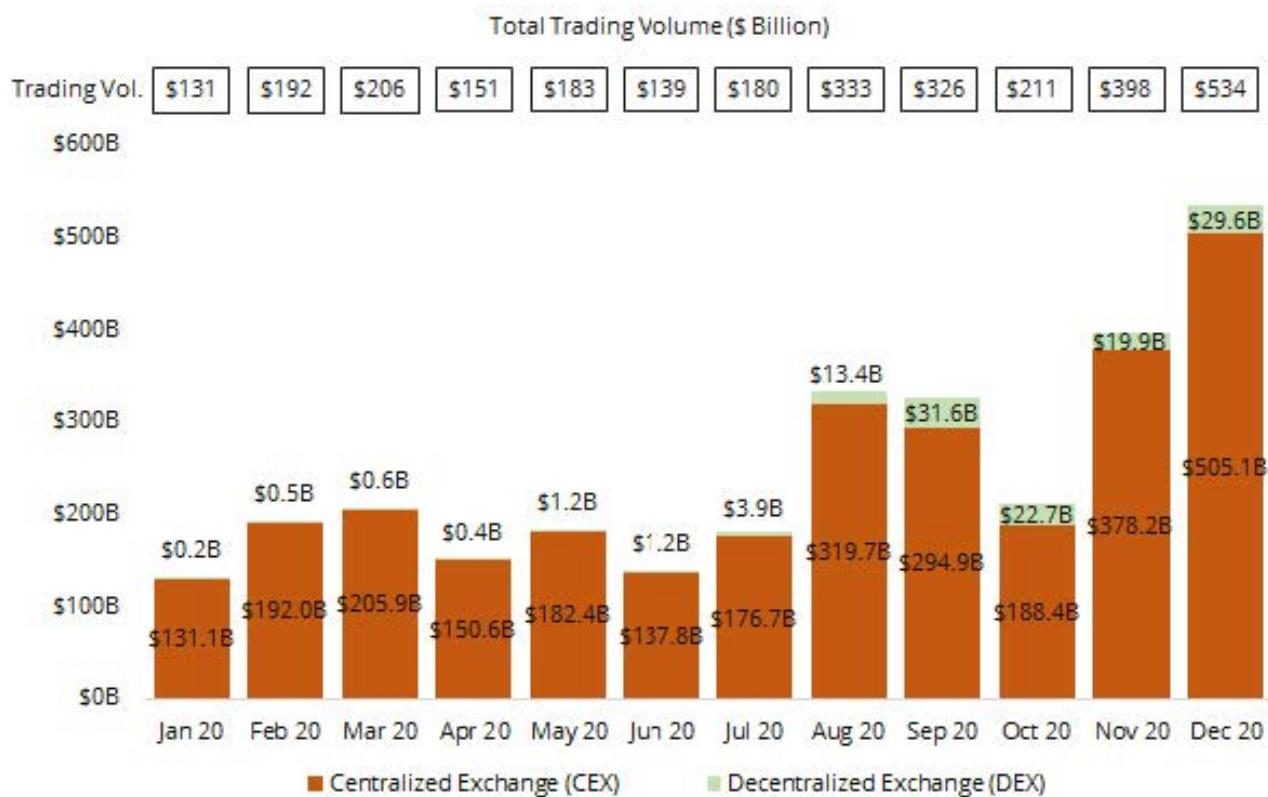
ЧАСТЬ ВТОРАЯ: ОЦЕНКА СЕКТОРОВ DEFI

ГЛАВА 3: ДЕЦЕНТРАЛИЗОВАННЫЕ БИРЖИ

Независимо от того, пытаетесь ли вы совершить простой обмен или активно торгуете, вам потребуются услуги биржи. В идеале биржа должна иметь низкую задержку и высокую ликвидность, чтобы у вас было лучшее исполнение цены и на вас не влияло проскальзывание цены.

Исторически сложилось так, что централизованные биржи (CEX) обеспечивали лучшую ликвидность и облегчали большинство крупных сделок. Однако у них есть несколько слабых мест - наиболее заметным из них является тот факт, что пользователи централизованных бирж на самом деле не владеют своими активами на бирже. Например, в сентябре 2020 года KuCoin пострадал от взлома на 281 миллион долларов после выявленной бреши в системе безопасности. CEX также могут остановить торговлю и заблокировать вывод средств пользователями в любое время.

В 2020 и 2021 годах децентрализованные биржи (DEX) быстро росли и начали конкурировать со своими централизованными аналогами. Соотношение топ-9 бирж DEX-CEX было всего с 0,2% в январе 2020 года и взлетело до 5,9% в декабре 2020 года. В 2020 году топ-9 DEX зафиксировали экспоненциальный рост объема торгов на 17,989% до 30 миллиардов долларов.



Но что именно делает DEX ... децентрализованной биржей?

DEX – это платформа, которая позволяет торговать и напрямую обменивать токены без необходимости в посреднике (т.е. в централизованном обмене). Вам не нужно проходить через тернии, связанные с процессами «Знай своего клиента» (KYC – Know Your Customer), и вы не подпадаете под юрисдикционные ограничения.

Типы децентрализованных бирж (DEX)

Существует два типа DEX:

1. DEX на основе ордеров (заказов)

Ордера – это список заказов на покупку и продажу определенного актива по различным уровням цен.

DEX на основе ордеров, такие как dYdX, Diversifi и Loopring, работают аналогично CEX, где пользователи могут устанавливать заказы на покупку и продажу либо по выбранным ими предельным ценам, либо по рыночным ценам. Основное различие заключается в том, что в CEX активы для торговли хранятся на кошельках бирж, в то время как для DEX активы для торговли хранятся на кошельках пользователей.

Ордера для DEX могут быть организованы как на блокчейне, так и вне его. В первом случае, DEX на основе ордеров все заказы записывает в блокчейн. Однако это больше нереально на Ethereum из-за высоких цен на газ. Тем не менее, это по-прежнему выполнимо в решениях Ethereum уровня 2, таких как xDai, или в блокчейнах с высокой пропускной способностью уровня 1, таких как Solana.

DEX, основанные на ордерах вне блокчейна, записывают временно их за пределами блокчейна. Ордера остаются вне блокчейна до тех пор, пока они не будут исполнены, после чего сделки выполняются в блокчейне. Хотя этот подход имеет меньшую задержку, некоторые могут утверждать, что DEX, использующие этот метод, считаются полу-децентрализованными (semiDEX – sDEX).

2. DEX на основе пула ликвидности

Пулы ликвидности – это резервы токенов, которые находятся в смарт-контрактах DEX и доступны пользователям для обмена токенами. В большинстве DEX, основанных на пуле ликвидности, используются автоматизированные маркетмейкеры (AMM), являющиеся математической функцией, которая алгоритмически определяет цены активов в зависимости от спроса и предложения.

AMM – одно из самых инновационных изобретений DeFi за последние годы. Это обеспечивает круглосуточное функционирование рынка, более высокую доступность капитала и эффективность. Существуют различные типы AMM, и разные DEX реализовали различные алгоритмы. Большинство DEX, выпущенных

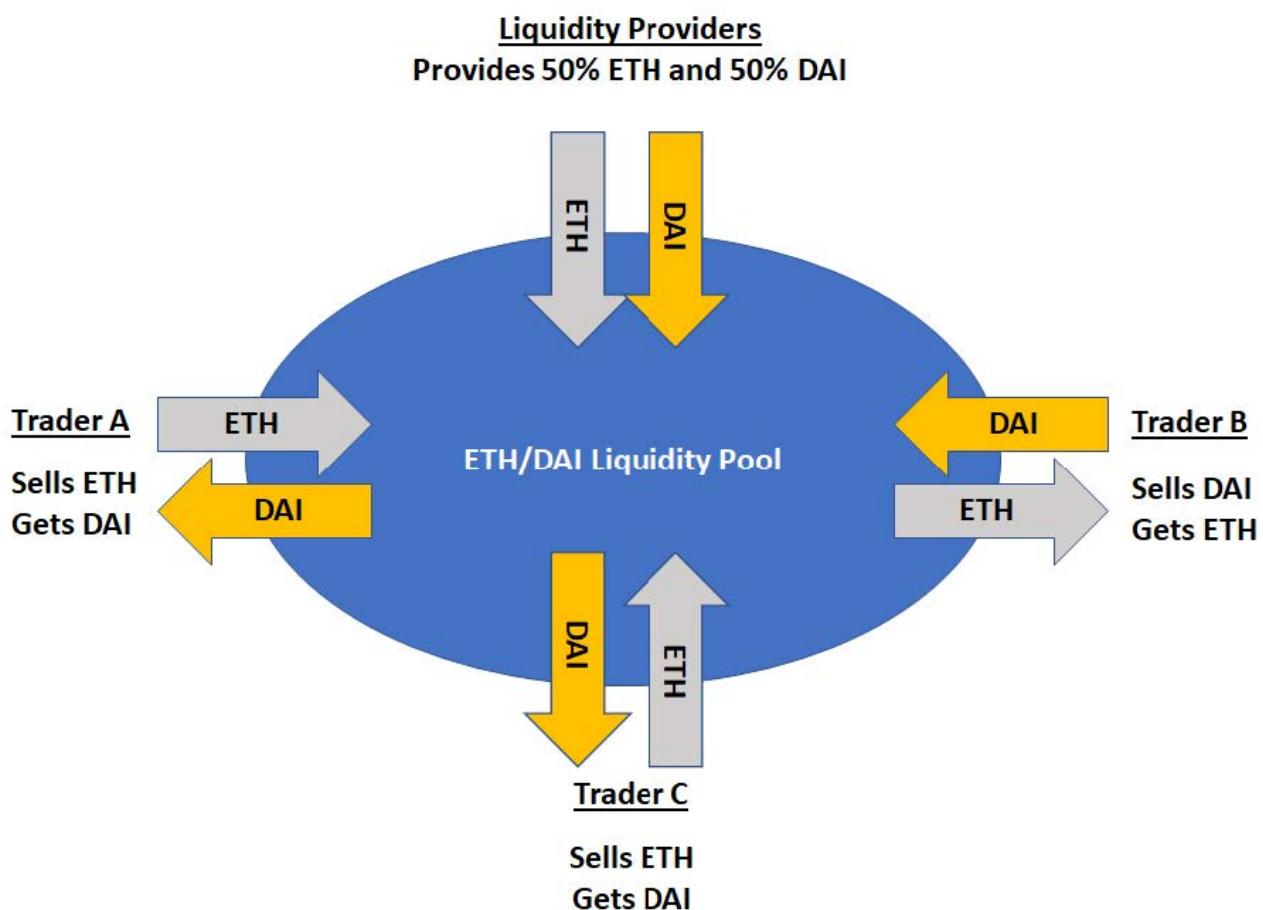
летом DeFi 2020 года, основаны на AMM, таких как Uniswap, Sushi Swap, Curve, Balancer и Bancor.

Поскольку многие из новых DEX основаны на AMM, в остальной части этой главы мы сосредоточимся на конкретных примерах AMM.

Автоматизированные маркетмейкеры (AMM)

В нашей книге «Что такое DeFi: Курс для новичков» мы рассмотрели Uniswap, самый популярный AMM. Вот краткое описание того, как работают пулы ликвидности в AMM.

В отличие от централизованных бирж, на которых заявки и запросы размещаются в ордерах, у AMM нет никаких ордеров. Вместо этого AMM полагается на пулы ликвидности. Пулы ликвидности – это, по сути, резервы, в которых хранятся два или более токенов, находящихся в смарт-контракте DEX, которые доступны пользователям для торговли.



Можно рассматривать пулы ликвидности как просто пулы токенов. Если вы хотите обменять ETH на DAI, вы будете торговать в пуле ликвидности ETH/DAI, добавив ETH и удалив сумму DAI, определенную алгоритмически, из пула ликвидности.

Вкладчики, называемые провайдерами ликвидности (LP), создают эти пулы ликвидности. Провайдеры ликвидности размещают свои токены в пул ликвидности на основе предопределенных отношений токенов для каждого АММ (в случае Uniswap – 50% для каждого токена, т.е. в равных долях).

Провайдеры ликвидности предоставляют средства в пулах ликвидности для того, чтобы получать доход от своих средств, за счет комиссий с пользователей, торгующих на DEX. Любой желающий может стать провайдером ликвидности, автоматически создавая торговую пару на рынке, внося свои средства в смарт-контракт.

С помощью АММ трейдеры могут беспрепятственно выполнять свои заказы без необходимости в централизованном маркетмейкере, обеспечивающем ликвидность на централизованной бирже, такой как Coinbase или Binance. Вместо этого, ордера исполняются автоматически с помощью смарт-контракта, который будет алгоритмически рассчитывать стоимость, включая любое проскальзывание при исполнении сделки. Таким образом, можно рассматривать обмен на основе ордеров как P2P-модели (взаимодействие человека с человеком), в то время как АММ является моделью взаимодействия человека с контрактом.

Какие существуют типы АММ?

АММ – это математическая функция для определения стоимости активов, алгоритмически основанная на пуле ликвидности. В настоящее время для удовлетворения различных стратегий ценообразования активов используется несколько формул АММ.

Рассмотрим некоторые из наиболее популярных формул АММ:

I. Маркетмейкер на основе постоянного значения произведения

$$x * y = k$$

Формула маркетмейкера на основе постоянного значения произведения количества токенов была впервые популяризована Uniswap и Bancor и стала самым популярным АММ на рынке. При построении графика это выпуклая кривая, где x и y представляют собой количества соответствующих токенов в пуле ликвидности, а k представляет произведение. Формула помогает создать диапазон цен на два токена в зависимости от доступного количества каждого токена.

Чтобы держать значение k неизменным, АММ действует так: когда предложение x увеличивается, предложение y уменьшается, и наоборот. Таким образом, результирующая цена по своей сути нестабильна, поскольку размер сделок может повлиять на цену в зависимости от размера пула. Непостоянные потери могут возникнуть из-за более высокого проскальзывания, вызванного крупными сделками.

II. Маркетмейкер на основе постоянного значения суммы

$$x + y = k$$

Формула маркетмейкера на основе постоянного значения суммы является прямой линией при построении графика. Это идеальная модель для торговли с нулевым проскальзыванием, но, к сожалению, не обеспечивает бесконечной ликвидности. Эта модель несовершенна, поскольку она предоставляет возможность арбитража, когда котируемая цена отличается от рыночной цены актива, торгуемого в другом месте. Арбитражеры могут истощить все резервы в пулах ликвидности, не оставляя больше доступной ликвидности для других трейдеров. Эта модель непригодна для большинства случаев использования АММ.

III. Маркетмейкер на основе постоянного среднего значения

$$\nu = \prod_t B_t^{w_t}$$

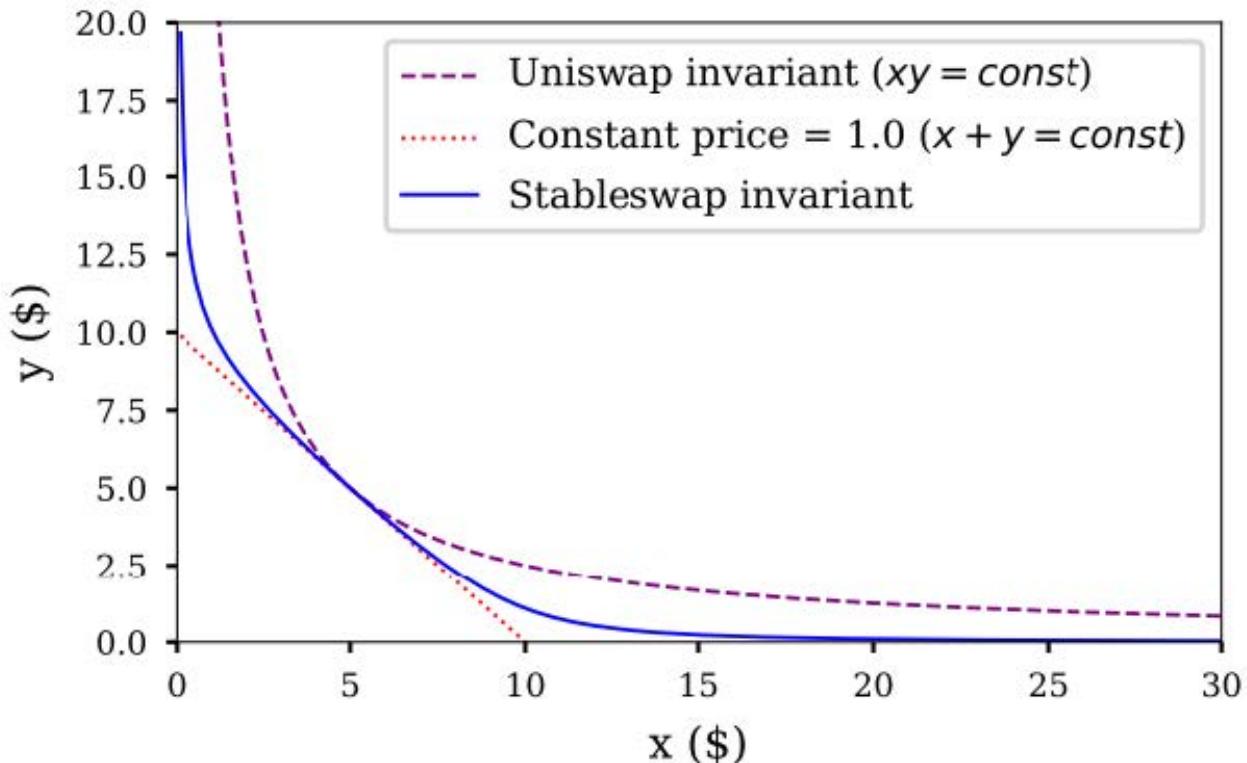
Формула маркетмейкера на основе постоянного среднего значения, или также известная как функция ценности, стала популярной благодаря Balancer. Это позволяет создавать пулы ликвидности с более чем двумя токенами и различными соотношениями токенов, выходящими за рамки стандартного распределения 50/50. Вместо произведения, неизменным остается средневзвешенное геометрическое значение. Это позволяет сохранять баланс различных активов в пуле и позволяет осуществлять обмен между любыми активами пула ликвидности.

IV. Гибридный маркетмейкер

$$An^n \sum X_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

Формула гибридного маркетмейкера представляет собой соединение формулы постоянного произведения и постоянной суммы. Она стала популярным благодаря Curve Finance.

Торговля происходит по кривой постоянной суммы, когда портфель относительно сбалансирован, и переключается на постоянное произведение, когда она не сбалансирована. Это позволяет снизить проскальзывание и непостоянные потери, но применимо только к активам с близкой стоимостью, поскольку цена желаемого торгового диапазона всегда близка к 1. Например, это будет полезно для торговли между стейблкоинами (DAI и USDC) и обернутыми активами (wBTC и sBTC).



На этом графике показаны кривые постоянного произведения (фиолетовая пунктирная линия), постоянной суммы (красная линия из точек) и гибридной кривой, используемой Curve Finance (синяя сплошная линия) в середине. Мы видим, что гибридная кривая свопа создает более глубокую ликвидность рядом с кривой постоянной суммы. Результатом является кривая, которая возвращает линейный обменный курс для большинства сделок и экспоненциальные цены для более крупных сделок.

Как определяются цены в формуле АММ на основе постоянного значения произведения?

Давайте рассмотрим простой пример данного типа АММ – как алгоритмически определяются цены на активы. Он работает, поддерживая постоянным значение произведения количества активов, доступных для каждого актива в пуле.

Посмотрим, как это работает, с помощью популярного АММ на основе постоянного значения произведения, который популяризировал Uniswap:

Важно отметить, что рыночная цена на АММ меняется только при изменении коэффициента резервирования активов в пуле. Таким образом, цена актива на АММ может отличаться от других бирж.

Пример

Формула маркетмейкера

$$x * y = k$$

x = количество токенов x в пуле

y = количество токенов y в пуле

k = постоянная общей ликвидности, которая определяет цену токенов в пуле ликвидности

Например:

По состоянию на 21 апреля 2021 года в пуле ликвидности DAI/ETH Uniswap насчитывалось 61 404 818 DAI и 26 832 ETH.

Коэффициент резервирования означает, что цена ETH на тот момент составляет $61\,404\,818\,DAI / 26\,832\,ETH = 2\,289\,DAI$.

Предположим, что 1 ETH теперь оценивается в 2289 DAI на Uniswap. Но когда цена падает до 2100 DAI в другом месте, например, на Balancer, появляется возможность арбитража. Арбитражеры воспользуются разницей в ценах, купив дешевый ETH на Balancer и продав его на Uniswap для быстрой прибыли (для простоты расчетов не будем учитывать комиссию за обмен). Арбитражеры будут повторять это до тех пор, пока цена не достигнет равновесия между двумя биржами.

Различные автоматизированные маркетмейкеры (AMM)

Uniswap



Uniswap – это децентрализованный протокол обмена на Ethereum, который позволяет осуществлять прямые обмены токенами, не храня ваши средства в бирже. Чтобы использовать Uniswap, все, что вам нужно сделать, это отправить свои токены из кошелька в смарт-контракт Uniswap, и взамен вы получите желаемые токены в своем кошельке.

Путешествие Uniswap началось в ноябре 2018 года, когда он запустил свою первую итерацию, Uniswap версии 1. Это один из первых DEX на базе АММ, который популяризировал формулу маркетмейкеров на основе постоянного значения произведения:

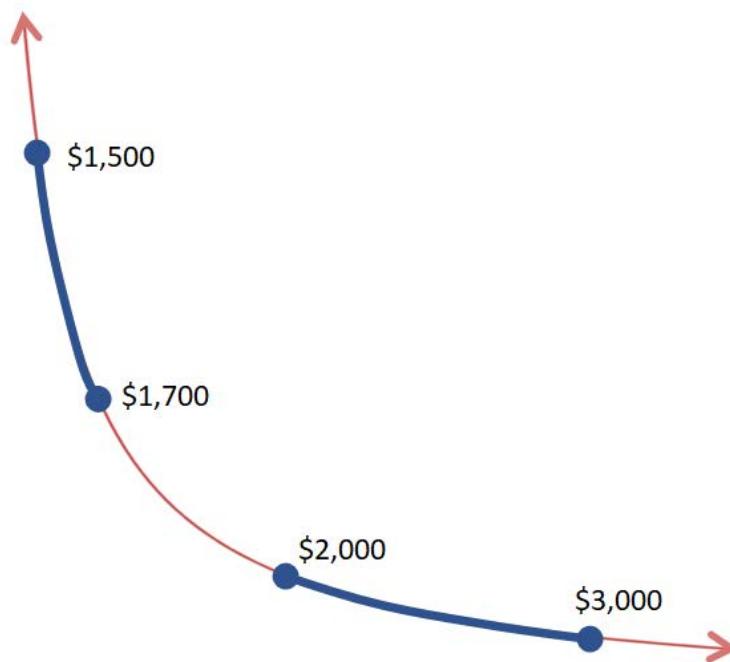
$$x * y = k$$

В мае 2020 года Uniswap обновил свой смарт-контракт до версии 2 с дополнительными функциями. Новая версия расширила торговые пары для поддержки любых токенов ERC-20.

5 мая 2021 года Uniswap выпустила последнюю версию Uniswap версии 3. В последней итерации Uniswap представила две основные новые функции:

1. Концентрированная ликвидность

С Uniswap версии 3 провайдеры ликвидности могут контролировать ценовые диапазоны, в которых они хотели бы предоставить ликвидность. Например, для пула ликвидности ETH/DAI может предоставить 30% своего капитала в ценовом диапазоне от 2000 до 3000 долларов, а оставшиеся 70% – в ценовом диапазоне от 1500 до 1700 долларов.



Новое активное управление ликвидностью в Uniswap версии 3 теперь обеспечивает более высокую эффективность использования капитала для провайдеров ликвидности. Побочным результатом этого является то, что провайдеры ликвидности получают неизменяемые токены (NFT) вместо взаимозаменяемых токенов ERC-20, представляющих их позиции.

2. Несколько уровней комиссии в пулах

Uniswap версии 3 предлагает три варианта комиссии в пуле, которую провайдеры ликвидности могут выбрать:

- a. 0,05%
- b. 0,30%
- c. 1,00%

Например, торговая пара USDC/DAI имеет низкую волатильность цен и может гарантировать более низкую комиссию за пул в размере 0,05%. Торговая пара ETH/DAI имеет более высокую волатильность цен и гарантирует комиссию за пул в размере 0,30%. Между тем, комиссия за пул в размере 1,00% может быть более подходящей для более волатильных или экзотических торговых пар.

SushiSwap



Протокол SushiSwap был запущен 28 августа 2020 года разработчиком под псевдонимом шеф-повар Номи. Это был форк исходного кода Uniswap версии 2 и использовал ту же модель маркетмейкера на основе постоянного значения произведения. SushiSwap ввел токен SUSHI в то время, когда Uniswap еще не имел своего токена UNI. Привлекательные вознаграждения за фарминг, предлагаемые SushiSwap, привлекли внимание многих людей в криптосообществе.

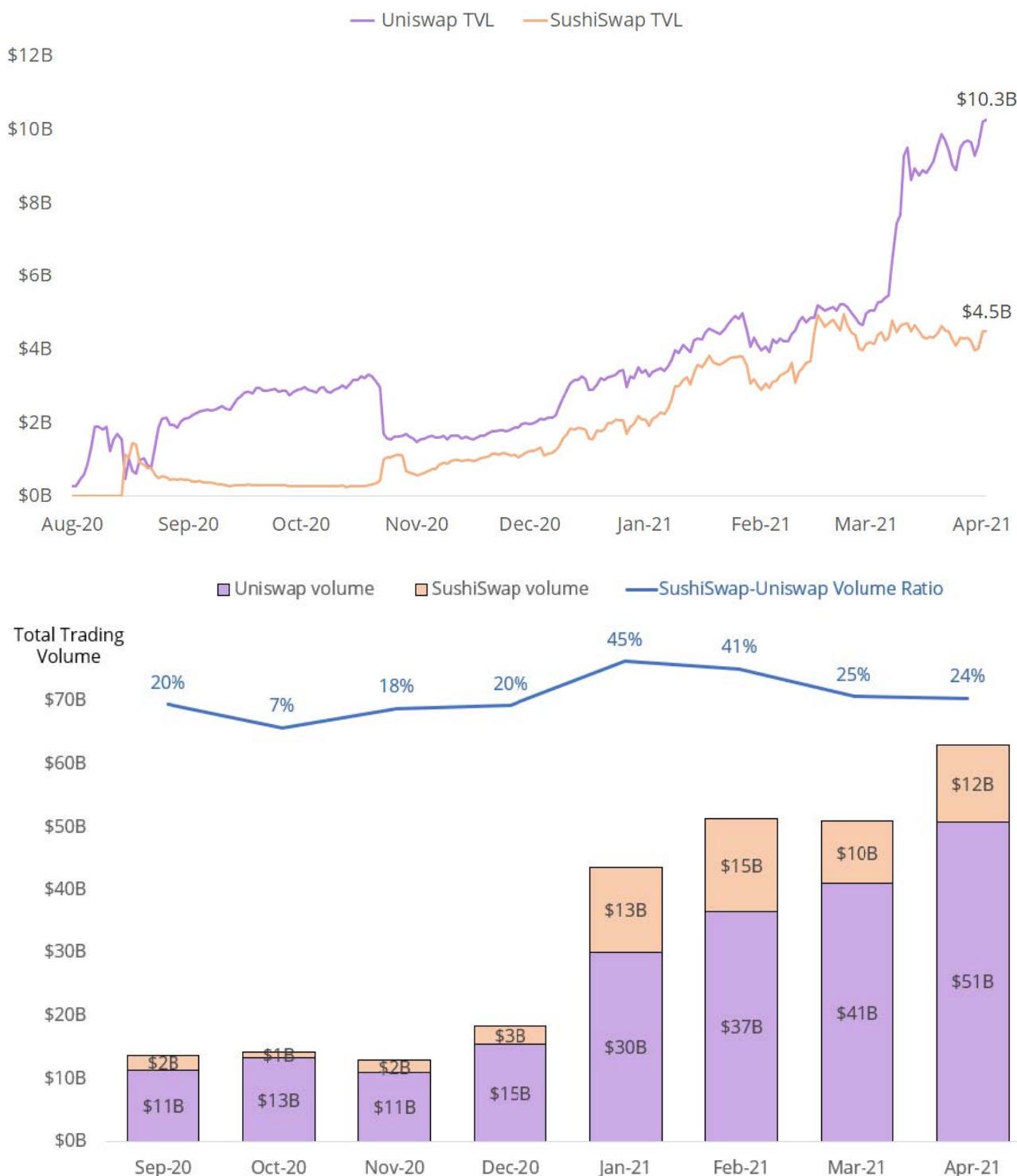
9 сентября 2020 года SushiSwap начал так называемую «атаку вампирского майнинга» на ликвидность Uniswap, в результате которой большая часть ликвидности Uniswap была перенесена на SushiSwap. Эта атака истощила более половины ликвидности Uniswap, и ее общая стоимость (TVL) упала с 1,55 миллиарда долларов до 470 миллионов долларов. Одновременно, TVL SushiSwap за ночь вырос до 1,13 миллиарда долларов.

Несмотря на «атаку вампирского майнинга», Uniswap сохранил устойчивость и очень быстро восстановил свое лидерство в TVL над SushiSwap. По состоянию на апрель 2021 года у SushiSwap сейчас 4,5 миллиарда долларов в TVL, что составляет почти половину от 10,3 миллиарда долларов в TVL Uniswap.

SushiSwap значительно вырос и в настоящее время является вторым по величине DEX после Uniswap. По состоянию на март 2021 года объем торгов Uniswap в четыре раза превышает объем торгов SushiSwap, что свидетельствует о

значительном лидерстве Uniswap на рынке DEX. В первые два месяца 2021 года SushiSwap показал высокие результаты и составил 45% от объема торгов Uniswap.

С момента своего запуска SushiSwap отличался тем, что предлагал более широкий ассортимент финансовых продуктов. Он также сотрудничал (объединился) с Yearn Finance, протоколом агрегатора фарминга, и теперь AMM является подразделением Yearn Finance. Ключевое различие между ними (Uniswap, SushiSwap) заключается в сборах за торговлю, доступных торговых парах и поддерживаемых блокчейнах.



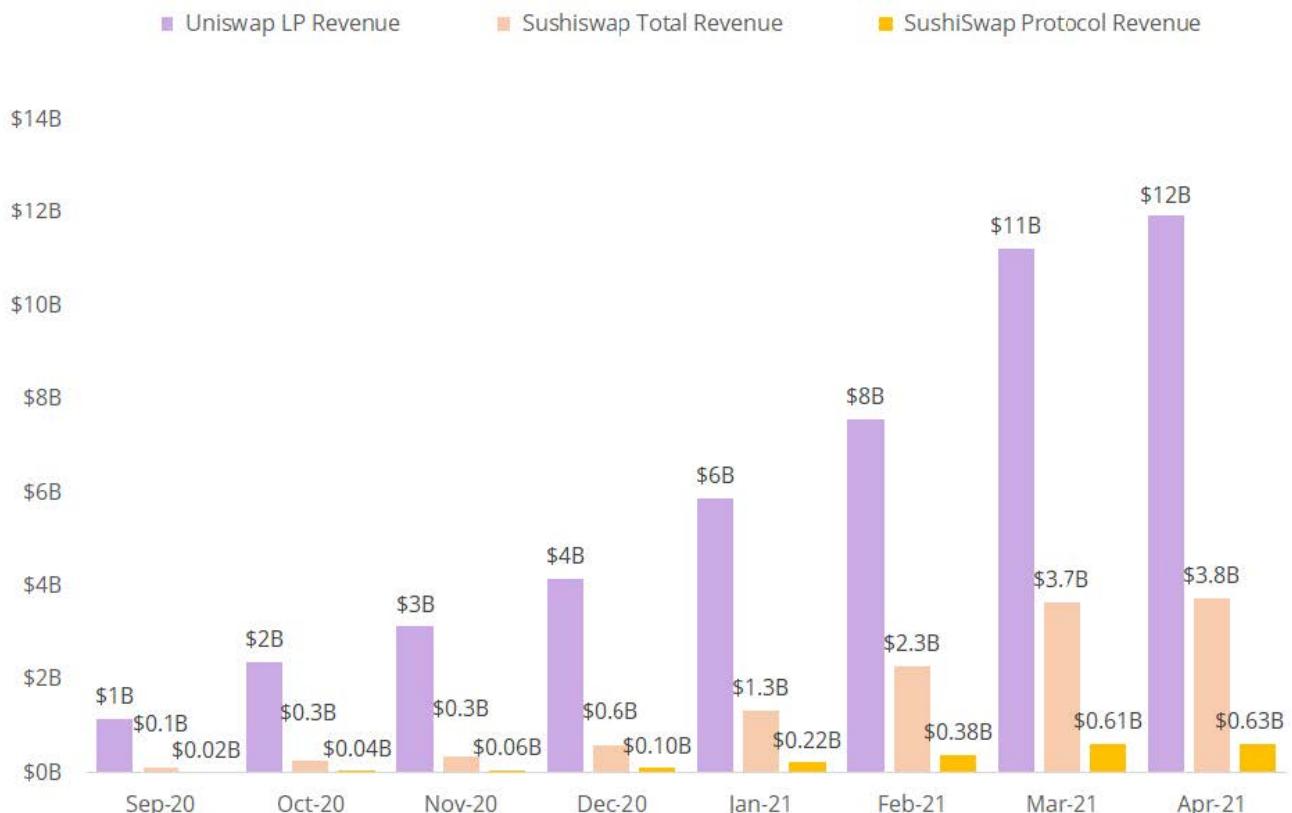
Параметры	Uniswap	SushiSwap
Тип комиссии	Фиксированная	Фиксированная
Торговые комиссии:	0,30 %	0,30 %
Идет протоколу	0,00 %	0,05 %
Идет провайдеру ликвидности	0,30 %	0,25 %

* на 1 апреля 2021 года

Из приведенной выше таблицы мы видим, что как Uniswap, так и SushiSwap имеют торговую комиссию в размере 0,3%. Однако в SushiSwap 0,05% от торговой комиссии поступает в протокол, который затем распределяется держателям токенов SUSHI.

Uniswap в настоящее время не распределяет сборы между держателями токена UNI, хотя это может быть активировано голосованием владельцев токенов UNI. По состоянию на апрель 2021 года провайдеры ликвидности Uniswap получают более высокую долю дохода (0,30%) по сравнению с SushiSwap (0,25%).

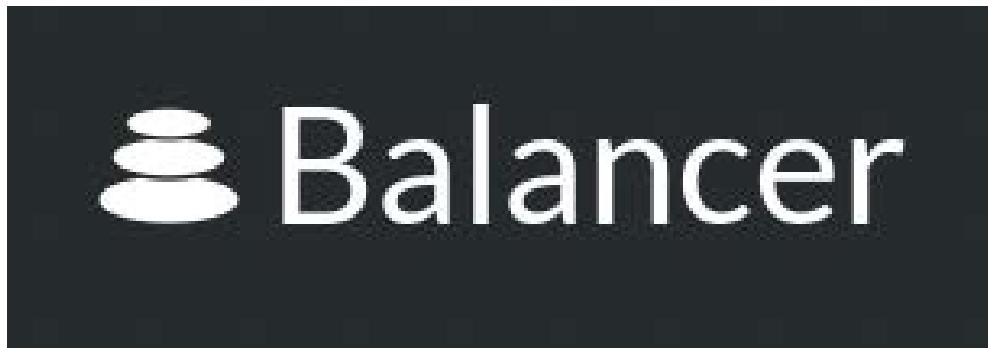
Из приведенной ниже диаграммы видно, что доходы от протоколов Uniswap и Sushiswap значительно выросли за последний год.



Uniswap также имеет более 2000 поддерживаемых торговых пар, что примерно в пять раз выше, чем SushiSwap, – это говорит о том, что на Uniswap поддерживается и торгуется больше токенов с низким уровнем объема торгов.

В настоящее время Uniswap поддерживает торговлю только на Ethereum с планами перехода на уровень 2 через Optimism. В свою очередь, SushiSwap работает на девяти различных блокчейнах, а именно Ethereum, Binance Smart Chain, Polygon, Fantom, Huobi Ecosystem, xDAI, Harmony, Avalanche и OKExChain.

Balancer



Balancer позиционирует себя как портфельный менеджер в дополнение к своему DEX на базе AMM. Вместо того, чтобы платить комиссионные за инвестиции в фонд, держатели пула Balancer собирают комиссионные с трейдеров, которые занимаются арбитражем пулов ликвидности. Это, по сути, создает индексный фонд, который получает дополнительный доход ребалансировке фонда, добавляя еще один источник дохода для провайдеров ликвидности.

В отличие от Uniswap, который поддерживает только два актива в одном пуле ликвидности, Balancer поддерживает пулы с несколькими активами. Создателям пула также разрешается устанавливать индивидуальные комиссии в диапазоне от 0,00001% до 10%. Эта гибкость открывает больше возможностей для создания пула.

Существует три типа пулов ликвидности:

1. **Публичный пул** – любой может добавить ликвидность, но параметры пула постоянно фиксированы. Это пул с наименьшим необходимым уровнем доверия к создателю.
2. **Частный пул** – гибкие параметры. Владелец – единственный, кто может изменять параметры и добавлять ликвидность. Это делает пул кастодиальным и централизованным.
3. **Смарт-пул** – любой может добавить ликвидность. Пул поддерживает фиксированные и динамические параметры, которые могут быть изменены на постоянной основе. Это самый гибкий пул.

Balancer версии 2 поддерживает до 16 различных активов в пуле и позволяет создавать смарт пулы. Смарт пулы особенно полезны для управления казначейством, где пулы могут действовать как механизм автоматического выкупа токенов. Плюс, это также позволяет предоставлять незанятые активы в протоколы кредитования, повышая доходность пулов.

Balancer также представил инновационный метод начальных предложений DEX (IDO), называемый пулами начальной загрузки ликвидности (LBP). Это недолговечные смарт-пулы с динамическими весами токенов с течением времени. Цена токена устанавливается по высокой цене и, как ожидается, будет падать на протяжении всей продажи. В этом случае «киты» и боты не склонны покупать токены с самого начала, что позволяет использовать более демократичный способ сбора средств.

Curve Finance



Curve Finance – это децентрализованная биржа на основе AMM, основной целью которой является облегчение обмена активами близкой стоимости. Это полезно в экосистеме DeFi, поскольку существует множество обернутых и синтетических токенов, которые стремятся имитировать цену базового актива. Curve Finance в настоящее время поддерживает стейблкоины в долларах США, Евро, обернутые/синтетические BTC и обернутые/синтетические ETH-активы.

Например, одним из крупнейших пулов ликвидности является 3CRV, пул стейблкоинов, состоящий из DAI, USDT и USDC. Соотношение трех стейблкоинов в пуле зависит от спроса и предложения на рынке. Внесение монеты с меньшим коэффициентом принесет пользователю более высокий процент от пула. Когда соотношение одной из монет существенно больше, это может послужить хорошим шансом для арбитража.

Curve Finance также поддерживает токены, приносящие доходность в Compound, Aave и Yearn Finance. Curve сотрудничала с Yearn Finance для выпуска пула yUSD, состоящий из токенов с доходностью yDAI, yUSDT, yUSDC, и yTUSD. Пользователи, участвовавшие в этом пуле, получают доходность от базовых токенов, комиссионные за обмен, генерируемые пулом Curve, и вознаграждения в виде CRV за предоставление ликвидности в Curve Finance. Провайдеры ликвидности этого пула могут зарабатывать из трех источников дохода.

Чтобы повысить ликвидность токенов с низким уровнем объема торгов, Curve представила концепцию базовых пулов и метапулов. Метапул – это пул одного токена, присоединённый к базовому пулу, что позволяет пользователям беспрепятственно торговать токеном пула. В настоящее время наиболее ликвидным базовым пулом является пул 3CRV.

Например, существует метапул с UST (стейблкоином в долларах США, выпущенной на блокчейне Terra) с базовым пулом 3CRV. Пользователи могут торговать UST и тремя стейблкоинами в долларах США в пуле 3CRV. Разделяя базовый пул и метапул, Curve позволяет пулу 3CRV избежать системных рисков UST.

Создание мета-пулов помогает Curve:

- Предотвращать разбавление существующих пулов.
- Вносить неликвидные активы.
- Большой объём и торговые комиссии для держателей токенов CRV.

Bancor



Запущенный в 2017 году, Bancor был одной из первых децентрализованных бирж на базе АММ. Bancor использует маркетмейкер на основе постоянного значения произведения, аналогичный Uniswap. Но подход Bancor отличается от произвольной формулы кривой с двумя активами, используемой Uniswap.

Вместо сопряжения базового токена с любым целевым токеном ERC-20, как это реализовано в Uniswap, Bancor использует свой собственный токен, Bancor Network Token (BNT), в качестве промежуточной валюты. Для каждого токена, торгуемого с BNT, существуют отдельные пулы.

Bancor в версии 2 вводит несколько инноваций, таких как односторонний стейкинг и страхование от непостоянных потерь.

Большинство АММ требуют, чтобы провайдеры ликвидности обеспечивали равное соотношение каждого актива, представленного в пуле. Это доставляет неудобства провайдерам ликвидности, которые хотят внести только один актив в пул. Версия 2 Bancor позволяет провайдерам ликвидности вносить вклад в один актив и поддерживать 100%-ную долю в нем. Провайдеры ликвидности могут лонговать актив с односторонней ликвидностью, получая при этом комиссию за обмен и вознаграждение за добычу ликвидности.

Непостоянные потери – это риск, который касается большинства провайдеров ликвидности на АММ. Bancor стимулирует ликвидность, предлагая компенсацию за любые непостоянные убытки. Начиная с первого дня вложения ликвидности, выплата увеличивается на 1% каждый день и достигает 100% через 100 дней. Это покрытие убытков побуждает провайдеров ликвидности оставаться в пуле

ликвидности не менее 100 дней. Существует 30-дневный срок ожидания, прежде чем сработает защита от непостоянных потерь.

Bancor также представила vBNT и Vortex для улучшения вариантов использования токенов BNT. Пользователи получают vBNT при размещении BNT в пуле Bancor из белого списка. Обменный курс BNT к vBNT составляет 1:1. vBNT может использоваться для нескольких функций:

- Голосование в управлении Bancor.
- Получение доли комиссий в пуле vBNT/BNT за обмен.
- Займы других токенов на Bancor, используя vBNT в качестве обеспечения (Vortex).

Vortex позволяет держателям BNT занимать под свои застейканные BNT. Полученные средства могут быть использованы как плечо или для любых других целей, повышающих эффективность капитала холдинга BNT.

Каковы различия между АММ?

Теперь, когда вы знакомы с различными видами АММ на рынке, давайте рассмотрим три признака, которые делают каждый АММ особенным. Для простоты мы сосредоточимся на Uniswap v2, Curve, Balancer и Bancor.

I. Комиссии пула

Чтобы стимулировать пользователей к увеличению ликвидности, децентрализованные биржи позволяют провайдерам ликвидности получать комиссионные за торговлю на своей платформе. Комиссии помогают провайдерам ликвидности справляться с колебаниями цен и непостоянными потерями.

Ниже приведена сводка комиссий пулов для четырех DEX в апреле 2021 года:

Параметры	Uniswap	Curve	Balancer	Bancor
Тип комиссии	Фиксированная	Фиксированная	Переменная	Переменная
Комиссии пула:	0,30 %	0,04 %	от 0,0001 % до 10 %	До 5 % *
Идет протоколу	0,00 %	0,02 %	Зависит от пула и может быть нулевой	0,00 % **
Идет провайдеру ликвидности	0,30 %	0,02 %	от 0,0001 % до 10 %	До 5 % *

* Комиссия за торговлю контролируется создателем пула. Самая высокая плата по состоянию на 26 апреля 2021 года составляла 5%.

*** Начисленная комиссия, которая поступает в протокол, используется в качестве страхования от непостоянных убытков, а не в качестве дохода. Комиссия будет сожжена, как только будет произведен вывод активов из пула ликвидности.*

Uniswap и Curve ввели фиксированную торговую комиссию за каждый swap, сделанный на их платформах. Основное различие заключается в разделении – Uniswap предоставляет всю торговую плату провайдерам ликвидности, в то время как Curve делит торговую плату поровну между протоколом и провайдерам ликвидности.

Для Balancer и Bancor торговые сборы являются переменными и контролируются только создателем пула.

II. Майнинг ликвидностью

Мы затронули эту концепцию в главе 2. Вкратце, майнинг ликвидностью относится к процессу предоставления ликвидности протоколу, а взамен провайдер ликвидности вознаграждается собственными токенами протокола.

Это один из самых популярных способов загрузки ликвидности на DEX и компенсации провайдерам ликвидности за риск непостоянных потерь.

У каждого из четырех DEX есть свой собственный токен:

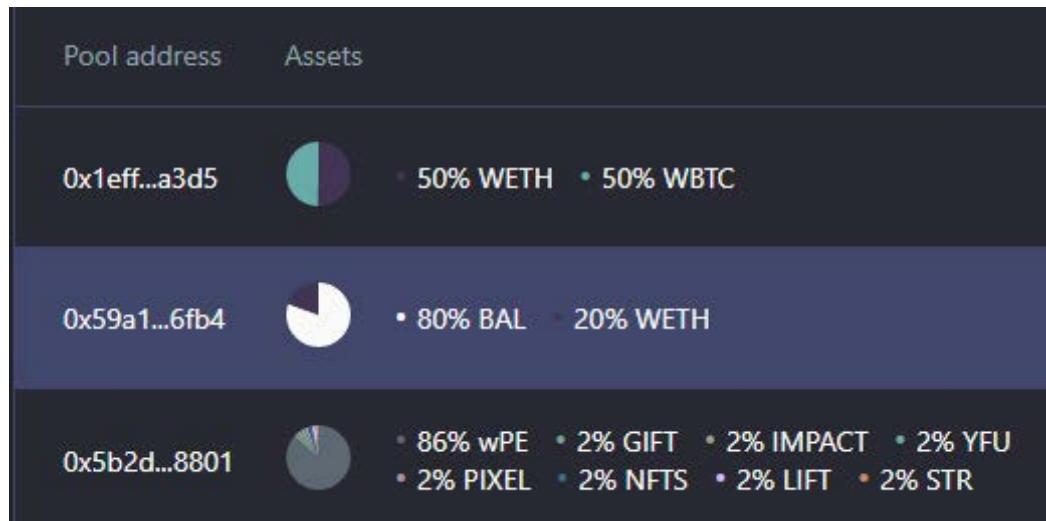
Protocol	Coin name	Ticker
	Uniswap	UNI
	Curve Dao Token	CRV
	Balancer	BAL
	Bancor Network Token	BNT

По состоянию на 1 апреля 2021 года Uniswap является единственной компанией без активной программы майнинга ликвидности из четырех DEX.

III. Веса активов в пуле

Большинство AMM, таких как Uniswap и Bancor, имеют стандартный баланс пула 50/50, в соответствии с которым провайдеры ликвидности должны предоставлять равную стоимость двух токенов. Однако Balancer имеет переменные критерии баланса пула, а Curve имеет динамические критерии баланса пула.

В Balancer пользователи могут устанавливать переменные веса для каждого пула. Пулы постоянно ребалансируются, чтобы гарантировать, что они соответствуют заданному набору весов. Например, пул 80/20 BAL/WETH на Balancer означает, что вам придется разделить свой капитал на 80% токенов BAL и 20% токенов WETH при обеспечении ликвидности в пуле.



В Curve веса пула являются динамическими и меняются в зависимости от наличия активов в пуле. В отличие от других AMM, Curve не ребалансирует свои пулы и не пытается поддерживать их в сбалансированном соотношении.

Давайте рассмотрим пример пула CRV, состоящего из DAI, USDC, и USDT. В идеале этот пул имеет одинаковый вес между тремя стейблкоинами. Однако на представленном ниже рисунке присутствует USDC с наибольшим весом (41,98%) и DAI с наименьшим весом (24,80%). Если вы заинтересованы в предоставлении ликвидности этому пулу, вам не нужны все три токена, а просто добавьте любой из трех токенов в пул. Поступая таким образом, вы будете динамически изменять вес пула.



Риски, связанных с использованием АММ

I. Ценовое проскальзывание

Основываясь на формулах АММ, котируемая цена зависит от соотношения запасов токенов.

В формуле маркетмейкера на основе постоянного значения произведения ($x * y = k$), чем больше ордер, тем больше проскальзывание цены. Проскальзывание зависит от размера пулов ликвидности – пулы с более низкой ликвидностью будут страдать более высокими ценовыми проскальзываниями при крупных ордерах.

Предположим, что текущая цена ETH/DAI составляет 2000 долларов, а начальная пара ликвидности имеет 62 500 000 DAI и 25 000 ETH. Это даст нам произведение в размере 1,56 миллиарда. Приведенная ниже таблица иллюстрирует ценовое проскальзывание или наценку, которую вам придется заплатить по мере увеличения размеров ваших транзакций.

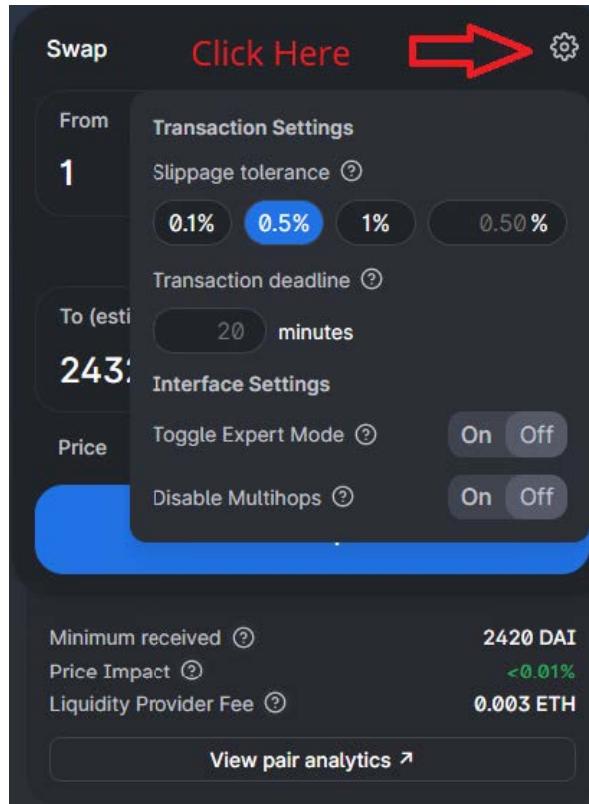
ETH Purchased	Cost per ETH in DAI	Total Cost in DAI	Premium	New DAI Reserve	New ETH Reserve	Product (k)
0	2,500			62,500,000	25,000	1,562,500,000,000
1	2,500.10	2,500	0.00%	62,502,500.10	24,999	1,562,500,000,000
10	2,501.00	25,010	0.04%	62,525,010.00	24,990	1,562,500,000,000
100	2,510.04	251,004	0.40%	62,751,004.02	24,900	1,562,500,000,000
1,000	2,604.17	2,604,167	4.17%	65,104,166.67	24,000	1,562,500,000,000
10,000	4,166.67	41,666,667	66.67%	104,166,666.67	15,000	1,562,500,000,000
20,000	12,500.00	250,000,000	400.00%	312,500,000.00	5,000	1,562,500,000,000
25,000	Infinity	Infinity	Infinity	Infinity	0	1,562,500,000,000

Вот еще один пример проскальзывания цены в Uniswap.

Пример

Исходя из ETH/DAI на Uniswap, 1 ETH стоит примерно 2433 в DAI.

Вы можете установить допустимое проскальзывание, перейдя в настройки транзакции. Uniswap устанавливает 0,5% по умолчанию:



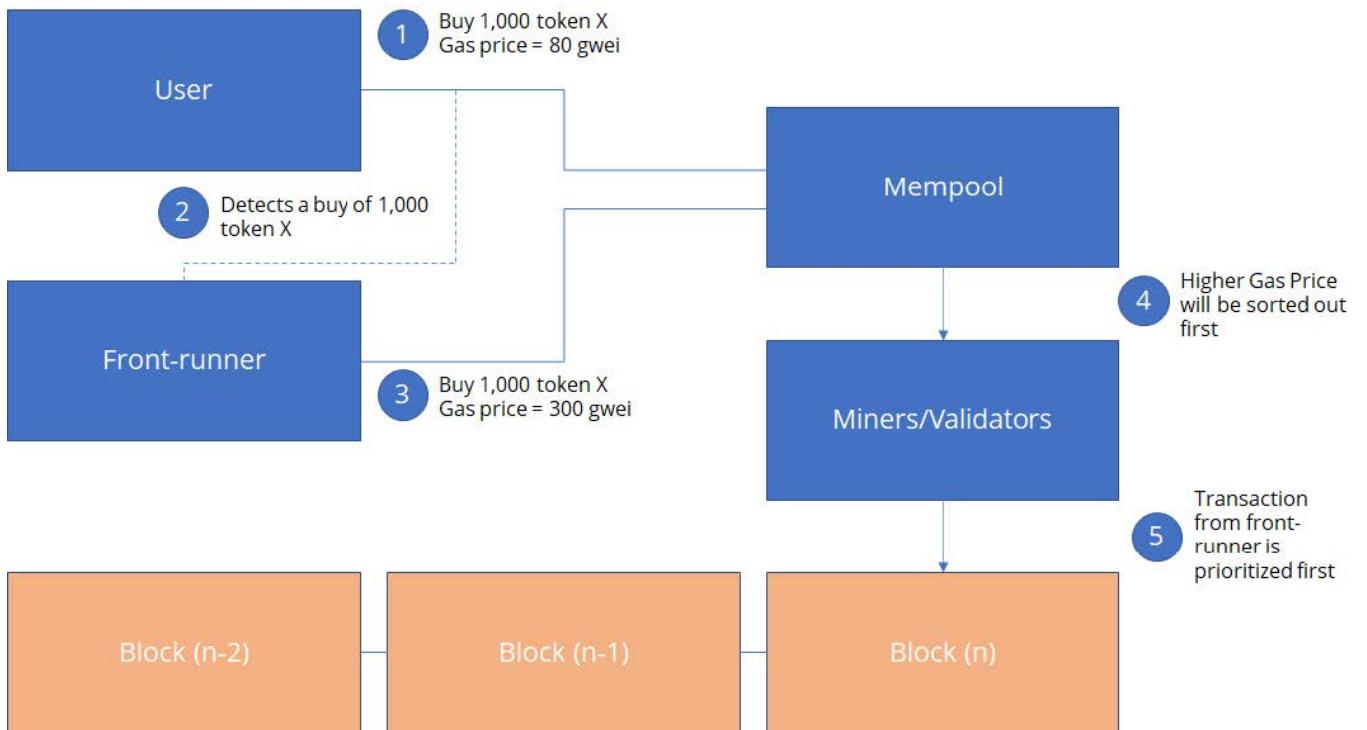
Обратите внимание на индикаторы в нижней части рисунка:

1. Минимальное полученное количество (Minimum Received) – это минимальное количество токенов, которое вы получите, исходя из вашего допустимого проскальзывания. Если ваш максимальное допустимое проскальзывание составляет 0,5%, то минимум, который вы получите, составляет $2433 \text{ DAI} * 0.95\% = 2420 \text{ DAI}$.
2. Влияние цены (Price impact) – это наценка, которую вам придется заплатить и которая будет учтена в отображаемой цене. Чем больше ваш ордер, тем больше будет влияние на цену.

II. Фронтраннинг

Поскольку ордера, сделанные на АММ, транслируются в блокчейн для всеобщего обозрения, любой может отслеживать блокчейн, чтобы подобрать подходящий ордер и зафронтранить его, установив более высокую комиссию за транзакцию, чтобы он выполнился быстрее, чем исходный ордер. А после выполнения атакуемого ордера, фронтраннер выполняет обратную операцию (это безрисковый арбитраж). Данная операция, известна как «Сэндвич-атака».

Ниже приведена иллюстрация того, как это может произойти



Ниже приведен скриншот «Сэндвич-атаки», произошедшей с токеном управления Ampleforth (FORTH) на Uniswap.

③ Front-runner sell	0x0c3114c9	2 mins ago	Uniswap V2: FORTH-USDT	OUT	0x22c1b8ca9a0d05fed1c...	433.424154915555526553	
② Victim buy	Swap Exact Token...	2 mins ago	Uniswap V2: FORTH-USDT	OUT	0x000000005736775fb...	648.741261968609786766	
① Front-runner buy	0xd149d05c	2 mins ago	Uniswap V2: FORTH-USDT	OUT	0x9edd647d7d6ecea6b...	305.984006609607719949	
	0x0df40ba9def225c63ed...	Delegate	2 mins ago	Uniswap V2: FORTH-USDT	OUT	0x860bd2dba9cd475a61...	129.211794675432082889
	0x05045cbf111ee846150...	Swap Exact Token...	2 mins ago	Uniswap V2: FORTH-USDT	IN	0x91d9b0e26d9d3d7018...	614.568298998974378013
1 Additional Info	Success (9 Block Confirmations)	Transaction Action:	Swap 12,796.192465 USDT For 305.984006609607719949 FORTH On Uniswap	Transaction Fee:	0.01473385272014 Ether (\$35.45)	Gas Info:	116,739 Gas Used From 300,000 Gas Limit @ 0.000000126210201562 Ether (126.210201562 Gwei)
2 Additional Info	Success (9 Block Confirmations)	Transaction Action:	Swap 10,000 USDT For 231.342974191954118827 FORTH On Uniswap	Transaction Fee:	0.01323169016392 Ether (\$31.84)	Gas Info:	105,015 Gas Used From 300,000 Gas Limit @ 0.000000126000001561 Ether (126.0000001561 Gwei)
3 Additional Info	Success (9 Block Confirmations)	Transaction Action:	Swap 305.984006609607719949 FORTH For 13,088.332297 USDT On Uniswap	Transaction Fee:	0.01074686813313 Ether (\$25.86)	Gas Info:	85,291 Gas Used From 300,000 Gas Limit @ 0.000000126000001561 Ether (126.0000001561 Gwei)
	Nonce: 21889 (in the position 62)	Nonce: 1205 (in the position 63)	Nonce: 21889 (in the position 64)				FORTH Price = \$41.81 Front runner = buy ~ 306 FORTH for ~ 12,796 USDT Gas price = 126.2 Gwei (\$35.45)
							FORTH Price = \$43.29 Victim buy= buy ~ 231 FORTH for ~10,000 USDT Gas price = 126.0 Gwei (\$31.84)
							FORTH Price = \$42.77 Front runner = sold ~ 306 FORTH for ~ 13,088 USDT Gas price = 126.0 Gwei (\$25.86)
							Front-runner's cost = total gas = \$61.31 Profit = \$13,088 - \$12,796 - \$61.31 = \$230.69

Таким образом, фронтраннер заработал около 230 долларов США за счет атаки.

III. Непостоянные потери

Еще одним недостатком АММ являются непостоянные потери, которые происходят, когда вы предоставляете ликвидность АММ. Непостоянные потери по сути являются разницей между ценой при хранении активов в пуле по сравнению с хранением их в вашем кошельке.

Примечание: потерь не будет до тех пор, пока вы не удалите свои токены из пула ликвидности.

Чем выше расхождение между стоимостью хранения ваших токенов в пуле и кошельке, тем выше непостоянные потери.

Пример

Предположим, что вы создали пул ETH/DAI на Uniswap, предоставив 10 000 DAI и 5 ETH в пул.

- Цена 1 ETH = 2000 в DAI
- Пул состоит из 5 ETH и 10 000 DAI
- Ликвидность пула использует формулу постоянного произведения ($x * y = k$) → $5 * 10\,000 = 50\,000$

Скажем, цена удваивается до 4000 DAI.

- Арбитражеры будут изменять стоимость активов, указанных в Uniswap, до тех пор, пока она не достигнет 1 ETH = 4000 DAI.

- Пул будет балансировать до тех пор, пока он не будет соответствовать константе пула на уровне 50 000.
- Новое соотношение пула составит 3,536 ETH и 14 142 DAI

Чтобы рассчитать свой непостоянный убыток, вы можете вычесть прибыль от удержания вне пула и внутри пула.

При 1 ETH = 2000 DAI ваш первоначальный капитал (5 ETH и 10 000 DAI) оценивается в 20 000 DAI.

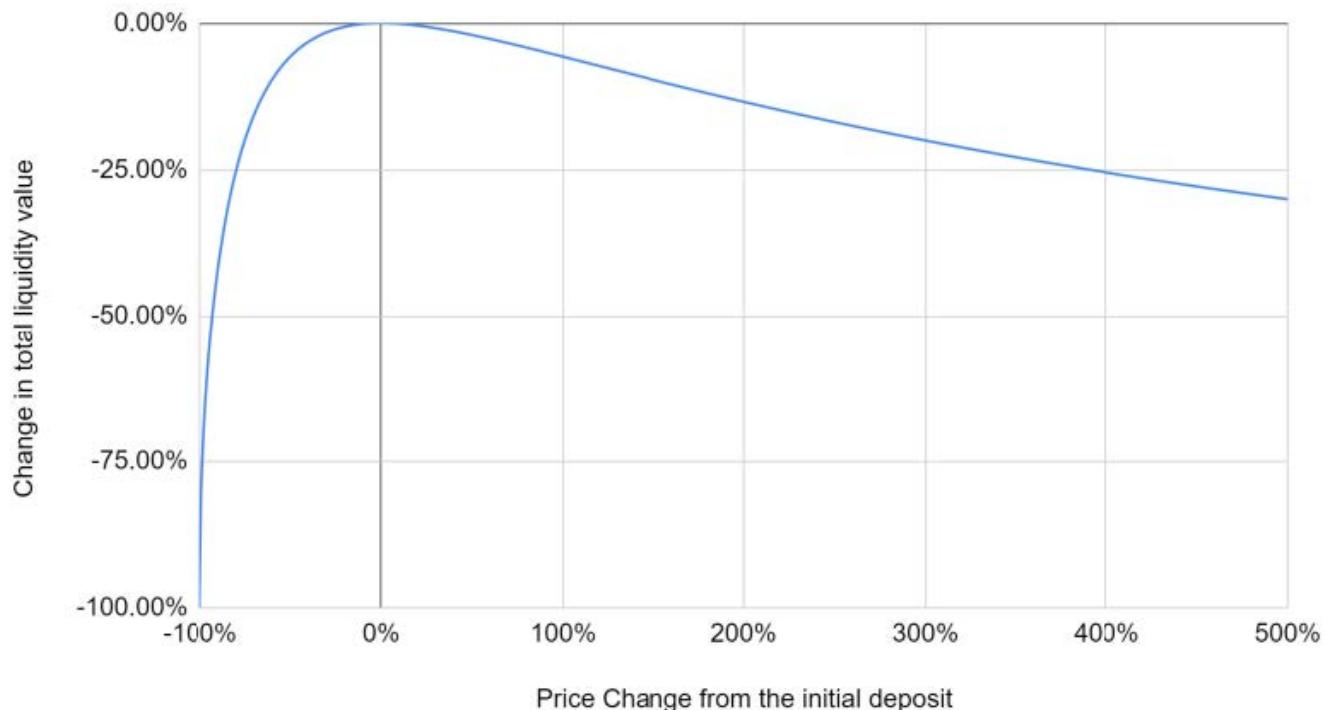
При 1 ETH = 4000 DAI

- При хранении активов в пуле:
 - Получаем $(3,536 \text{ ETH} * 4000 \text{ DAI}) + 14\,142 \text{ DAI} = 28,286 \text{ DAI}$
 - окупаемость инвестиций составляет +41% (без учета прибыли от комиссии)
- При хранении за пределами пула:
 - $(5 \text{ ETH} * 4000 \text{ DAI}) + 10\,000 \text{ DAI} = 30\,000 \text{ DAI}$
 - рентабельность инвестиций составляет +50%
- Таким образом, ваш непостоянный убыток составляет:
 - $30\,000 \text{ DAI} - 28,286 \text{ DAI} = 1716 \text{ DAI}$

Этот убыток будет только в том случае, если вы выведете свою ликвидность из Uniswap.

На графике ниже показана альтернативная стоимость, которую вы получите, если будете держать свои токены за пределами пула (HODL) и внутри пула.

Degree of divergence from holding tokens in liquidity pool (LP) vs. outside the pool (HODL)



- изменение цены в 1,25 раза = потеря 0,6% по сравнению с HODL
- изменение цены в 1,50 раза = 2,0% убытка по сравнению с HODL
- изменение цены в 1,75 раза = 3,8% убытка по сравнению с HODL
- 2-кратное изменение цены = 5,7% убытка по сравнению с HODL
- 3-кратное изменение цены = 13,4% убытка по сравнению с HODL
- 4-кратное изменение цены = 20,0% убытка по сравнению с HODL
- 5-кратное изменение цены = 25,5% убытка по сравнению с HODL

Таким образом, торговые пары, которые торгуются в небольшом ценовом диапазоне (например, стейблкоины), менее подвержены непостоянным потерям.

Децентрализованные биржи, заслуживающие упоминания



PancakeSwap

PancakeSwap – это форк (ответвление) Uniswap, но он построен на блокчейне Binance. Это самая крупная биржа среди АММ-бирж на Binance Smart Chain, и ее объем даже превышает объем Uniswap по состоянию на апрель 2021 года.



TerraSwap

TerraSwap существует в блокчейне Terra, и это единственный протокол DEX в блокчейне Terra. Вы можете выбрать, чтобы ваша торговая комиссия была представлена в любых активах блокчейна Terra.



0x Protocol

0x – это уровень инфраструктуры DEX с двумя основными предложениями: API взаимодействия с DEX, который позволяет проектам запускать DEX с белой этикеткой, и ориентированный на потребителя агрегатор DEX, называемый Matcha. Такие проекты, как Tokenlon, Metamask, Zapper и Zerion интегрировали 0x для запуска своих сервисов обмена.

Вывод

DEX'ы играют жизненно важную роль в создании пространства DeFi, поскольку они отражают текущее поведение рынка, особенно цены и ликвидность криптовалют. Они определяют стоимость различных криптовалют по отношению друг к другу и иллюстрируют динамичный характер сделок и движения капитала.

Рекомендуемая литература

1. Основы AMM

<https://defiweekly.substack.com/p/understanding-amms-the-basics-f30>

2. Типы AMM

<https://blog.chain.link/challenges-in-defi-how-to-bring-more-capital-and-less-risk-to-automated-market-maker-dexs/>

3. Понимание влияния стоимости в AMM

<https://research.paradigm.xyz/amm-price-impact>

4. Проблема фронтраннинга в Ethereum

<https://www.coindesk.com/new-research-sheds-light-front-running-bots-ethereum-dark-forest>

5. Uniswap V3

<https://uniswap.org/blog/uniswap-v3/>

ГЛАВА 4: АГРЕГАТОРЫ DEX

Ликвидность необходима для обеспечения возможности совершения сделок без серьезного влияния на рыночную цену. Рынок DEX чрезвычайно конкурентный, и несколько DEX конкурируют за пользователей и ликвидность. Таким образом, ликвидность часто является разрозненной и приводит к неэффективному управлению капиталом.

В то время как влияние на небольшие транзакции может быть несущественным, более крупные транзакции DEX будут подвержены более высокому проскальзыванию цен. Именно поэтому агрегаторы DEX помогают трейдерам получить лучшую цену используя различные DEX.

Агрегаторы DEX ищут наиболее экономически эффективные маршруты транзакций, объединяя ликвидность из разных DEX. Направляя одну транзакцию через несколько путей ликвидности, трейдеры, совершающие крупные сделки, могут воспользоваться преимуществами экономии газа и минимизировать стоимость ценового воздействия низкой ликвидности.

Мы кратко рассмотрели агрегаторы DEX в нашей книге «Что такое DeFi: для начинающих», используя 1inch в качестве примера. В следующем разделе мы рассмотрим новейшие агрегаторы DEX, такие как Matcha и Paraswap, и сравним эти протоколы.

Протоколы агрегаторов DEX

1inch Network



1inch Network – это агрегатор DEX, который ищет наиболее дешевые цены в нескольких источниках ликвидности. Первоначальный протокол включает в себя алгоритм Pathfinder, который ищет оптимальные маршруты между различными рынками. С момента своего создания в сети Ethereum, 1inch стал поддерживать блокчейны Binance и Polygon. Протокол агрегатора 1inch также претерпел два значительных обновления и с марта 2021 года находится в версии 3.

По состоянию на 31 мая 2021 года в Ethereum насчитывается более 50 источников ликвидности, более 20 источников ликвидности на блокчейне Binance и более 10 источников ликвидности в Polygon. Примечательно, что всего за два года агрегатор DEX 1inch превысил общий объем в 40 миллиардов долларов только в сети Ethereum.

В отличие от других агрегаторов DEX, 1inch имеет два собственных токена. Один – газовый токен (CHI), а другой – токен управления (1INCH).

CHI – это газовый токен, который способствует возмещению средств за хранилища данных в Ethereum. Газовые токены помогают смарт-контрактам удалять ненужные хранилища данных во время процесса транзакции и снижать плату за газ. Вы можете рассматривать CHI как купон на скидку, который можно использовать для удешевления ваших транзакций, позволяя пользователям экономить до 42% от своих сборов за газ.

Токен 1INCH, выпущенный в декабре 2020 года, способствовал превращению протокола в более децентрализованную организацию. Обладатели 1INCH голосуют за конкретные настройки протокола в рамках модели децентрализованной автономной организации (DAO). Модель управления позволяет инвесторам контролировать два основных аспекта:

1) **Управление пулом** – определяет конкретные параметры для каждого пула, такие как комиссии за обмен, плата за влияние на цену и время обмена (Чем больше это время, тем больше разброс цен. Время обмена может составлять от минуты до пяти минут).

2) **Управление организацией** – управляет общими параметрами для всех пулов, такими как плата за обмен по умолчанию, плата за влияние цены по умолчанию, время обмена по умолчанию, вознаграждение за реферал и вознаграждение за управление.

Кроме того, стейккая токен 1INCH, пользователи получают прибыль в связи с положительным проскальзыванием, который представляет собой чистую положительную разницу между сделками обмена, когда цена исполнения немного лучше, чем указанная цена. Примечательно, что 1inch Network также имеет множество партнерских отношений с другими протоколами, где стимулы к добыче ликвидности являются обычным явлением для торговых пар с 1INCH.

Другие важные функции включают в себя лимитные ордера, возможность выбора процесса маршрутизации Pathfinder и выбора между максимизацией прибыли или минимизацией затрат на газ.

1inch Network также включает в себя свой собственный протокол ликвидности. Автоматизированный маркетмейкер защищает пользователей от фронтраннинга и предлагает больше возможностей для провайдеров ликвидности.

Matcha



Matcha

Matcha – это агрегатор децентрализованной биржи (DEX), созданный компанией 0x Labs. Matcha работает по протоколу 0x с различными продуктами, включая общие среди обменников ордера P2P (собственная ликвидность 0x) и их проприетарный API. Matcha извлекает данные из API 0x и эффективно направляет заказы по всем доступным источникам ликвидности (более 20 по состоянию на 31 мая 2021 года).

В отличие от других агрегаторов DEX, Matcha использует комбинацию компонентов на блокчейне и вне блокчейна на протяжении всего торгового процесса. Котировки генерируются вне блокчейна с помощью API 0x, чтобы минимизировать затраты на газ, прежде чем выполнить ордер на блокчейне. API 0x находит наиболее экономически эффективный способ торговли (включая затраты на газ) и может даже автоматически распределять отдельные заказы по нескольким источникам ликвидности, если это лучше для трейдера.

На сегодняшний день было четыре основных обновления API 0x (который использует Matcha), последним из которых является версия 4, выпущенная в марте 2021 года. Благодаря этому обновлению версии 4 пользователи Matcha снизили затраты на газ (до 70% экономии газа по обычным ордерам и 10% для лимитных ордеров) и получают лучшие цены.

Начиная с версии 3 0x, с пользователей Matcha взимается небольшая плата за протокол (оплачивается в ETH) за внесение в перечень ордеров 0x. Плата пропорциональна стоимости газа выполнения ордеров и линейно зависит от цены на газ. Здесь важно отметить, что Matcha технически не взимает никаких комиссий с транзакций, кроме необходимых сетевых сборов, требуемых либо самим блокчейном, либо источником ликвидности.

В отличие от 1inch, Matcha передает все положительные проскальзывания обратно пользователю. Другие важные функции включают в себя лимитные ордера и недавнюю поддержку сети Binance Smart Chain и сети Polygon.

Paraswap



ParaSwap был впервые разработан в сентябре 2019 года и использует собственный алгоритм маршрутизации Hopper. ParaSwap проверяет курс для данной пары на всех поддерживаемых биржах и отображает эффективную ставку (с учетом проскальзывания) для каждой пары.

ParaSwap реализует несколько решений для снижения потребления газа на платформе, таких как внедрение газового токена REDUX. Затраты на газ учитываются при анализе путей обмена.

Последнее обновление ParaSwap, версия 3, было выпущено в январе 2021 года. Она включала значительное обновление пользовательского интерфейса и улучшенные контракты на обмен. Акцент был сделан на снижении общих затрат на газ на 30%, особенно для сделок, заключенных с использованием только одного DEX.

Доходы от протокола генерируются по двум основным направлениям. Первое – через сторонние интеграторы, которые взимают комиссию за обмен. ParaSwap берет 15% от этой комиссии. Второе – через положительное проскальзывание, где 50% направляется в протокол, а остальные 50% передаются пользователю.

В настоящее время ParaSwap имеет 48 источников ликвидности. Это дополняется собственными пулами (ParaSwap-пулами), которые обеспечены частными маркетмейкерами. ParaSwap также недавно интегрировался с блокчейном Binance и сетью Polygon.

Факторы производительности агрегаторов DEX

«Под капотом» агрегаторов DEX скрывается множество деталей, из-за которых их трудно объективно сравнивать. Хотя пользователи могут ориентироваться на указанную цену, они не обязательно достоверны. И вот почему:

Пример

Допустим, пользователь хочет обменять 1000 USDC на 1000 USDT.

Агрегатор X расценивает 1000 USDC как 1000 USDT и имеет ориентировочную стоимость транзакции в 5 долларов США, что дает реализованный обменный курс $1 \text{ USDC} = 0,995 \text{ USDT}$. После обмена 1000 долларов США, пользователь получит 995 долларов США.

Агрегатор Y расценивает 1000 USDC как 1005 USDT и имеет ориентировочную стоимость транзакции в 15 USDT, что дает реализованный обменный курс 1 USDC = 0,990 USDT. После обмена 1000 USDC, пользователь получит только 990 USDT.

В этом примере агрегатор X более экономичен с точки зрения затрат после учета комиссии за транзакцию. Вы должны помнить, что в этом примере используются оценочные данные, которые агрегатор DEX предоставляет перед обменом.

На самом деле, когда человек выполняет обмен, разница во времени между утверждением обмена и успешным выполнением обмена в блокчейне повлияет на конечную цену. В течение этого периода могут измениться внешние рыночные факторы, такие как загруженность сети и размер выбранных пулов ликвидности. Алгоритм маршрутизации протокола также повлияет на результат, поскольку более эффективные транзакции сокращают использование сети и сводят к минимуму количество неудачных транзакций.

Еще один момент – размер транзакции. Экономия затрат, получаемая от агрегаторов DEX, пропорционально выше для более крупных транзакций, поскольку они подвержены более высокому проскальзыванию цен. Для небольших транзакций, возможно, не потребуется полагаться на разные пулы ликвидности, поскольку один пул ликвидности является наиболее оптимальным путем.

Если мы классифицируем все эти показатели, мы получим четыре основных фактора, определяющих производительность агрегатора DEX:

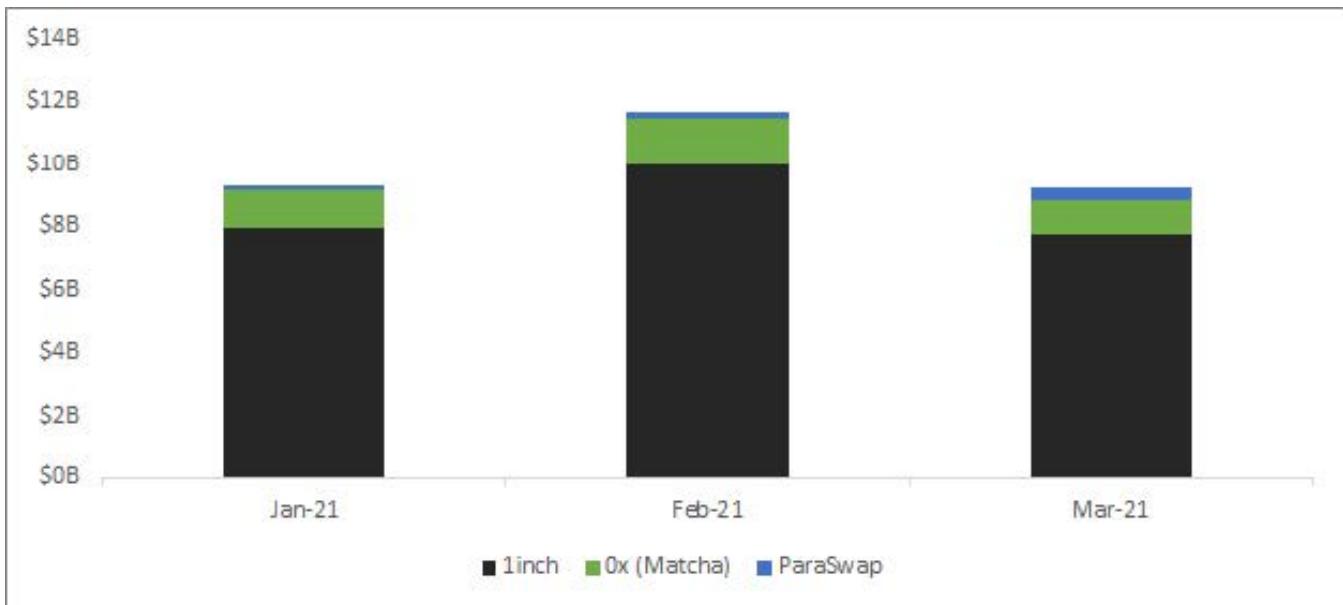
1. Алгоритм маршрутизации
2. Источники ликвидности
3. Текущее состояние рынка
4. Размер транзакции

Какой агрегатор DEX представляет наибольшую ценность?

Агрегаторы DEX стали неотъемлемой частью экономики DEX. Хотя трудно определить, какой агрегатор DEX представляет наибольшую ценность, следующая таблица дает некоторую ясность:

Состояние на 31.05.2021	1inch	Matcha	ParaSwap
Количество Источников ликвидности	Более 80	Более 20	48
Токен	1INCH + CHI	Нет	Нет
Алгоритм маршрутов	Pathfinder	0x API	Hopper
Лимитные ордера	Да	Да	Нет
Возможность стейкинга	Да	Нет	Нет
Комиссия	Составляет 0,25% фиксированной комиссии по всем сделкам	70 000 gwei	Нет, но сторонние интеграторы взимают 15% от размера комиссии
Поддержка блокчейна	Ethereum, Binance Smart Chain и Polygon		
Возврат положительного проскальзывания	Переменная. Около 20% положительного проскальзывания приходится на рефереров и 80% на вкладчиков 1inch	100 %	50 %

1inch имеет множество преимуществ как пионер в этой области. По состоянию на 31 мая 2021 года протокол имеет наибольшее количество источников ликвидности – более 80. 1inch также является единственным агрегатором DEX с собственными токенами, что дает ему явное преимущество перед другими протоколами и позволяет пользователям вкладывать токены 1inch и получать плату за использования протокола. 1inch также более децентрализован, чем другие протоколы, в которых отсутствует DAO. Все эти преимущества отражаются в объеме торгов, самом базовом показателе.



В общем объеме торгов за 1 квартал 2021 года преобладает 1inch. В марте 2021 года на 1inch приходилось 84,2% общей доли рынка и объем торгов составлял 7,76 миллиарда долларов. Конечно, это также может быть вызвано целым рядом причин, включая лояльность пользователей и информационную асимметрию. Однако, в целом высокие показатели удержания пользователей свидетельствуют о том, что рынок признает преимущества 1inch.

Сопутствующие риски

Хорошей практикой является не рассматривать котировки на агрегаторах DEX как истину в первой инстанции. В то время как агрегаторы DEX стремятся обеспечить соответствие выполняемой транзакции указанной цене, это происходит не всегда.

Еще один момент – размер транзакции. Хотя агрегаторы DEX обеспечивают лучшую экономию средств при более крупных транзакциях, иногда мелким трейдерам может быть лучше взаимодействовать напрямую с DEX.

Агрегаторы DEX обычно надежны, но были случаи, когда транзакции перенаправлялись через небольшие и неликвидные пулы. Пользователь всегда должен проверять, что ваше проскальзывание не слишком велико, прежде чем одобрить транзакцию.

Агрегаторы, заслуживающие упоминания



DEX.AG (ребрэндинг в Slingshot)

DEX.AG – один из небольших агрегаторов DEX, использующий собственный проприетарный алгоритм маршрутов X Blaster. Проект переименовался в Slingshot в ноябре 2020 года. На момент написания статьи (1 апреля 2021 года) протокол интегрирован с 18 источниками ликвидности, не взимает никаких торговых сборов и еще не выпустил актуальную версию их обновления.



Totle

Totle – это еще один небольшой агрегатор DEX, который использует свой собственный API (Totle API). На момент написания статьи (1 апреля 2021 года) интегрирован с 15 источниками ликвидности

Вывод

DEX – это жизненная основа DeFi.. Однако, для многих опытных пользователей (особенно китов), агрегаторы DEX еще более важны, поскольку они могут обеспечить лучшую экономическую эффективность для крупных транзакций. Агрегаторы DEX даже развились до такой степени, что у них появились собственные пулы ликвидности, что еще больше стирает грань между агрегаторами DEX и самими DEX.

Сектор DEX является ярким примером универсальности DeFi. Агрегаторы DEX построены поверх DEX для обслуживания различных целей пользователя. Таким образом, мы извлекаем выгоду из более полного набора инновационных продуктов, созданных в результате возросшей конкуренции и взаимной интеграции.

Рекомендуемая литература

1. Обзор агрегаторов

[DEX https://www.delphidigital.io/reports/defi-aggregators/](https://www.delphidigital.io/reports/defi-aggregators/)

2. Сравнение Различных Агрегаторов DEX

<https://medium.com/2key/defi-dexes-dex-aggregators-amms-and-built-in-dex-marketplaces-which-is-which-and-which-is-best-fba04ca48534>

3. Исследование 0x от октября 2020 года по агрегаторам DEX

<https://blog.0xproject.com/a-comprehensive-analysis-on-dex-liquidity-aggregators-performance-dfb9654b0723>

4. Обновление 1inch версии 3 и сравнение с другими агрегаторами DEX

<https://blog.1inch.io/introducing-the-1inch-aggregation-protocol-v3-b02890986547>

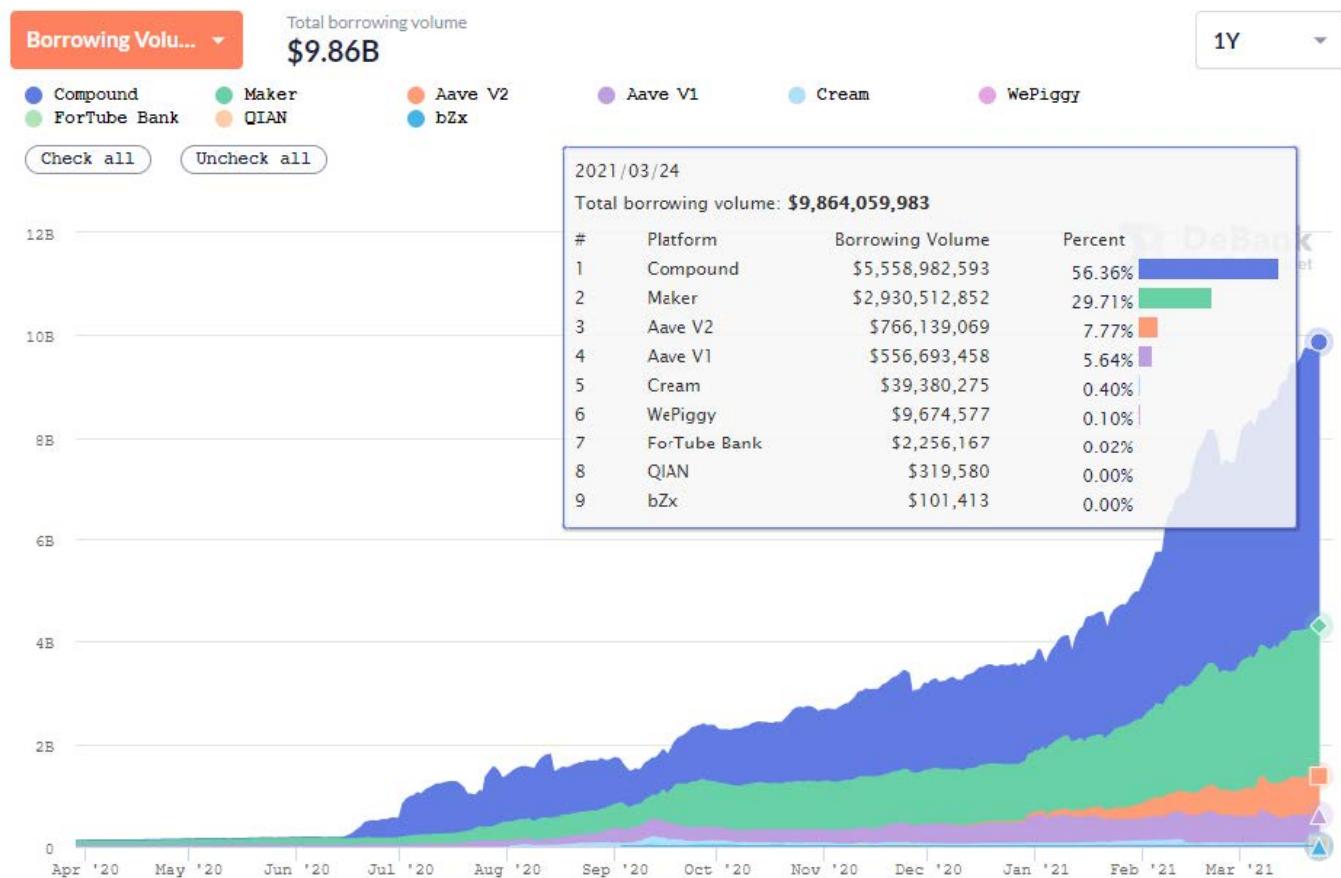
ГЛАВА 5: ДЕЦЕНТРАЛИЗОВАННОЕ КРЕДИТОВАНИЕ

Рынок капитала в традиционной финансовой системе недоступен для многих – только богатые образно говоря имеют VIP-карту для доступа к нему.

Представьте, что вы венчурный инвестор, желающий профинансируировать свое следующий бизнес. Вы можете взять кредит и предложить свои активы в качестве залога. Залоговый капитал останется нетронутым и будет продолжать расти с течением времени, и его можно будет выкупить позже. Конечно, это не безрисковая стратегия. Если вы не будете осторожны, вы можете не выполнить платеж по кредиту и потерять свой залог.

Протоколы кредитования в DeFi теперь обеспечили доступ к долговым инструментам для всех. Используя свои криптовалюты в качестве залога, вы можете заимствовать у этих протоколов и использовать их. Как один из крупнейших инструментов DeFi, децентрализованное кредитование выросло в геометрической прогрессии, объем заимствований достиг 9,7 миллиарда долларов в апреле 2021 года. Это в 102 раза больше, чем годом ранее!

Ведущими протоколами кредитования DeFi являются Compound, Maker, Aave и Cream.



Обзор протоколов кредитования

Compound



Compound Finance – это протокол финансового рынка, разработанный Compound Labs. Это основанный на Ethereum протокол финансового рынка с открытым исходным кодом, где любой может без проблем одолживать или занимать криптовалюты. По состоянию на 1 апреля 2021 года на платформе Compound доступно девять различных токенов.

1. 0x (ZRX)
2. Basic Attention Token (BAT)
3. Compound (COMP)
4. Dai (DAI)
5. Ether (ETH)
6. USD Coin (USDC)
7. Tether (USDT)
8. Uniswap (UNI)
9. Wrapped Bitcoin (WBTC)

Compound работает в качестве пула ликвидности, построенного на блокчейне Ethereum. Поставщики кладут активы в пул ликвидности, чтобы получать проценты, в то время как заемщики берут кредит в пуле ликвидности и выплачивают проценты по своему долгу. По сути, Compound устраняет разрыв между кредиторами, которые хотят получать проценты с незанятых средств, и заемщиками, которые хотят заимствовать средства для производственного или инвестиционного использования.

В Compound процентные ставки обозначаются в годовой процентной доходности (APY), и процентные ставки различаются между активами. Compound выводит процентные ставки с помощью алгоритмов, учитывающих спрос и предложение активов.

По сути, Compound убирает сложности при кредитовании/заемствовании, позволяя поставщикам/заемщикам напрямую взаимодействовать с протоколом для получения процентных ставок без необходимости согласования условий кредита (например, срока погашения, процентной ставки, контрагента, обеспечения), тем самым создавая более эффективный финансовый рынок.

Compound является крупнейшей платформой кредитования DeFi по объему заемствований с долей рынка 56% (по данным на 1 апреля 2021 года). В июне 2020 года Compound представила свой токен управления Compound (COMP).

Maker



Maker – старейший протокол заемствования в DeFi. Он позволяет получать кредиты с избыточным обеспечением, поддерживая более 30 различных токенов для выпуска DAI, децентрализованного стейблкоина, привязанной к доллару США. Помимо того, что это протокол заемствования, Maker также выступает в качестве эмитента стейблкоина (DAI).

19 декабря 2017 года Maker первоначально начал с одним активом в качестве залога для выпуска DAI (SAI). Он выпускался с использованием эфира (ETH). 18 ноября 2019 года Maker обновил SAI до DAI, который может быть выпущен с использованием 29 различных токенов в качестве обеспечения.

Maker теперь даже принимает USDC, централизованный стейблкоин, который помогает управлять нестабильностью стоимости DAI. Maker добился огромного прогресса в преодолении разрыва с традиционными финансами, внедрив первый «реальный» актив в качестве залога с помощью Centrifuge. 21 апреля 2021 года компания успешно оформила свой первый кредит MakerDAO на сумму 181 тыс. долларов с домом в качестве залога, фактически создав один из первых ипотечных кредитов на основе блокчейна.

В отличие от других протоколов кредитования, пользователи не могут предоставлять активы для займа в Maker. Они могут только занимать DAI путем внесения залога. DAI является крупнейшим децентрализованным стейблкоином, и в экосистеме DeFi наблюдается растущее его заемствование. Мы более подробно рассмотрим DAI в главе 6.

Aave



Aave – еще один известный протокол децентрализованного финансового рынка, аналогичный Compound. По состоянию на апрель 2021 года пользователи могут предоставлять и занимать 24 различных актива на Aave, что значительно больше по сравнению с Compound.

И Compound, и Aave работают аналогично, когда кредиторы могут предоставлять ликвидность, внося криптовалюты в доступные кредитные пулы и получая проценты. Заемщики могут брать кредиты, подключаясь к этим пулам ликвидности, выплачивая проценты.

Aave отличается от Compound тем, что впервые применила новые принципы кредитования, такие как переключение ставок, обмен залога и флэш-займы.

Переключение ставок: Заемщики на Aave могут переключаться между переменными и стабильными процентными ставками.

Обмен залога: Заемщики могут обменять свое обеспечение на другой актив. Это помогает предотвратить снижение ставки по кредитам ниже минимального уровня обеспечения и их ликвидацию.

Флэш-займы: Заемщики могут брать кредиты с нулевым обеспечением, если заемщик погашает кредит, проценты и сборы в рамках одной и той же транзакции. Флэш-займы полезны для арбитражных трейдеров, поскольку они эффективны с точки зрения капитала при совершении арбитражных сделок в различных приложениях DeFi.

Cream Finance



Cream Finance (C. R. E. A. M) была основана в июле 2020 года Джоном Хуангом и Лео Ченом. Cream – это форк Compound, который также обслуживает экзотические активы с малым объемом торгов. Cream стала партнером (объединилась) в экосистему Yearn Finance в ноябре 2020 года. Она развернута в Ethereum, Binance Smart Chain и Fantom.

У Cream более мягкая политика привлечения активов по сравнению с Compound и Aave. Используя стратегию быстрого развития, Cream за короткое время привлек больше активов, чем любой другой протокол кредитования. Он решил сосредоточиться на активах с более низкой ликвидностью или относящихся к нишевым категориям. Это был один из первых кредитных протоколов, который принимал токены получающие доход, и токены провайдера ликвидности в качестве обеспечения.

Cream также запустила Iron Bank, услугу кредитования без залога, предлагаемую партнерам, включенным в белый список. Как один из своих партнеров, Yearn Finance может использовать заемные средства Cream для дальнейшего увеличения дохода, полученного от фарминга.

В преддверии предстоящего запуска ETH 2.0 Cream также предлагает услугу стейкинга в ETH 2.0, где пользователи могут стейкать ETH для получения CRET2, которые могут быть предоставлены и взяты в качестве залога. Вся работа по стейкингу ETH 2.0 будет выполняться Cream, а доходность распределяется между держателями CRET2. По сути, CRET2 – это кастодиальная услуга стейкинга с оплатой комиссии в размере 8% от вознаграждения валидатора. В дополнение к ETH 2.0, Cream также предлагает стейкинговые услуги для Binance Smart Chain и Fantom.

Cream позиционирует себя как более рискованный кредитный протокол по сравнению с Compound и Aave, облегчая и стимулируя рыночный спрос на плечо и шорт нишевых активов.

Подробное сравнение протоколов

По состоянию на 24.03.2021	Compound	Maker	Aave	Cream
Количество поддерживаемых активов:				
В качестве обеспечения	8	29	21	47
В качестве займа	9	1	25	65
Объем заемных средств (BV)	5,559 млн.\$	2,931 млн.\$	1,324 млн.\$	39 млн.\$
Объем заблокированных средств (TVL)	6,910 млн.\$	6,090 млн.\$	5,010 млн.\$	202 млн.\$
Коэффициент использования (BV/TVL)	0,80	0,48	0,26	0,19

В таблице выше приведена информация о 4 крупнейших протоколах кредитования: Compound, Maker, Aave и Cream.

Мы последовательно рассмотрим каждый параметр сравнения, чтобы оценить эффективность капитала протокола с точки зрения объема заемных средств и общей заблокированной стоимости (TVL). Впоследствии мы рассмотрим связанные с этим риски для каждого из них.

Количество поддерживаемых активов

Чтобы гарантировать возможность получения кредитов без доверия, заемщикам необходимо будет внести активы (обеспечение) большей стоимостью, чем сумма займа. Это известно, как сверхобеспечение и лежит в основе платежеспособности протоколов кредитования DeFi. Сколько заемщики могут занять, зависит от коэффициента обеспечения каждого актива по различным протоколам кредитования DeFi.

Среди протоколов кредитования DeFi Cream имеет наибольшее число поддерживаемых активов – 45 активов могут быть использованы в качестве обеспечения, а 65 активов доступны для заимствования.

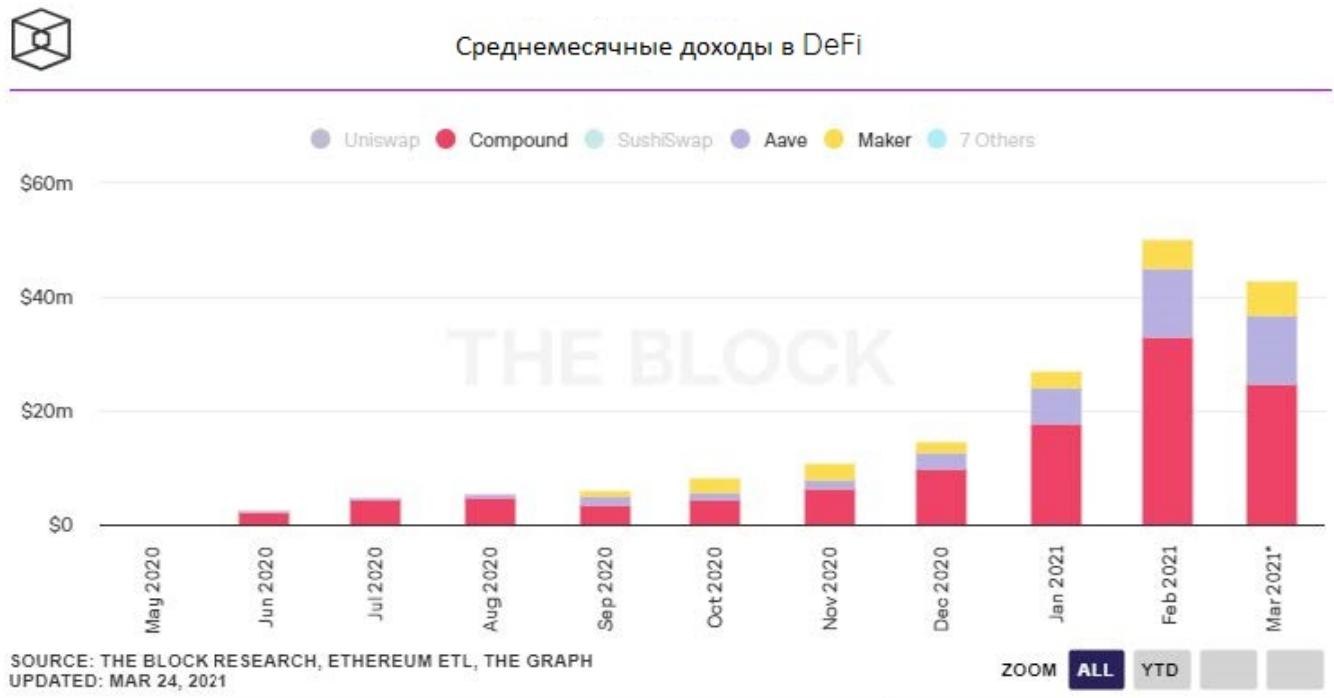
В отличие от Cream, Compound имеет наименьшее количество поддерживаемых активов – только 8 активов могут быть использованы в качестве обеспечения, а 9 активов доступны для заимствования. Компания Compound более консервативна в своей стратегии привлечения активов.

Доход

Одним из важнейших показателей для кредитных платформ является объем их заимствований. Этот показатель важен, потому что заемщики платят комиссионные за свои кредиты и тем самым генерируют доход для этих протоколов. Вот разбивка того, как каждый протокол получает доход:

- **Compound:** Часть процентов, выплаченных заемщиком, пойдет в его резерв, который действует как страховка и контролируется держателями токенов COMP. Каждый поддерживаемый актив имеет свой коэффициент резервирования, который определяет, сколько средств поступает в резерв. Вы можете проверить каждый из коэффициентов резервирования, нажав на соответствующие страницы активов.
- **Maker:** Когда заемщики погашают свои кредиты, они выплачивают основную сумму вместе с процентной платой, которая определяется комиссией. Каждое поддерживаемое обеспечение имеет свои комиссии.
- **Aave:** Платформа имеет 2 вида комиссий:
 - 0,00001% от суммы кредита собирается при получении кредита в Aave V1.
 - 0,09% взимается с суммы флэш-займов – подробнее о флэш-займах читайте в главе 14.
- **Cream:** Часть процентов, выплачиваемых заемщиками поставщикам, поступает в резерв протокола Cream и распределяется держателям токенов CREAM в качестве вознаграждения.

По состоянию на апрель 2021 года Compound генерирует самый высокий доход среди протоколов кредитования, как видно на изображении ниже:

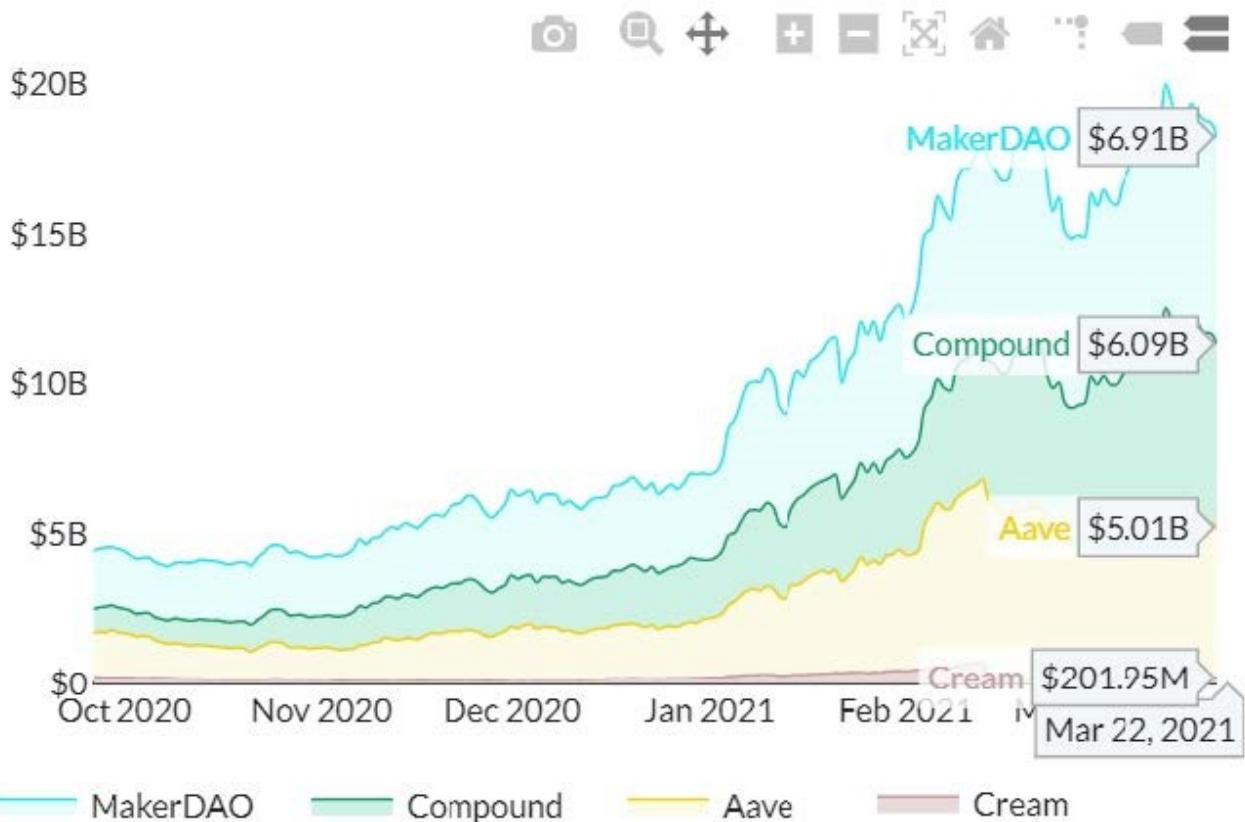


Объем заблокированных средств (TVL)

В то время как во всех протоколах кредитования наблюдается рост TVL с октября 2020 года, стоит отметить, что TVL для Aave и для Maker являются более естественными, чем Compound. Это связано с тем, что у Compound есть постоянные стимулы для заемщиков и кредиторов в рамках их программы майнинга ликвидности.

Примечание: Aave относительно недавно запустила программу майнинга ликвидности – в конце апреля 2021 года.

Кредитные протоколы / Объем заблокированных средств (TVL)

Средние значения за сутки

Коэффициент использования (BV/TVL)

Протоколы кредитования DeFi получают доход от займов. Между тем, объем заблокированных средств в кредитных платформах определяется объемом размещения пользовательских активов для получения дохода или для использования в качестве обеспечения.

Разделив объем заемных средств на объем заблокированных средств, мы можем получить коэффициент использования каждого протокола – чем выше коэффициент использования, тем эффективнее работает TVL.

Повторно рассмотрим изображение:

По состоянию на 24.03.2021	Compound	Maker	Aave	Cream
Количество поддерживаемых активов:				
В качестве обеспечения	8	29	21	47
В качестве займа	9	1	25	65
Объем заемных средств (BV)	5,559 млн.\$	2,931 млн.\$	1,324 млн.\$	39 млн.\$
Объем заблокированных средств (TVL)	6,910 млн.\$	6,090 млн.\$	5,010 млн.\$	202 млн.\$
Коэффициент использования (BV/TVL)	0,80	0,48	0,26	0,19

На первый взгляд кажется, что у Compound самый высокий коэффициент использования (0,80), а у Cream самый низкий (0,19). Тем не менее, высокий коэффициент использования Compound может быть обусловлен его программой майнинга ликвидности, которая вознаграждает заемщиков токенами COMP, в то время как низкий коэффициент Cream может быть связан с тем, что в прошлом он пострадал от нескольких эксплайтов. Учитывая вопросы безопасности, Cream укрепила безопасность с помощью увеличения вознаграждения за ошибки в протоколе до 1,5 миллиона долларов с помощью Immunefi, страхового покрытия с помощью Armor.fi/Nexus Mutual, и открытого отчета безопасности от DeFi Safety.

Ставки по кредитам и займам

Теперь давайте рассмотрим два основных типа пользователей протоколов кредитования: кредиторов и заемщиков.

Кредиторы

Предложения на рынке вкладов

	Compound	Aave	Cream
USDC	5,51 %	7,50 %	16,13 %
ETH	0,16 %	0,33 %	1,60 %
DAI	7,75 %	8,71 %	13,50 %
WBTC	0,45 %	0,18 %	2,22 %
USDT	2,43 %	7,13 %	26,11 %

Основываясь на приведенной выше таблице, Cream обеспечивает самый высокий показатель годовой доходности, а Compound обеспечивает самый низкий показатель годовой доходности для большинства активов. Кредиторам может показаться, что желательнее зарабатывать с самыми высокими процентами в Cream, но высокие проценты часто означают более высокие базовые риски внесения вашего актива в эти кредитные протоколы по сравнению с другими.

Cream вынужден предлагать высокие API-интерфейсы для привлечения капитала в свой протокол, поскольку ранее он несколько раз был взломан. В целом, Compound обеспечивает самый низкий показатель годовой доходности для всех поддерживаемых активов по сравнению со своими конкурентами, поскольку его бренд фокусируется на безопасности платформы.

Заемщики

	Compound	Aave (переменная ставка)	Aave (постоянная ставка)	Cream	Maker
USDC	7,25 %	8,23 %	15,23 %	23,20 %	-
ETH	2,76 %	2,06 %	5,57 %	8,02 %	-
DAI	10,78 %	14,71 %	22,71 %	21,26 %	0 % – 9 %
WBTC	4,82 %	1,61 %	5,01 %	9,80 %	-
USDT	3,67 %	6,80 %	14,80 %	42,04 %	-

Что касается заемщиков, вы, как правило, ищите кредитные платформы, которые предлагают самую низкую процентную ставку, потому что это означает более низкие затраты по займам. Compound предлагает наиболее конкурентоспособные ставки по займам по сравнению со своими аналогами. Однако Compound имеет ограниченный список активов, которые пользователи могут заимствовать.

Что касается Aave, то он предоставляет заемщикам два варианта ставок: переменную ставку и стабильную ставку. Пользователи могут переключать свои тарифы в любой момент времени, в зависимости от того, что им выгоднее.

Cream взимает самые высокие ставки по займам – в первую очередь потому, что у нее самый разнообразный список активов, которые пользователи могут занимать. Более высокие ставки по займам на Cream необходимы для компенсации высоких требований кредиторов за принятие дополнительного риска по предоставлению своего капитала.

Довольно любопытно, что некоторые заемщики Cream являются институционалами, использующими Cream Iron Bank, такие как Alpha Finance и Yearn Finance. Iron Bank предоставляет новую услугу кредитования без залога, в которой другим протоколам не требуется предоставлять обеспечение для заимствования у Cream.

Теперь давайте сосредоточимся конкретно на заемщиках DAI. Maker является единственным эмитентом DAI, и он предоставляет самую дешевую процентную ставку любому из своих заёмщиков для поддерживаемых на платформе активов. Объемы заимствований Maker являются вторыми по величине после Compound и заблокированы в основном для выпуска DAI, который по состоянию на 1 апреля 2021 года является четвёртым по величине стейблкоином в мире. Это делает Maker невероятно важным игроком в экосистеме DeFi.

Сопутствующие риски

При использовании децентрализованных протоколов кредитования и заимствования вы должны быть осведомлены о технических рисках, таких как ошибки в смарт-контрактах. Хакеры могут использовать экспloit и забрать ваше обеспечение, содержащееся в этих протоколах, если разработчики не будут осторожны при развертывании своего кода.

Кроме того, многие протоколы кредитования полагаются на ценовых оракулов (подробнее об этом в главе 12) для предоставления данных о ценах в блокчейне. Ценовые оракулы могут ошибиться или на них могут повлиять эксплойты. В ноябре 2020 года ценовой оракул Compound был взломан путем повышения цены DAI на 30% на Coinbase Pro, в результате чего были ликвидированы кредиты на сумму 89 миллионов долларов.

Однако для заемщика основные риски связаны с потерей вашего обеспечения из-за неправильного управления коэффициентом обеспечения. Криптовалюта известна своей чрезвычайной волатильностью, и вы рискуете, что ваш кредит упадет ниже минимального коэффициента обеспечения и ваш залог будет ликвидирован, вы понесете значительные убытки и заплатите ликвидационный сбор. Таким образом, жизненно важно постоянно контролировать и поддерживать нормальное соотношение залогового обеспечения по вашим кредитам.

Протоколы кредитования, заслуживающие упоминания



Venus

Протокол Venus – это протокол рынка токенов и стейблкоинов, который работает на блокчейне Binance Smart Chain. Протокол, первоначально инкубированный Binance, является форком Compound и MarkerDAO. Swipe взяли разработку протокола Venus в свои руки с момента его приобретения компанией Binance.



Anchor

Протокол Anchor – это протокол кредитования, работающий на блокчейне Terra. Механизмы кредитования на платформе работают аналогично Compound и Aave. Протокол Anchor имеет целевой показатель доходности 20% для UST, стейблкоина в долларах США, созданного на блокчейне Terra.



Alchemix

Alchemix отличается от других игроков в области кредитования тем, что предоставляет самопогашающиеся кредиты без риска быть ликвидированным. Проще говоря, ваше обеспечение будет использовано для получения процентов, а заработанные проценты будут использованы для погашения кредита, который вы оформили на Alchemix.



Liquity

Liquity – это протокол заимствования DeFi, который позволяет вам использовать его стабильную валюту, Liquity USD (LUSD), без процентов. Вам необходимо использовать Ethereum в качестве залога и поддерживать минимальный коэффициент залога всего в 110%. Возврат необходимо будет производить в LUSD. Кредиты обеспечены стабилизационным пулом, содержащим LUSD, и другими заемщиками, коллективно выступающими в качестве гарантов на крайний случай.

Вывод

Протоколы кредитования и заимствования DeFi получили невероятное распространение – они доминировали в рейтинговых диаграммах TVL DeFi. Однако большинство кредитов в настоящее время все еще имеют избыточное обеспечение, что свидетельствует о низкой эффективности использования капитала.

В реальности кредитные организации используют кредитные баллы, получаемые на основе личной информации, такой как место работы, размер зарплаты и кредитная история, прежде чем принимать решение о предоставлении вам кредита. В DeFi сложно создать кредитную историю в связи с псевдоанонимностью.

Несколько протоколов направлены на развитие инструментов кредитования с недостаточным обеспечением, такие как TrueFi, Cream и Aave. В этих протоколах включенные в белый список организации могут получить кредит без предоставления какого-либо обеспечения.

Кредиты с недостаточным обеспечением станут следующим этапом развития протоколов кредитования и заимствования DeFi. Назрела необходимость предоставления кредитов с недостаточным обеспечением, чтобы протоколы кредитования и заимствования DeFi могли быть более эффективными с точки зрения использования капитала и эффективно конкурировать с традиционными кредитными организациями.

В то время как кредитование DeFi в настоящее время все еще в основном ограничено миром цифровых активов, с небольшим количеством ссылок на реальные активы, Maker добился огромного прогресса в апреле 2021 года, приняв в качестве залога реальные активы, такие как недвижимость. Таким образом, можно предположить лучшую интеграцию между традиционными финансами и DeFi в будущем.

Рекомендуемая литература

1. Оценка протоколов кредитования DeFi

<https://messari.io/article/a-closer-look-at-defi-lending-valuations>

2. Как оценить риски кредитования

<https://newsletter.banklesshq.com/p/how-to-assess-the-risk-of-lending>

3. Панель мониторинга протоколов кредитования

<https://terminal.tokenterminal.com/dashboard/Lending>

ГЛАВА 6: ДЕЦЕНТРАЛИЗОВАННЫЕ СТЕЙБЛКОИНЫ И СТАБИЛЬНЫЕ АКТИВЫ

В нашей книге «Что такое DeFi: Курс для начинающих» мы установили, что стейблкоины являются неотъемлемой частью криптоэкосистемы. По состоянию на 1 апреля 2021 года общая рыночная капитализация стейблкоинов составляет 64,5 миллиарда долларов – в 12 раз больше, чем в предыдущем году.

Поскольку как институциональные, так и небольшие инвесторы стекаются на крипторынки, спрос на стейблкоины будет продолжать расти. Это неудивительно, поскольку стейблкоины являются неволатильными активами, которые обеспечивают глобальный трансфер денег в крипторынок.

В нашей книге для начинающих рассмотрены некоторые ключевые различия между централизованным стейблкоином Tether (USDT) и децентрализованным стейблкоином DAI от Maker. В этой главе мы рассмотрим некоторые недостатки USDT и DAI, прежде чем касаться других децентрализованных стейблкоинов.

Централизованный стейблкоин

Tether (USDT)



USDT (ранее известная как RealCoin) централизованный стейблкоин, которая впервые начала торговаться на бирже Bitfinex в 2015 году. Будучи первым стейблкоином на рынке, он обладает большим преимуществом в объемах и последовательно сохраняет свои позиции лидера рынка стейблкоинов. По состоянию на апрель 2021 года рыночная капитализация USDT составляет 40 миллиардов долларов, что составляет более 66% от общей доли рынка стейблкоинов.

USDT обеспечивает привязку к доллару США с помощью системы обеспечения 1:1. Удерживая наличные деньги в качестве резервного обеспечения, выдается равная сумма в USDT. Теоретически, это надежный и простой метод обеспечения. В конце концов, это повторение Золотого стандарта, когда доллар США в прошлом веке был обеспечен золотом.

Однако проблема заключается в непрозрачном процессе выпуска Tether. Из-за централизованного характера его выпуска многие в криптообществе скептически относятся к тому, что у Tether есть резервный фонд. В марте 2019 года скептицизм был частично оправдан, когда Tether изменил свою стратегию, включив кредиты своих дочерних компаний в качестве обеспечения USDT.

На протяжении многих лет многочисленные правительственные учреждения начали расследования организации Tether. В феврале 2021 года расследование генерального прокурора Нью-Йорка в отношении внутренних финансов Bitfinex и Tether завершилось без каких-либо официальных обвинений. Тем не менее, генеральный прокурор Нью-Йорка наложил коллективный штраф в размере 18,5 миллиона долларов для урегулирования обвинений в том, что Bitfinex объединил клиентские и корпоративные средства.

История Tether продолжается и вряд ли разрешится в ближайшее время. Недавние события, такие как листинг на Coinbase, еще больше укрепили его легитимность. Технический директор Bitfinex Паоло Ардайно также подтвердил, что Tether зарегистрирован и регулируется FinCEN.

Децентрализованный стейблкоин

DAI



Maker – одна из первых попыток DeFi создать децентрализованный «Центральный банк». В качестве протокола кредитования DAI выдается как побочный продукт спроса на займы, в то время как залог (обычно в ETH) депонируется в хранилище Maker.

Эти хранилища сверхобеспечены (обычно 150% и выше, за исключением стейблкоинов), что помогает защититься от «черного лебедя», когда стоимость обеспичительных активов значительно падает. Maker помогает регулировать количество DAI, контролируя процентные ставки по кредитам, чтобы влиять на спрос и предложение.

Проблема с этим стейблкоином заключается в том, что избыточное обеспечение ограничивает эффективность использования капитала, что

затрудняет масштабирование в соответствии со спросом. Арбитражная механика, используемая для снижения цены DAI, требует большего капитала для погашения большого количества DAI.

Например, основное хранилище ETH, коэффициент обеспечения которого составляет 150%, потребует от заемщика раскошелиться на 1,5 доллара за 1 DAI. Это привело к сценариям, таким как печально известный Черный четверг и запуск майнинга ликвидности Compound, когда цена DAI выросла выше отметки в 1 доллар, поскольку она не могла справиться со спросом.

Maker пытается решить эти проблемы несколькими методами, такими как создание модуля стабильной привязки (Peg Stability Module). Однако очевидно, что спрос на DAI по-прежнему зависит от размера обеспечения, а не от спроса на более децентрализованное средство транзакций.

Как мы решаем задачу стейблкоинов?

Все стейблкоины имеют свои собственные недостатки и не ограничиваются недостатками Tether или DAI. В основе проблемы лежит балансирование принципов децентрализации DeFi против создания валюты, которая может надежно поддерживать свою привязку.

Хотя централизованные стейблкоины эффективны, их использование требует доверия по отношению к центральной организации и сопряжено с теми же системными рисками, которые угрожают традиционным финансам. С другой стороны, хотя DAI и децентрализована, она все еще неэффективна с точки зрения капитала и не может удовлетворить текущий рыночный спрос.

С момента создания Tether и DAI появилось несколько децентрализованных протоколов стейблкоинов, направленных на повышение децентрализации, стабильности цен и эффективности использования капитала. Мы называем эти протоколы алгоритмическими стейблкоинами.

Что такое алгоритмические стейблкоины и стабильные активы?

Как следует из названия, алгоритмические стейблкоины используют алгоритмы для управления структурой рынка стейблкоинов и лежащей в их основе экономики. Вы можете думать об алгоритмических стейблкоинах как об автоматизированном федеральном резерве, где вместо решений, принимаемых человеком, заранее запрограммированный код выполняет конкретные действия для контроля и влияния на цену.

В то время как большинство алгоритмических стейблкоинов привязаны к доллару США, есть привязки и к другим валютам, а некоторые даже имеют плавающую привязку, тем самым создавая новый тип активов, которые мы бы классифицировали как алгоритмические стабильные активы. В отличие от алгоритмических стейблкоинов, алгоритмические стабильные активы можно рассматривать как еще одну форму обеспечения.

Если классифицировать рынок стейблкоинов или стабильных активов в его текущем состоянии, то можно представить себе следующее разбиение:



Существует два способа классификации различных децентрализованных алгоритмических стейблкоинов:

- Не имеет обеспечения (ESD, AMPL и BAC)
- Частично/полностью обеспечен собственным токеном (FRAX, sUSD и UST)

Мы классифицировали UST и sUSD как алгоритмические стейблкоины, потому что они поддерживаются собственным токеном, в отличие от DAI, который поддерживается сторонними активами, такими как ETH и USDC. Это ключевой критерий, поскольку зависимость от собственных активов в качестве обеспечения создает рекурсивную стоимость, требующую алгоритмических функций для регулирования цены.

Алгоритмические стейблкоины могут быть дополнительно разбиты на различные категории – основными подкатегориями являются модели ребайза и модели с доходом, получаемым от эмиссии стейблкоинов (сенюораж).

Модель ребейза

Модель ребейза контролирует цену, изменяя количество стейблкоина в обращении. В зависимости от того, находится ли цена стейблкоина выше или ниже необходимой привязки, протокол автоматически увеличит или уменьшит количество монет в кошельке каждого держателя в течение фиксированного периода.

Причина этого заключается в том, что, жестко контролируя объем обращения, на цену стейблкоина можно влиять, основываясь на простой инфляционной/дефляционной экономической теории.

Новаторским протоколом для этой модели является Ampleforth (AMPL), датируемый еще 2019 годом.

Ampleforth

Ampleforth

Каждые 24 часа весь объем циркулирующего предложения Ampleforth (AMPL) либо пропорционально увеличивается, либо уменьшается, чтобы гарантировать, что цена останется на уровне 1 доллара. Если цена AMPL торгуется на 5% или более выше целевого показателя в 1 доллар, ребейз расширит предложение для кошельков, содержащих AMPL. Если цена AMPL торгуется на 5% или более ниже целевого уровня в 1 доллар, ребейз уменьшит количество монет в кошельках, содержащих AMPL.

Это затронет каждого владельца кошелька, но они сохранят ту же долю рынка, что и раньше. Ребейз, как в плюс, так и в минус, не является развлечением, поскольку пропорционально влияет на все AMPL.

Поскольку ребейз происходит с фиксированными интервалами, пользователи могут приурочить свои сделки к покупке или продаже AMPL непосредственно до ребейза, чтобы увеличить стоимость своих активов.

Модель сеньоража

Модель сеньоража контролирует цену, внедряя систему вознаграждений, которая влияет на динамику рынка. Если цена выше привязки, создаются новые токены и выдаются участникам, которые предоставляют ликвидность или сделали ставку в токенах.

Если цена ниже привязки, токены перестают создаваться, и вводятся механизмы для сокращения предложения. Пользователи могут приобретать купоны, которые сжигают базовые токены, чтобы удалить их из предложения. Эти купоны могут быть обменены на большее количество токенов в будущем, но только тогда, когда цена вернется или превысит предполагаемую привязку.

Существует три основные реализации этой модели:

Empty Set Dollar



Empty Set Dollar (ESD) – это модель сенюоража с одним токеном. Как следует из этого термина, в этой модели есть только один токен. Пользователи предоставляют ликвидность или долю в децентрализованной автономной организации (DAO) через собственный токен протокола – токен ESD эффективно действует как в качестве стейблкоина, так и в качестве токена управления.

В начале каждой эпохи система будет измерять средневзвешенную по времени цену (Time-Weighted Average Price – TWAP). Если TWAP превысит 1 доллар, протокол вступит в фазу инфляции и будет производить токены в качестве вознаграждения для участников DAO и провайдеров ликвидности. И наоборот, если цена упадет ниже 1 доллара, протокол вступит в фазу ограничения, когда пользователи перестанут получать какие-либо вознаграждения.

Во время фазы ограничения пользователи могут приобретать купоны, сжигая ESD, чтобы получить премию в размере до 45%, если протокол снова вступит в фазу расширения. Однако купоны действуют только в течение 30 дней, а это означает, что покупатели купонов рискуют ничего не получить, если система будет находиться в фазе сокращения более 30 дней. Эпохи в ESD делятся 8 часов.

Basis Cash



Basis Cash – это модель сенюоража с двумя токенами. Как следует из этого термина, существует дополнительный токен, так называемый долевой токен. Стейблкоином является Basis Cash (BAC), в то время как ее долевой токен – Basis Share (BAS).

Как и ESD, Basis Cash полагается на механизм TWAP, который будет создавать или прекращать создание BAC, в зависимости от того, будет ли цена BAC выше или ниже 1 доллара. Когда BAC превышает 1 доллар, протокол вступает в фазу расширения, когда пользователи могут получать только что сформированные BAC из хранилища DAO путем размещения BAS.

Когда BAC ниже 1 доллара, протокол вступает в фазу сокращения, когда новые BAC не будут формироваться для пользователей, разместивших BAS. Базовые бонды (аналогичные купонам ESD) становятся доступными для покупки по цене (BAC)². Покупатели базовых облигаций смогут выкупить BAC, когда протокол снова вступит в фазу расширения.

Эпохи Basis Cash делятся 24 часа, и, в отличие от купонов ESD, у базисных облигаций нет срока годности.

Frax Finance



Frax заимствует принципы из модели сенюоража, чтобы создать свою собственную уникальную модель, стейблкоин которой (FRAX) поддерживается двумя типами обеспечения – централизованным стейблкоином с фиатной поддержкой (USDC) и собственным долевым токеном Frax Share (FXS). Хотя Frax в настоящее время использует фиатные стейблкоины в качестве обеспечения, протокол намерен в конечном итоге полностью диверсифицироваться в децентрализованное обеспечение.

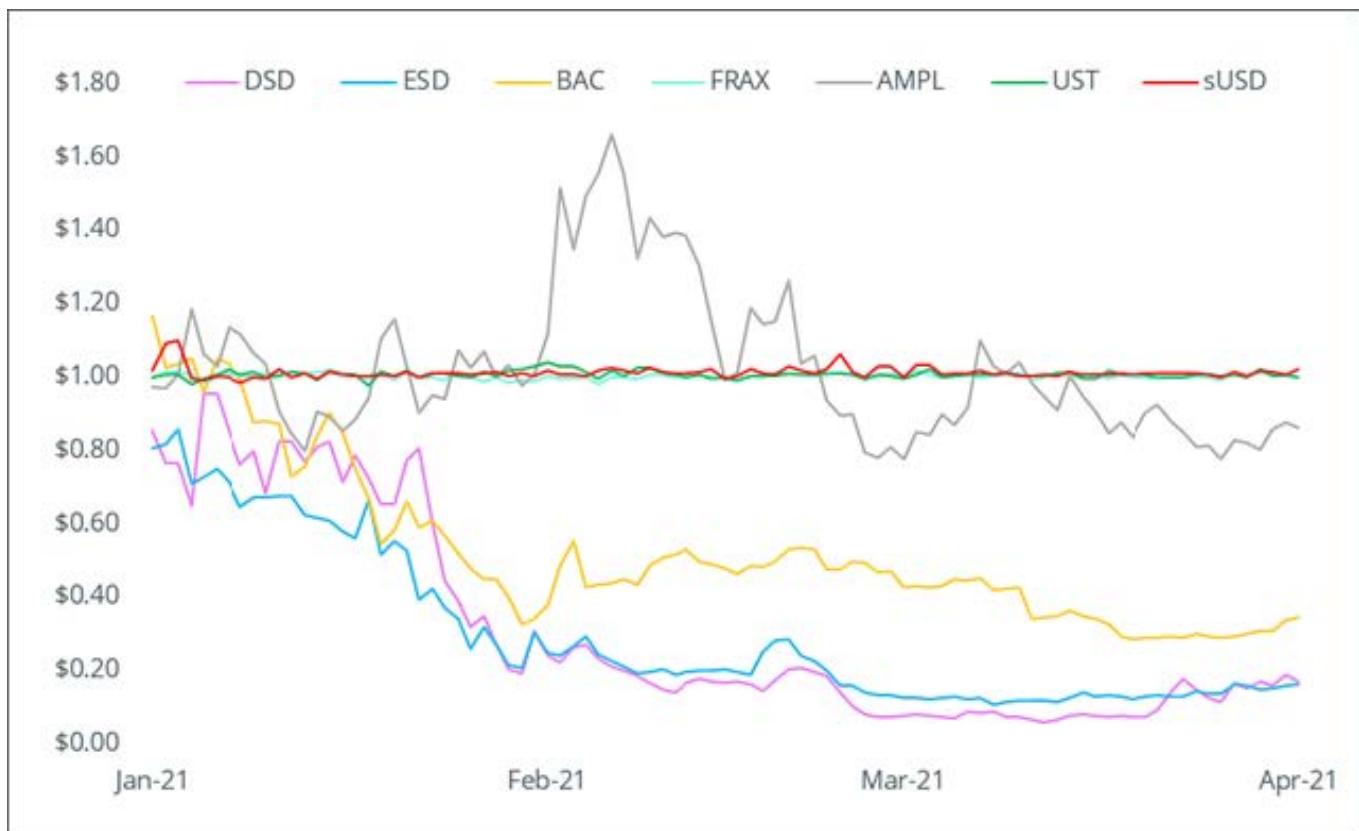
В отличие от Basis или ESD, Frax использует подход частичного обеспечения. Frax имеет регулируемый коэффициент обеспечения, управляемый PID-контроллером (proportional-integral-derivative - PID). Коэффициент обеспечения корректируется в соответствии с коэффициентом роста, который измеряет объем ликвидности FXS по сравнению с общим предложением FRAX.

Стейблкоины Frax (FRAX) могут быть сформированы и выкуплены за 1 доллар. Это стимулирует арбитражеров покупать или формировать FRAX, возвращая цену к ее привязке. С другой стороны, FXS накапливает комиссионные, доходы от сенюра и избыточного обеспечения. Примечательно, что Frax запустил veFXS, который предоставляет часть прибыли от контроллера алгоритмических операций на рынке (Algorithmic Market Operations Controller AMO) вкладчикам FXS, аналогично тому, как veCRV получает часть комиссионных за транзакции в Curve Finance.

Когда FRAX превышает 1 доллар, PID снижает коэффициент обеспечения, а когда FRAX ниже 1 доллара, PID увеличивает коэффициент обеспечения. Как частота обновления, так и параметры величины изменения могут быть скорректированы с помощью управления FXS.

По состоянию на 8 мая 2021 года FRAX на 85,25% поддерживается USDC и на 14,75% – FXS.

Как ранее обстояли дела с алгоритмическими стейблкоинами?



В течение последнего квартала 2020 года мы видели много алгоритмических стейблкоинов, запущенных на рынке. Многие из этих стейблкоинов используют модель сеньоража.

Несмотря на воодушевление криптообщества, большинство из этих протоколов потерпели неудачу. Если мы посмотрим на историческую цену топ-7 алгоритмических стейблкоинов по рыночной капитализации, только UST, sUSD и FRAX смогли сохранить привязку к доллару США.

Хотя каждый протокол имеет свою собственную механику действий и свои причины провала, можно сделать некий общий обзор по проблемам со стейблкоинами типа сеньоража.

Исторически сложилось так, что систему фиатной валюты было легче внедрить, потому что страны обладают централизованными полномочиями. Например, монархии и правительства обладают монополией чеканить монеты и гарантировать их ценность. Сравните это с рынком стейблкоинов, где новые протоколы должны делать то же самое в одночасье на основе экспериментального продукта, в децентрализованной среде, сильно насыщенной конкуренцией и признанными личностями.

Чтобы преодолеть это, алгоритмические стейблкоины предлагали привлекательные стимулы в виде огромных вознаграждений за майнинг ликвидностью. Проблема с этим подходом заключается в том, что он в первую очередь привлек спекулянтов, стремящихся сделать быстрый рывок, породив новый вид фермеров, известных как Algo-фермеры.

У Algo-фермеров была одна цель – найти новые алгоритмические протоколы стейблкоинов раньше, чем кто-либо другой, фармить этот стейблкоин, обеспечивая ликвидность, и выйти, как только другие Algo-фермеры начнут вливаться. Таким образом, распределение было централизовано внутри первой группы Алго-фермеров и переложено на опоздавших. Запуск алгоритмических стейблкоинов фактически превратился в игру в музыкальные стулья, поскольку у спекулянтов было мало стимулов для того, чтобы совершать и активно вносить свой вклад в одно сообщество, быстро переходя к другим алгоритмическим клонам стейблкоинов.

Неудивительно, что такие потрясения привели к массовым колебаниям цен. Большинство алгоритмических стейблкоинов были разработаны с учетом некого сообщества единомышленников, но это не стимулировало пользователей поддерживать систему во время сокращений или даже противодействовать манипуляциям с ценами со стороны более крупных игроков.

Кроме того, алгоритмические стейблкоины в основном торгуются на автоматизированных маркетмейкерах, таких как Uniswap, что усилило волатильность из-за неизменяемых характеристик Uniswap. На стадии дефляции провайдеры ликвидности также не заинтересованы в предоставлении ликвидности из-за непостоянного риска потерь, что приводит к дальнейшей волатильности.

Почему FRAX стал успешным?

В то время как sUSD, UST и FRAX имеют свои собственные причины успешности, мы сосредоточимся на FRAX, потому что на сегодняшний день у него лучшее удержание привязки, средняя цена составляет 1,001 доллара США в течение 1 квартала 2021 года. Вот некоторые из причин, по которым мы считаем, что до сих пор они были успешными:

1. Frax частично обеспечен USDC, что вселяет уверенность сообщества в систему для поддержания ее привязки. По состоянию на 8 мая 2021 года 85,25% FRAX обеспечивается USDC.
2. Frax сохраняет коэффициент обеспечения гибким, удовлетворяя рыночным требованиям для ценообразования FRAX на уровне 1 доллара.
3. Обеспечение переводится в другое место для получения процентов. Это помогает получать внешние доходы и поддерживает протокол на плаву, который затем используется для выкупа и сжигания FXS.
4. Волатильность цен FRAX смещается в сторону FXS из-за его выкупа и механики сжигания.

Хотя это всего лишь упрощенные причины успешности, модель все равно необходимо будет постоянно пересматривать, особенно во времена кризиса, когда цены на валюту значительно падают и когда вознаграждение за добычу ликвидности в конечном итоге прекращается.

Следующее поколение алгоритмических стейблкоинов и стабильных активов

Хотя FRAX в значительной степени добился успеха, можно утверждать, что он не является по-настоящему децентрализованным. Это связано с тем, что он все еще по большей части обеспечен USDC, который обеспечен денежными резервами, хранящимися в централизованной организации (Консорциум CENTRE – с Coinbase и Circle в качестве соучредителей).

Новые участники рынка пытаются избежать этой дилеммы. Они по-прежнему тяготеют к обеспеченной системе, но имеют свои отличительные особенности, что затрудняет классификацию в рамках существующей системы алгоритмических стейблкоинов. Мы рассмотрим три примера.

Fei Protocol



Fei был запущен в конце 1 квартала 2021 года. Как и Frax, Fei использует частично обеспеченную систему, но вместо этого поддерживается исключительно ETH. Стейблкоин Fei (FEI) привязана к 1 доллару США, что подкрепляется инновационными концепциями для поддержания их привязки и обеспечения общей финансовой стабильности протокола.

Вместо того, чтобы брать залоговое обеспечение, Fei вводит механизм, известный как контролируемая протоколом стоимость (Protocol Controlled Value – PCV). По сути, Fei покупает ETH у пользователей через только что сформированный FEI. Затем Fei будет использовать ETH для поддержки своих пулов ликвидности, обеспеченных залогом. Другие распространенные случаи использования включают управление казначейством и страховые фонды. Во время первоначального запуска Fei выделил 100% PCV, финансируемого залогом ETH, в пул Uniswap с использованием торговой пары ETH.

Когда цена FEI превышает 1 доллар, протокол позволяет пользователям формировать новые FEI непосредственно из системы по сниженной цене (аналогично FRAX), используя ETH в качестве оплаты. Таким образом трейдеры снижают цену до тех пор, пока цена не достигнет отметки в 1 доллар. Когда цена FEI ниже 1 доллара, протокол облагает налогом продавцов FEI (налог которых затем сжигается и удаляется из предложения) и награждает дополнительными FEI покупателей (в дополнение к их первоначальной покупке). Торговый алгоритм гарантирует, что сумма налога превысит сумму, которую получают покупатели.

В чрезвычайных ситуациях, когда цена FEI в течение длительного периода находится ниже установленного уровня, FEI может изъять свою ликвидность, обеспеченную PCV, из Uniswap и купить FEI на рынке. В это же время FEI сжигается. Как только привязка будет восстановлена, Fei вернет оставшуюся ликвидность обратно в Uniswap.

У Fei также есть собственный токен управления (TRIBE), который в конечном итоге станет основой для DAO. В будущем владельцы TRIBE смогут принять решение о корректировке распределения PCV и добавлении/корректировке залога.

Reflexer



В отличие от других алгоритмических стейблкоинов, собственный токен Reflexer (RAI) не является стейблкоином с фиксированной привязкой. Запущенный в 1 квартале 2021 года, RAI призван стать стабильным залогом и заменить существующие залоговые активы, такие как ETH или BTC, которые естественно изменчивы. RAI использует модель с избыточным обеспечением на основе ETH и имеет плавающую привязку, которая изначально была установлена на уровне 3,14 доллара.

Reflexer использует принципы режима управляемого плавающего курса, аналогичные тому, как работают центральные банки. Поскольку цены постоянно колеблются, Reflexer разработал систему, в которой рыночные взаимодействия между теми, кто создает RAI и трейдерами (держателями RAI) стимулируются к погоне за выкупной ценой RAI (плавающая привязка), чтобы поддерживать цену RAI относительно стабильной.

Чтобы создать RAI, пользователям необходимо внести ETH в качестве обеспечения с коэффициентом обеспечения не менее 145%. Затем с пользователей взимается комиссия (процентная ставка по займам). На момент написания статьи (май 2021 года) комиссия за стабильность составляет 2% годовых. Однако она является переменной и может быть изменена путем голосования.

Когда цена RAI находится выше плавающей привязки, система понижает привязку. Это позволяет пользователям создавать больше RAI и продавать его обратно за ETH для более высокой прибыли. Когда цена RAI находится ниже плавающей привязки, система повышает привязку. Это делает заимствования более дорогими и стимулирует тех, кто создает RAI, погашать свои кредиты RAI, тем самым выводя RAI из обращения и повышая цену.

В чрезвычайных ситуациях (Урегулирование) протокол отключается и позволяет только тем, кто создает RAI и держателям RAI выкупать ETH-обеспечение из системы по текущей цене выкупа.

У Reflexer также есть еще один собственный токен (FLX), который выступает в качестве кредитора последней инстанции, управляет определенными функциями и позволяет пользователям размещать его в пуле, защищающем систему. Существуют также долговые аукционы, которые создаются для погашения FLX в обмен на RAI – таким образом RAI, полученный на аукционе, будет использоваться для ликвидации долгов из системы. На более длительном временном горизонте FLX должен стать токеном «без управления», постепенно автоматизируя систему с течением времени и сводя к минимуму необходимость управления.

Float Protocol



Float очень похож на FRAX, в части того, как он использует модель сеньоража из двух токенов и частичное обеспечение. Однако, в отличие от FRAX, собственный актив Float (FLOAT) имеет плавающую ставку, начальная цена привязки составляла 1,61 доллара. Токен управления Float (BANK) действует как токен управления и механизм регулирования для поддержки цены FLOAT.

Float использует тот же механизм, что и PCV (контролируемая протоколом стоимость) Fei, где пользователи могут только приобретать недавно выпущенный FLOAT из протокола. Однако Float продает FLOAT на голландском аукционе, где цены сначала указаны по максимально возможной цене и снижаются в сторону минимальной цены. Чтобы приобрести FLOAT, пользователи должны заплатить комбинацией BANK и ETH. Коэффициент оплаты активов зависит от общего спроса на FLOAT и в количестве ETH в хранилище обеспечения протокола (корзина).

Если корзина превышена, лишние ETH используется для покупки FLOAT по целевой цене, а BANK используется для создания FLOAT. ETH (или любые другие будущие торговые активы), полученные на голландском аукционе, затем хранятся в качестве обеспечения в корзине. BANK сжигается всякий раз, когда пользователь создает FLOAT.

Когда цена FLOAT превышает плавающую привязку, любой пользователь может начать аукцион. Первоначально он может быть запущен только по истечении минимум 24 часов, но в будущем ограничение будет удалено, как только команда протокола убедится, что пользователи привыкли к функции аукциона. Как только начинается аукцион, система создает и продает новый FLOAT, начиная с рыночной цены плюс дополнительная премия. Цена снижается с течением времени, пока не достигнет целевой цены.

Когда цена FLOAT ниже плавающей привязки, протокол предлагает купить FLOAT у пользователей в форме обратного голландского аукциона. FLOAT покупается парно с ETH и с только что созданным BANK.

Коэффициент первоначального обеспечения (коэффициент корзины) был установлен на уровне 100% при запуске, но может быть изменен путем голосования руководства. Во время чрезвычайных ситуаций активы, хранящиеся в корзине, могут быть использованы для поддержки плавающей цены, если она ниже ее привязки.

Какое будущее у новых алгоритмических стейблкоинов и стабильных активов?

Старые алгоритмические стейблкоины ставили эффективность капитала выше всего остального. Привязки были фиксированными и полностью зависели от индивидуальной механики теории игр, в то время как методы начальной загрузки по большей части были не протестированы.

Стейблкоины стали известны из-за своей привязки к доллару США, но новые разработки в этой области изменили само это определение. Теперь у нас есть новый класс активов, известный как алгоритмические стабильные активы.

Мы рассматриваем FLOAT и RAI как алгоритмически стабильные активы в первую очередь потому, что они имеют плавающую привязку. Но основное внимание следует уделять тому, могут ли эти активы поддерживать стабильную цену или нет. Чтобы ответить на этот вопрос, мы рассмотрели три основных фактора.

1. Обеспечение

Новые алгоритмические стейблкоины применяют более консервативный подход, при котором обеспечение имеет приоритет над эффективностью капитала.

Подход Fei к контролируемой протоколом стоимости (PCV) использует «обеспечение ликвидности», когда обеспечение автоматически перенаправляется в пулы ликвидности Uniswap с участием Fei. Голосование (через собственный токен TRIBE) позволит пользователям контролировать соотношение PCV, которое фактически является коэффициентом обеспечения.

Это похоже на коэффициент обеспечения корзины Float. Однако Float имеет дополнительное преимущество в виде плавающей привязки и токена управления (BANK), который необходим для приобретения FLOAT. Это увеличивает его стоимость и помогает «хранить» сверхволатильность в токенах BANK, а не в FLOAT. BANK может быть использован в качестве залога, хотя Fei также можно было бы использовать для обеспечения TRIBE, хотя и с меньшей инерционной пользой, поскольку он меньше используется. Другими словами, как FLOAT, так и Fei, позволяют рыночным силам определять идеальное соотношение залогового обеспечения (аналогично FRAX).

Противоположное решение применяется в RAI Reflexer, который сверхобеспечен и менее подвержен событиям «черного лебедя». Существует минимальное требование к обеспечению, но нет максимального. Действительно, можно утверждать, что Reflexer имеет высокий шанс успеха, поскольку он является форком Dai от Maker (с несколькими обеспечениями) и сумел сохранить свою стабильность после «черного четверга» (несмотря на то, что на это ушло много времени). Кроме того, RAI не ограничивается фиксированной привязкой, что придает ему большую гибкость.

2. Стимулы и сдерживающие факторы для трейдеров

Алгоритмические стейблкоины и стабильные активы предназначены для рынка, чтобы помочь ему в качестве некого якоря. Первые поколения алгоритмов сосредоточились на вознаграждении «правильного» поведения пользователей (то есть арбитражеров). Этот тренд все еще продолжается для новых алгоритмических стейблкоинов и стабильных активов, которые обладают аналогичной механикой вознаграждения за создание актива, когда цена выше привязки. Однако существует заметная разница в подходе во время дефляционной фазы.

Новые протоколы используют тактику «отрицательного подкрепления». Fei штрафует продавцов торговым налогом всякий раз, когда FEI продается ниже установленного уровня. Reflexer действует косвенно, повышая ставку заимствования за счет повышения привязки, что побуждает заемщиков погашать свои кредиты (аналогично Maker). Float немного отличается, поскольку позволяет пользователям "сражаться" с ним на обратном голландском аукционе. Вместо того, чтобы наказывать или вознаграждать пользователей, Float позволяет решать все рынку.

3. Полномочия в чрезвычайных ситуациях

Возможно, самым интересным развитием протоколов является стремление к усилению полномочий. Системный дизайн каждого протокола имеет встроенные функции для защиты своего рынка, когда его собственный актив значительно обесценивается. Можно провести параллели с традиционными финансами, где регулирующие органы или централизованные финансовые органы вмешиваются во время финансовых кризисов.

Fei по существу закрывает доступ к ликвидности, удаляя свою ликвидность, обеспеченную PCV, из пулов Uniswap – аналогично тому, как страна может ввести ограничения на снятие средств в банке. Затем Fei продаст свои активы и предложит выкупить избыток FEI с рынка. Float использует аналогичную тактику, за исключением того, что покупки финансируются из корзины. Reflexer останавливает все заимствования и разрешает только погашение кредитов.

Сопутствующие риски

Нельзя не подчеркнуть, что алгоритмические стейблкоины все еще находятся в экспериментальной фазе. Протоколы все еще пытаются выяснить, как успешно работать без значительных колебаний цен.

Многие алгоритмические протоколы стейблкоинов также в значительной степени зависят от компетентных арбитражеров для поддержания привязки цены. Если вы не уверены в том, как работает протокол, вы окажетесь в крайне невыгодном положении, если попытаетесь конкурировать с опытными арбитражерами (или даже ботами).

Алгоритмические стейблкоины требуют сильного сообщества, которое верит в основы проекта. Чаще всего краткосрочные спекулянты будут использовать свои кредитные плечи для контроля и манипулирования ценой. На децентрализованном рынке только объединенное сообщество может преодолеть эту дилемму.

Другими словами, вам потребуется значительное время и ресурсы, чтобы понять каждый проект. Только тогда вы сможете решить, может ли он конкурировать со многими альтернативными стейблкоинами/стабильными активами, которые уже имеют присутствие на рынке.

Стейблкоины, заслуживающие упоминания



Empty Set Dollar v2 (ESD)

ESD регулирует стабильность монеты двумя токенами, вводя новый токен ESDS. ESD v2 (также известный как Continuous ESD) будет очень похож на Frax в том, что у него будет частично обеспеченный стейблкоин, включающая банковский резерв, поддерживаемый USDC. Вместе с ESDS эти две новые функции, как мы надеемся, помогут снизить волатильность токенов ESD.



Dynamic Set Dollar v2 (DSD)

В то время как большинство протоколов стейблкоинов сосредоточены на частичной или полностью обеспеченной модели, DSD (форк ESD) считает, что это отвлекает от идеала децентрализации. Несмотря на первоначальную неудачу, DSD обновила свою модель, представив новый токен CDSD, который частично можно обменять 1:1 на токены DSD. Идея состоит в том, чтобы перенести волатильность токенов DSD на CDSD – аналогично модели Frax, но без какого-либо обеспечения.



Gyroscope (GYR)

Механика Gyroscope представляет собой объединение нескольких алгоритмических протоколов стейблкоинов со своей собственной изюминкой. GYR имеет избыточное обеспечение и обеспечен несколькими активами, разделенными на отдельные хранилища (аналогично Maker). Как и в большинстве алгоритмических стейблкоинов, существует арбитражная механика, но с добавлением дополнительного кредитного механизма с привлечением заемных средств. Во время кризиса пользователи получат более выгодную ставку погашения, чем дольше они будут ждать погашения своих кредитов.



TerraUSD (UST)

Подобно DSD v2, UST представляет собой модель с двумя токенами без обеспечения (наряду с LUNA) и полностью полагается на арбитраж для поддержания привязки к 1 доллару. На момент написания статьи UST является единственным успешным протоколом алгоритмических стейблкоинов с поддержанием стабильной ценовой привязки – вероятно, из-за высокого спроса и процветающей экосистемы (Terra), которая включает сеть майнинга в свои механизмы ценовой стабильности.

Вывод

Алгоритмические стейблкоины - это эффективный подход DeFi к замене центрального банка, в то время как алгоритмические стабильные активы - это способ DeFi подражать золотому стандарту и создавать надежное цифровое обеспечение. В традиционных финансах успешная денежно-кредитная система требует компетентного и независимого финансового органа. В DeFi компетентность исходит от псевдоанонимных людей, которые заинтересованы в сотрудничестве и рациональных действиях.

Успешные алгоритмические стейблкоины и стабильные активы требуют более длительных временных рамок, чтобы проявить себя, особенно во время кризиса. Ни краткосрочные стимулы, ни краткосрочные спекуляции сами по себе не являются устойчивыми - они должны стать чем-то большим, чем просто мысленный эксперимент, и обеспечить экономическую пользу за счет широкого внедрения. Будет интересно проследить за тем, как будут работать алгоритмические стейблкоины и стабильные активы в ближайшие годы.

Рекомендуемая литература

1. Понимание рисков токенов ребейза с помощью анализа смарт-контракта
<https://www.coingecko.com/buzz/understanding-risk-of-rebase-tokens-through-smart-contract-analysis>
2. Понимание Fei, Float and Rai
<https://medium.com/float-protocol/float-and-the-money-gods-5509d41c9b3a>
3. Изучение ключевых факторов успеха алгоритмических стейблкоинов
<https://messari.io/article/the-art-of-central-banking-on-blockchains-algorithmic-stablecoins>
4. Глубокий анализ моделей ребейза и сеньоража
<https://insights.deribit.com/market-research/stability-elasticity-and-reflexivity-a-deep-dive-into-algorithmic-stablecoins/>
5. Влияние Uniswap на алгоритмические стейблкоины
<https://medium.com/stably-blog/what-uniswaps-liquidity-plunge-reveals-about-stablecoins-4fcbee8d210c>

ГЛАВА 7: ДЕЦЕНТРАЛИЗОВАННЫЕ ПРОИЗВОДНЫЕ ФИНАНСОВЫЕ ИНСТРУМЕНТЫ (ДЕРИВАТИВЫ)

Принятие цифровых активов привело к созданию сложных финансовых продуктов для пользователей и трейдеров. В настоящее время использование крипто-деривативов более распространено на централизованных платформах, таких как Binance Futures, Deribit, FTX и Bybit.

С ростом децентрализованных платформ деривативов трейдеры теперь также могут торговать крипто-деривативами. В этой главе мы рассмотрим децентрализованные деривативы в трех отдельных разделах – децентрализованные бессрочные активы, децентрализованные опционы и синтетические активы.

Децентрализованные бессрочные деривативы

Являясь одним из самых популярных деривативов в криптопространстве, бессрочные свопы позволяют пользователям открывать позицию с кредитным плечом по фьючерсному контракту без даты истечения срока действия. Ранее бессрочные деривативы были доступны только на централизованных биржах, однако децентрализованные платформы, такие как Perpetual Protocol и dYdX, с тех пор проложили путь для широкого сообщества DeFi и дали доступ к позициям с использованием заемных средств (с кредитным плечом), полностью контролируя свои собственные средства.

Perpetual Protocol



Perpetual Protocol – это децентрализованный протокол, который предлагает торговлю бессрочными контрактами, позволяя пользователям открывать длинные (лонг) или короткие позиции (шорт) с кредитным плечом до 10x на различных

криптоактивах. Для достижения этой цели в Perpetual Protocol используется уникальный подход виртуальных автоматизированных маркетмейкеров (vAMM).

Функционируя аналогично AMM Uniswap и Balancer, трейдеры могут совершать транзакции непосредственно через vAMM. Основное отличие заключается в «виртуальной» части.

В обычных AMM активы хранятся в смарт-контракте, а биржевая цена каждого актива определяется с помощью определенной математической функции. Виртуальные AMM в Perpetual Protocol вообще не хранят никаких активов.

Вместо этого реальные активы хранятся в хранилище смарт-контрактов, номинированном в USDC, которое становится обеспечением для пользователей при открытии позиции с привлечением заемных средств. Общая сумма средств в хранилище, по сути, определяет предел прибыли трейдеров. Каждый бессрочный контракт будет иметь свой собственный конкретный виртуальный AMM, но все они защищены страховым фондом протокола.

Perpetual Protocol способен обеспечить повышенную скорость торговли и минимальные стоимость газа, используя сайдчейн xDai для совершения сделок. С помощью виртуального AMM пользователи получат доступ к высокой ликвидности и низкому проскальзыванию для своих торговых нужд.

Как и во всех формах торговли бессрочными контрактами, процентные ставки и коэффициенты ликвидации являются важнейшими аспектами Perpetual Protocol. Процентные ставки устанавливаются на почасовой основе, в то время как коэффициенты ликвидации устанавливаются на уровне 6,25% от запаса актива. Это означает, что трейдеры с позициями, которые опускаются ниже коэффициента запаса 6,25%, столкнутся с риском быть ликвидированными ботами-хранителями. Боты-хранители заработают 20% от ликвидированной прибыли, а оставшаяся часть будет отправлена в страховой фонд протокола.

Протокол имеет свой собственный токен PERP, который в первую очередь служит токеном управления для платформы. Владельцы токенов PERP получают право голоса пропорционально количеству токенов. Кроме того, они могут поставить PERP на фиксированный период, чтобы получить еще больше PERP и долю комиссии за транзакции протокола в USDC.

Этот фиксированный период, известный как эпоха, длится семь дней. Держатели токенов не могут выводить свои средства до конца каждой эпохи. Комиссия за транзакцию протокола в USDC может быть выплачена сразу же после конца эпохи, в то время как вознаграждение в виде PERP заблокировано на срок до 6 месяцев. Те, кто застекал PERP на фиксированный период могут быть уверены в нулевых непостоянных потерях, но они все равно будут подвержены риску из-за волатильности цены самого токена PERP.

Это все, что вам нужно знать о Perpetual Protocol. По состоянию на апрель 2021 года торговля ведется в реальном времени в блокченах Ethereum и xDai, так что вы можете пойти и попробовать.

dYdX



dYdX – это децентрализованный протокол обмена для кредитования, заимствования, спотовой торговли, маржинальной торговли и торговли бессрочными своп-контрактами. Один из первых проектов, специализирующихся на децентрализованной бессрочной торговле, dYdX поддерживает три актива для спотовой и маржинальной торговли – ETH, USDC и DAI. Для бессрочных свопов доступны 11 различных контрактов, включая BTC, ETH, AAVE и LINK.

dYdX имеет некоторые общие характеристики с другими платформами кредитования и заимствования, такими как Aave и Compound, которые позволяют пользователям вносить свои активы для получения процентов или использовать свои депонированные активы в качестве обеспечения для заимствования. Тем не менее, dYdX выделяется тем, что включает маржинальную торговлю с кредитным плечом до 5x, используя либо DAI, либо USDC. Пользователи также могут использовать кредитное плечо до 10x при торговле бессрочными контрактами на dYdX.

Кредитование на dYdX является гибким и автоматически согласовывается с заемщиками, поэтому нет периода ожидания, прежде чем вы сможете начать получать проценты по депозитам. Процентные платежи увеличиваются каждый раз, когда транзакция совершается с использованием этого актива.

Процентные ставки динамически обновляются в зависимости от уровня использования – более высокое использование приводит к более высоким процентным ставкам для кредиторов. Для заемщиков требуется первоначальный коэффициент обеспечения в размере 125%, в то время как минимальный коэффициент в 115% необходимо поддерживать, чтобы предотвратить автоматическую ликвидацию.

dYdX предлагает спотовым трейдерам функции, аналогичные функциям централизованных бирж, такие как рыночные, лимитные и стоп-ордера. Торговые сборы за маржинальные или спотовые позиции ограничены только участниками, где взимаемая сумма составляет либо 0,3%, либо переменные затраты на газ, в зависимости от того, стоимость чего выше. Чтобы минимизировать стоимость газа, трейдерам следует обращать внимание на размер заказа – платформа взимает дополнительные сборы при небольших заказах для оплаты сборов за газ для завершения транзакции.

Для бессрочных рынков dYdX все контракты обеспечены залогом в USDC. Однако в каждом контракте используются разные оракулы, размеры ордеров и маржинальные требования. Ставки финансирования непрерывно начисляются каждую секунду до тех пор, пока позиция остается открытой. Ставки пересчитываются каждый час и представлены в виде 8-часового тарифа, аналогичного Binance Futures. К сожалению, бессрочные контракты на dYdX недоступны для жителей Соединенных Штатов.

В 1 квартале 2021 года dYdX в партнерстве со Starkware разработала торговый протокол уровня 2, позволяющий проводить более быстрые и дешевые транзакции. Используя механизм масштабируемости, известный как StarkEx, сделки будут согласовываться вне блокчейна с использованием роллапов с доказательством с нулевым разглашением (zK-Rollup) и будут рассчитываться в основной сети Ethereum. Теперь пользователи могут получить доступ к рынкам уровня 2, создав ключ Stark, используемый для идентификации вашей учетной записи на втором уровне на dYdX и отправки транзакции для регистрации учетной записи в блокчейне.

Сравнение Perpetual Protocol и dYdX (уровень 1)

Параметр	Perpetual Protocol	dYdX (уровень 1)
Поддерживаемые контракты	BTC, ETH, YFI, LINK, DOT, SNX	BTC, ETH, LINK, AAVE, UNI, SOL, SUSHI, YFI, 1INCH, AVAX, DOGE
Модель обмена	Виртуальный АММ	Книга ордеров
Максимальное плечо	10x	10x
Начальная маржа	10%	10%
Минимальная маржа	6,25%	7,5%
Расчет начисления процентов	1 час	1 секунда
Комиссия за транзакцию	0,1%	Продажа: -0.025% Покупка: наибольшее из 0.2% или стоимости газа за транзакцию

С точки зрения специфики контрактов, обе платформы предлагают очень схожие варианты кредитного плеча и маржинальные требования для своих соответствующих рынков. Perpetual Protocol предлагает более широкий спектр активов и гораздо более щадящую ставку финансирования для открытых позиций, показывая в среднем 60 миллионов долларов в ежедневном объеме торгов по сравнению с 15 миллионами долларов, сделанными в dYdX (уровень 1) в первом квартале 2021 года. С другой стороны, dYdX использует «экспоненциальный» подход, постоянно принося пользу своим держателям позиций, даже если более высокие сборы могут отпугнуть мелких трейдеров.

На наш взгляд, dYdX может иметь потенциал для конкуренции с Perpetual Protocol после внедрения как технологии уровня 2, так и большего количества рынков для популярных токенов, таких как Aave и Uni, и с более низкими комиссиями.

Бессрочные деривативы, заслуживающие упоминания



Futureswap

Futureswap – это децентрализованная биржа **бессрочными контрактами**, которая позволяет пользователям торговать с кредитным плечом до 10x на любых парах ERC-20.



NCDEX

NCDEX – это децентрализованный протокол бессрочного обмена на основе AMM, который в настоящее время использует вторую итерацию их протокола Mai Protocol. Любой пользователь может создать **торговлю бессрочными контрактами**, если есть ценовая информация для базового актива и токенов ERC-20 для использования в качестве обеспечения.



Injective Protocol

Основанная на блокчейне Injective, эта платформа деривативов уровня 2 поддерживает полностью децентрализованную книгу ордеров и двунаправленный мост для перевода токенов в Ethereum и обратно. По состоянию на апрель 2021 года он все еще находится в тестовой сети.

Децентрализованные опционы

Опционы уже давно являются основным элементом традиционных финансов, предлагая покупателям возможность делать ставки на движение цен в любом направлении, чтобы хеджировать стоимость своих активов или увеличить свою доходность с минимальным капиталом. Поскольку DeFi продолжает создавать шумиху во всей криптоиндустрии, вполне естественно, что появляются и протоколы децентрализованных опционов.

Криптовладельцы исторически торговали опционами на централизованных биржах, таких как Deribit, но существует запрос на протоколы децентрализованных опционов. В этой главе мы рассмотрим два ведущих протокола децентрализованных опционов, Hegic и Oryx.

Hegic



Hegic – это децентрализованный сетевой протокол, который позволяет пользователям покупать два вида американских опционов: пут и колл, а также размещать опционы на ETH и WBTC. Пользователи также могут продавать опционы, являясь провайдерами ликвидности, получая доход. Используя интерфейс платформы, пользователи могут настраивать условия опционов, которые они хотят приобрести, такие как цена исполнения и дата истечения срока действия.

Цены на опционы будут автоматически рассчитаны после выбора условий, включая расчетную комиссию в размере 1% от приобретенных размеров опционов. Хотя опционы не подлежат торговле, пользователи могут использовать их в любое время, поскольку ликвидность заблокирована в опционном контракте.

Hegic работает с использованием модели пула ликвидности. Другими словами, пользователи объединяют свои средства и используют их в качестве обеспечения для страхования всех проданных опционов. По состоянию на апрель 2021 года существует два отдельных пула для ETH и WBTC. Провайдеры ликвидности блокируют ETH или WBTC и получают определенное количество write-токенов в соответствии с предоставленным активом.

Write-токены представляют собой требования провайдера о премиях, уплаченных пользователями за покупку опционов. Хотя любой желающий может приобрести опционы в пулах ликвидности, максимальный лимит покупки для каждого пула установлен на уровне 80% от общего базового обеспечения.

Следует отметить то, что в Hegic, вы можете получать вознаграждение за использование платформы. У HEGIC есть программа майнинга ликвидности, которая вознаграждает пользователей, которые ставят свои write-токены, и вознаграждает покупателей опционов в зависимости от размера и

продолжительности приобретенных опционов. Эти награды приходят в виде токенов rHEGIC, которые могут быть обменены на токены HEGIC, как только будут достигнуты определенные вехи на платформе Hegic.

Токены HEGIC также могут быть застейканы, чтобы заработать комиссии протокола, где 100% расчетных сборов от обоих пулов распределяются владельцам лотов Hegic. Чтобы владеть таким лотом, вам понадобится 888 000 HEGIC (около 120 000 долларов по состоянию на 25.07.2021). Если это перебор для вас, вы можете делегировать любую сумму в существующий лот на сайте www.hegicstaking.co.

Hegic накопила более 50 миллионов долларов общей заблокированной стоимости (TVL) и обеспечила более 22 миллионов долларов торгового объема за один день. С этими цифрами Hegic остается одним из лучших протоколов децентрализованных опционов.

И это в значительной степени все о Hegic! Далее мы рассмотрим другую децентрализованную платформу опционов под названием Оруп.

Оруп



Оруп – одна из первых платформ децентрализованных американских опционов. Первая версия, Oryp V1, позволяет создавать токенизованные американские опционы в виде oTokens, блокируя 100% базового актива в качестве обеспечения. Это гарантирует, что держатели всегда смогут воспользоваться опционами, поскольку они полностью обеспечены.

При условии наличия достаточной ликвидности у её провайдеров, Оруп может предложить широкий спектр опционов по таким активам, как ETH, WBTC, UNI и SNX, хотя и с фиксированной продолжительностью и ценой исполнения. oTokens может быть реализован путем отправки достаточного количества стейблкоинов и сжигания oTokens в обмен на базовый актив, или он может быть перепродан другим сторонам через Uniswap. Кроме того, Оруп не взимает никаких дополнительных комиссий за транзакции или расчеты.

Вторая версия, Oryun V2, была запущена с дополнительными функциями, такими как автоисполнение опционов и флэш-создание токенов, что является инновационным развитием существующей концепции флэш-займов, популяризированной Aave. Последняя итерация предлагает европейские опционы через систему книг ордеров, аналогичную Deribit, но в настоящее время ограничена WETH и с меньшим диапазоном цен исполнения и дат истечения срока действия.

Сравнение Hegic и Oryun

Какие преимущества у протоколов перед друг другом? В таблице ниже мы сравниваем обе платформы на основе нескольких параметров.

Параметр	Hegic	Oryun V1	Oryun V2
Тип опциона	Американский	Американский	Европейский
Модель ликвидности	Пул с одним активом	Пул Uniswap	Книга ордеров
Тип расчета	Деньги	Деньги	Деньги
Активы обеспечения	ETH, WBTC	ETH, WBTC, UNI, SNX	WETH, WBTC
Доход выплачивается в	ETH	DAI, ETH, USDC	USDC
Необходимо обеспечение	100%	100%	100%

Здесь мы видим, что обе платформы опционов должны быть полностью обеспечены продавцами опционов, но они сильно отличаются с точки зрения моделей ликвидности и количества поддерживаемых активов.

Американские опционы, по-видимому, предпочтительны для обоих протоколов из-за степени гибкости, которую они предлагают в быстро меняющемся пространстве DeFi. Это контрастирует с европейскими опционами, которым отдают предпочтение централизованные биржи деривативов, такие как Deribit. В Oryun V2 небольшие книги ордеров с меньшим выбором цен исполнения указывают на более низкий спрос на продукты с большими временными ограничениями, учитывая изменчивый характер пространства цифровых активов.

Децентрализованные опционы, заслуживающие упоминания



FinNexus позволяет пользователям создавать опционы практически на любой актив, при условии наличия надежного источника цены. Протокол использует систему единого пула с несколькими активами (Multi-Asset Single Pool - MASP), которая позволяет размещать опционы по различным базовым активам, используя в качестве обеспечения только один тип активов.



Auctus – это протокол DeFi, который позволяет пользователям выполнять флэш-исполнения, в которых им не нужно владеть токенами исполнения, чтобы выполнить опционы. Они также предлагают фармить через свои Auctus-хранилища и специальный раздел для внебиржевой торговли опционами.



Premia предлагает вторичную торговую площадку для пользователей, которые могут покупать и продавать свои опционы. Пользователи могут создавать, переводить и использовать несколько типов опционов с меньшим количеством транзакций, экономя как время, так и затраты на газ.



Antimatter позиционирует себя как Uniswap опционов, предоставляя возможность обмена на свои продукты с бессрочными опционами. Пользователи могут создавать длинную или короткую позицию, покупая эти поляризованные опционные токены, которые можно обменять, не беспокоясь о сроках исполнения.



С помощью протокола Siren пользователи могут выбирать, быть ли продавцом или покупателем опционов, купив bTokens или wTokens определенной серии опционов у автоматизированного маркетмейкера SirenSwap. bTokens представляют сторону покупателя, позволяя держателям выполнять опционы, в то время как wTokens представляют сторону продавца, которая будет использоваться для снятия обеспечения или получения платежа при исполнении.

Синтетические активы

Синтетические активы – это активы или комбинация активов, которые имеют ту же стоимость или эффект, что и другие активы. Синтетические активы отслеживают стоимость базовых активов и позволяют использовать активы без необходимости хранения самого фактического актива.

Примеры синтетических активов включают практически любые отслеживаемые активы, от реальных акций до цен на газ Ethereum и даже показателей на сайте CoinGecko. Пользователи, торгующие этими синтетическими активами, могут иметь финансовые позиции в этих активах, не владея самими фактическими активами.

В этой главе мы сравним два крупнейших протоколов в секторе синтетических активов DeFi, а именно Synthetix и UMA.

Synthetix



Мы подробно рассмотрели Synthetix в нашей книге «Что такое DeFi: Для начинающих», но вот небольшой обзор.

Synthetix – это децентрализованная платформа для создания и торговли синтетическими активами, известными как Синты (Synths), за счет обеспечения, предоставляемого пользователями платформы.

Синты позволяют пользователям отслеживать стоимость базового актива, не покупая сам фактический актив. Существует два типа Синтов – Обычные Синты (например, sDEFI) и Обратные Синты (например, iDEFI). Не у всех Синтов есть обратный аналог.

Синты могут быть созданы для различных классов активов, таких как криптовалюты, фиатные валюты, сырьевые товары, фондовые индексы и акции. Цены на активы отслеживаются с помощью Chainlink, децентрализованного оракула, который собирает данные о ценах из нескольких источников.

Синты создаются с использованием избыточного обеспечения, концепция аналогична Maker в создании Dai. Чтобы создать Синт, пользователям придется поставить токен платформы Synthetix (SNX) в качестве залога. Поскольку стоимость SNX может быстро изменяться в любом направлении, для снижения рисков ликвидации требуется большой коэффициент обеспечения в размере 500%

Чтобы поддерживать коэффициент обеспеченности не менее 500%, пользователи могут сжигать Синты, если они ниже целевого коэффициента, или создавать больше Синтов, если они превышают пороговое значение. Обратите внимание, что по состоянию на январь 2021 года единственный Синт, который пользователи могут создавать, это sUSD.

Синты в основном торгуются на бирже Synthetix, децентрализованной бирже, которая полагается не на книги ордеров, а на ликвидность пользователей. Биржа Synthetix позволяет пользователям торговать напрямую через смарт-контракт, который постоянно поддерживает достаточную ликвидность, что снижает риск проскальзывания. Это особенно полезно для крупных сделок, которые в противном случае привели бы к значительному проскальзыванию цен на других биржах.

Чтобы стимулировать стейкинг и создание Синтов, пользователи имеют возможность получать комиссионные за обмен и вознаграждения за стейкинг SNX. Сборы, полученные в результате торговли на бирже Synthetix, отправляются в пул, где вкладчики SNX могут забрать свою долю собранных сборов. Вкладчики также могут претендовать на вознаграждение токенами SNX до тех пор, пока их коэффициент обеспечения не опустится ниже текущего порогового значения.

Теперь, когда мы освежили в памяти информацию по Synthetix, давайте погрузимся в проект под названием UMA.

UMA



UMA (Universal Market Access) – это децентрализованный протокол для создания и реализации синтетических активов в сети Ethereum. UMA предоставляет инфраструктуру для построения безопасных финансовых контрактов, используя две основные части своей технологии - основу для создания и развертывания производных инструментов, а также оракул для их обеспечения, известный как Механизм проверки данных (DVM – Data Verification Mechanism).

В отличие от Synthetix, эти финансовые контракты разработаны так, чтобы быть «бесценными», что означает, что они не требуют, чтобы ценовая информация в блокчейне была указана. Вместо этого контракты будут основываться на надлежащем обеспечении контрагентов по контрактам. Это стимулируется вознаграждением пользователей, которые идентифицируют недостаточно обеспеченные позиции. Для дальнейшей проверки ненадлежащего обеспечения в контрактах может использоваться DVM

DVM является оракулом, созданным для ответа на запросы о ценах по этим контрактам, и используется только для разрешения споров, касающихся ликвидации и урегулирования контрактов. Запросы на цену поступают от держателей токенов UMA, которые голосуют за наиболее точное значение в определенное время. Держатели токенов отдают свои голоса в течение нескольких дней.

Как только голоса будут приняты, цена или значение с наибольшим количеством голосов будет передано обратно в финансовый контракт. Залоговое обеспечение затем распределяется среди держателей токенов на основе этой проголосованной цифры. DVM построен таким образом, что существует экономическая гарантия в отношении обоснованности запрашиваемой цены.

По сути, это означает, что злоумышленники лишены мотивации. Это достигается за счет обеспечения того, чтобы стоимость искажения DVM, взятая как общая стоимость более половины токенов для голосования UMA, всегда превышала прибыль от действий злоумышленников или общего обеспечения, доступного в рамках контракта. Это неравенство поддерживается путем корректировки цены токенов за счет дополнительных комиссий по контрактам.

Помимо DVM, в экосистеме UMA также есть несколько других важных участников. К ним относятся:

Спонсоры токенов – физические лица, которые вносят залог в смарт-контракт для создания синтетических токенов. Они несут ответственность за поддержание своего собственного коэффициента обеспечения, чтобы предотвратить ликвидацию.

Ликвидаторы – сеть наблюдателей, которые стимулируются для проверки того, правильно ли обеспечена позиция с помощью ценовых каналов вне блокчейна. У участников спора есть 2-часовая задержка для проверки точности ликвидации до ее завершения.

Спорщики – это мотивированные пользователи, которые отслеживают контракты. Они ссылаются на свои цены вне блокчейна, чтобы подтвердить событие ликвидации. Если ликвидация не происходит, будет вызван в действие DVM.

DVM – оракул будет стремиться разрешить спор, предложив провести голосование по наиболее точной оценке актива в заданный момент времени.

Держатели токенов – держатели токенов UMA коллективно голосуют за цену актива в определенное время. Держатели токенов будут ссыльаться на данные вне блокчейна, чтобы предоставить информацию DVM. Затем DVM подсчитает голоса и сообщит о наиболее согласованной цене в цепочке.

Если спорщик прав, то спорщик и затронутый спонсор токенов будут вознаграждены. Если ликвидатор прав, то ликвидатор будет вознагражден, в то время как спорщик будет наказаны, а спонсор токенов потеряет часть средств из-за завершенной ликвидации.

Некоторые продукты, созданные с использованием платформы UMA, включают синтетические «доллары доходности», которые представляют собой токены, приближающиеся к определенной стоимости по истечении срока погашения, а также токены uGAS, которые можно использовать для спекуляций на ценах на газ Ethereum. UMA также представила колл-опционы по популярным токенам DeFi, таким как Sushi и Balanced, а также свои собственные KPI-опционы UMA.

Эти KPI-опционы отслеживают TVL UMA и его ценовые показатели, определяя сумму UMA, которую владелец опциона может выкупить при погашении.

Теперь, когда вы знаете немного больше об UMA и о том, как она работает, давайте сравним эти две платформы (Synthetix и UMA) синтетических активов.

Сравнение Synthetix и UMA

Параметры	Synthetix	UMA
Синтетический токен	Synths	uTokens
Основные активы	Фиатные, криптовалютные, сырьевые товары, фондовые индексы, акции	Виртуально любой актив
Оракул	Chainlink	Data Verification Mechanism
Коэффициент обеспечения	500 %	Зависит от токена
Возможность вклада токенов	Да	Да

Как Synthetix, так и UMA предлагают синтетические активы с избыточным обеспечением, которые могут служить в качестве посредников для широкого спектра активов. На Synthetix стоимость Синтов и коэффициент обеспечения определяются ценовой информацией в блокчейне.

В UMA урегулирование синтетических контрактов поддерживается за счет стимулирования поведения участников сети. Благодаря гораздо более гибким требованиям к обеспечению, основанным на глобальном коэффициенте обеспечения для всех спонсоров токенов, мы можем видеть, что UMA может стать более эффективной платформой с точки зрения капитала. Однако у Synthetix есть преимущество в опциях, так как он поддерживает более 50 Синтов в своем каталоге.

Более того, Synthetix построила экосистему вокруг Синтов, при этом обмен между перекрестными активами dHEDGE и Curve Finance являются одними из основных факторов спроса. dHEDGE, децентрализованная платформа управления активами, позволяет пользователям инвестировать sUSD в различные инвестиционные портфели. Выбранные менеджеры портфелями затем будут менять sUSD на другие синтетические активы в рамках своей стратегии. С другой стороны, обмен между активами Curve Finance используют Synthetix в качестве моста, позволяя трейдерам обменивать активы на сумму до десятков миллионов долларов с нулевым или небольшим проскальзыванием.

С точки зрения ликвидности, еще предстоит выяснить, сможет ли UMA конкурировать, не имея специальной платформы для торговли этими активами. Его биржевые объемы также невелики, и ежедневный объем торгов составляет всего около 20 миллионов долларов. Тем не менее, синтетическим активам еще предстоит пройти долгий путь, прежде чем мы увидим массовое розничное и институциональное внедрение.

Синтетические активы, заслуживающие внимания



Mirror Protocol

Доступный как в блокчейнах Ethereum, так и в блокчейнах Terra, Mirror Protocol выпускает синтетические активы, называемые mAssets, которые имитируют цену реальных активов, таких как акции и индексы. Некоторые из предложений включают mAMZN и mQQQ.



DEUS Finance

Протокол DeFi, который позволяет пользователям получать данные от оракулов и маркировать их как mAssets. mAssets-активы привязаны 1:1 к их реальным аналогам с использованием данных по ценам оракулов.

Сопутствующие риски

При работе с децентрализованными платформами деривативов важно отметить, что торговля с использованием заемных средств и использование деривативов является весьма рискованным делом. Поддержание здорового соотношения залогового обеспечения и отслеживание ликвидационной цены ваших позиций имеют важное значение для безопасной навигации по этому конкретному разделу DeFi.

Поскольку синтетические активы в основном полагаются на оракулов в качестве основного источника ценовой информации, ложные данные могут привести к нежелательным последствиям. Кроме того, поскольку синтетические активы в основном создаются путем внесения залога, может возникнуть нехватка ликвидности для этих активов, что приведет к резкому искажению цен по сравнению с реальными активами.

В случае с опционами убедитесь, что вы можете своевременно выполнять условия опциона, так как некоторые платформы не предлагают функции автоматического исполнения. Поскольку открытый интерес продолжает расти, следует учитывать большие периоды истечения срока действия опционов, поскольку волатильность имеет тенденцию к увеличению.

Вывод

Децентрализованные деривативы и синтетические активы предлагают обычным пользователям возможность участвовать на ранее недоступных рынках или рынках, которых не существовало. Эти продукты были упрощены для удобства пользователя и больше не предназначены для избранных. Пользователи также теперь могут участвовать в этих рынках деривативов без посредника.

Это конкретный класс DeFi все еще находится в относительно зачаточном состоянии, и по состоянию на 1 апреля 2021 года общая заблокированная стоимость составляет менее 10% всего пространства. Действительно, начальная загрузка ликвидности – это проблема, с которой сталкивается почти каждый перспективный проект DeFi, и производные финансовые инструменты не являются исключением. Даже при наличии стимулов сама природа этих продуктов с изначально более высокой волатильностью может показаться перевешивающей вознаграждение для участников.

Хотя такие протоколы, как Charm и Perpetual Protocol, могут работать с минимальной ликвидностью, им еще предстоит пройти долгий путь, прежде чем они смогут конкурировать с крупными централизованными биржами, которые могут предлагать большие объемы и более высокое кредитное плечо до 125x.

Рекомендуемая литература

Децентрализованные бессрочные активы

1. Documentation and Frequently Asked Questions about Perpetual Protocol

<https://docs.perp.fi/>

2. Research, Insights, and Announcements from dYdX

<https://integral.dydx.exchange>

3. The latest news from dYdX

<https://dydx.exchange/blog>

Децентрализованные опционы

1. Articles and announcements from Hegic

<https://medium.com/hegic>

2. Hegic Protocol - On-chain Options Trading Protocol

<https://defipulse.com/blog/hegic-protocol-on-chain-options-trading-protocol/>

3. Opyn Review

<https://defirate.com/opyn/>

4. Beginner's Guide to Options: Opyn V2

<https://medium.com/opyn/a-beginners-guide-to-defi-options-opyn-v2-4d64f91acc84>

Синтетические активы

1. Documentation & System Overview of Synthetix

<https://docs.synthetix.io/>

2. The latest news and announcements about Synthetix

<https://blog.synthetix.io/>

3. What is Synthetix? Everything you need to know about one of the leading DeFi protocols

<https://medium.com/coinmonks/what-is-synthetix-everything-you-need-to-know-about-one-of-the-leading-defi-protocols-bc19bdd2949c>

4. UMA Documentation

<https://docs.umaproject.org/>

5. List of Projects using UMA

<https://umaproject.org/projects.html>

6. UMA: Universal Market Access. Interview with Allison Lu

<https://defiprime.com/uma>

ГЛАВА 8: ДЕЦЕНТРАЛИЗОВАННОЕ СТРАХОВАНИЕ

По мере запуска проектов DeFi и быстрого внедрения инноваций в существующие проекты мы наблюдаем увеличение числа взломов и эксплойтов, приводящих к значительным потерям.

Развитие DeFi неизбежно остановится, если экосистема будет приветствовать только тех, кто принимает высокие риски. Наличие надежной системы страхования является важной мерой для снижения рисков, которые пользователи принимают на себя при взаимодействии с приложениями DeFi, тем самым привлекая больше пользователей в это пространство.

Что такое страхование?

Страхование-крупная отрасль, общий объем страховых премий которой достиг \$6,3 трлн. во всем мире в 2019 году. Мир по своей природе хаотичен, и всегда существует риск несчастных случаев. Ниже приведена простая структура управления рисками, чтобы показать, что мы должны делать с различными видами рисков.



В рамках этой системы управления рисками следует исключить риски с высоким ущербом одновременно с низкой вероятностью риска, такие как стихийные бедствия и неизлечимые болезни. Страхование создано для борьбы с этими видами рисков.

Как работает страхование?

Страхование действует на основе двух основных допущений:

1. Закон больших чисел

Страховой случай, покрываемый страхованием, должен быть независимым. Если событие повторяется достаточно часто, результат будет сходиться к ожидаемому значению.

2. Объединение рисков

Страховой случай имеет такие свойства, как низкая вероятность и высокий ущерб. Таким образом, страховые взносы, уплачиваемые большой группой людей, субсидируют убытки по нескольким крупным страховым случаям.

По сути, страхование – это инструмент для объединения капитала и обобщения крупных убытков, чтобы участники не испытали финансового краха при одном катастрофическом событии.

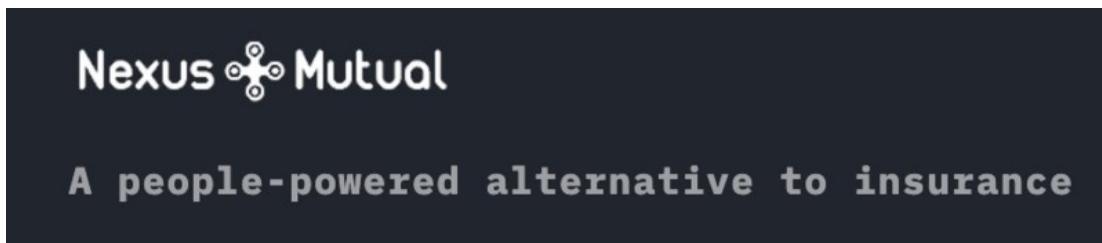
Нужно ли страхование в криптоиндустрии?

Страхование дает людям возможность идти на риск, обобщая стоимость любых катастрофических событий. Это важный инструмент управления рисками для привлечения к участию большего числа людей, выходящих за рамки текущей нишевой базы пользователей. Индустрия DeFi требует страховых продуктов, чтобы институциональные игроки, обладающие значительным капиталом для развертывания, были убеждены в том, что безопасно участвовать в DeFi.

Протоколы страхования DeFi

Ниже мы подробно рассмотрим три протокола страхования DeFi - Nexus Mutual, Armor Protocol и Cover Protocol.

Nexus Mutual



Nexus Mutual является крупнейшим протоколом страхования на крипторынке с большим отрывом. По состоянию на 1 мая 2021 года его общая стоимость (TVL) составляет 450 миллионов долларов по сравнению с 7 миллионами долларов по второму по величине протоколу страхования DeFi, Cover Protocol. Nexus Mutual была основана Хью Карпом, бывшим финансовым директором Munich Re в Великобритании.

Nexus Mutual был зарегистрирован как совместное предприятие в Великобритании. В отличие от компаний, которые следуют модели акционеров, совместное предприятие регулируется его членами, и только членам разрешается вести дела с совместным предприятием. Это похоже на компанию, которой управляют исключительно члены для своих членов.

Типы страховок

Nexus Mutual предлагает два типа страховок:

1. Страховка протоколов

Покрытие рисков протоколов DeFi, которые хранят средства пользователей, необходимы, поскольку эти смарт-контракты могут быть взломаны из-за уязвимостей в смарт-контрактах. Страхование протоколов ранее было обновлено 26 апреля 2021 года и на данный момент включает следующие страховые события:

- Ошибки в разработке экономики протокола
- Серьезные ошибки оракула
- Атаки на управление
- Защита активов на уровне 2 в Ethereum
- Защита смарт-контрактов, не связанных с Ethereum
- Защита протоколов, обеспечивающих кроссчейновые операции

Nexus Mutual предлагает покрытия для основных протоколов DeFi, таких как Uniswap, MakerDAO, Aave, Synthetix и Yearn Finance.

2. Страховка депозитарных рисков

Страховка взлома средств или остановки вывода средств. Nexus Mutual охватывают централизованные биржи, такие как Binance, Coinbase, Kraken, Gemini, и централизованные кредитные услуги, такие как BlockFi, Nexo и Celsius.

В общей сложности пользователи могут приобрести страховку для 72 различных протоколов смарт-контрактов, централизованных бирж, кредитных услуг и депозитов.

Покупка страховки

Чтобы купить страховку у Nexus Mutual, пользователям сначала нужно будет зарегистрироваться в сервисе и пройти процесс «знай своего клиента» (KYC). Существует единовременный членский взнос в размере 0,002 ETH. После одобрения пользователи могут приобрести страховку, используя ETH или DAI.

Nexus Mutual преобразует платеж в NXM, токен протокола, представляющий право на общий капитал. 90% NXM сжигается в качестве стоимости покрытия. 10% от NXM останется в кошельке пользователя. Он будет использован в качестве залога при заявке на страховой случай и будет возвращен, если претензий нет.

Оценка страхового случая

Пользователи могут подать заявку на страховой случай в любое время в течение страхового периода или в течение 35 дней после окончания страхового периода. Поскольку для каждой отправки заявки требуется, чтобы пользователи блокировали 5% премии, пользователям разрешается отправлять не более двух заявок для каждого полиса.

В отличие от традиционных страховщиков, результат заявки на страховой случай определяется голосованием участников – участники имеют полное право решать, является ли случай страховым. Участники могут использовать (стейкать) свой NXM для участия в качестве эксперта по рассмотрению претензий, на который распространяется семидневный период блокировки.

Когда голосование придет к единому мнению, 20% премии по полису будут пропорционально распределены между этими участниками. Однако, если голосование не будет согласовано между участниками, то они не получат никаких вознаграждений, а период блокировки будет продлен еще на семь дней.

Чтобы иметь право на получения страховой суммы, пользователи должны будут доказать, что они потеряли свои средства:

- Страхование протоколов – потеря не менее 20% своих средств
- Депозитарное страхование потеря не менее 10% своих средств

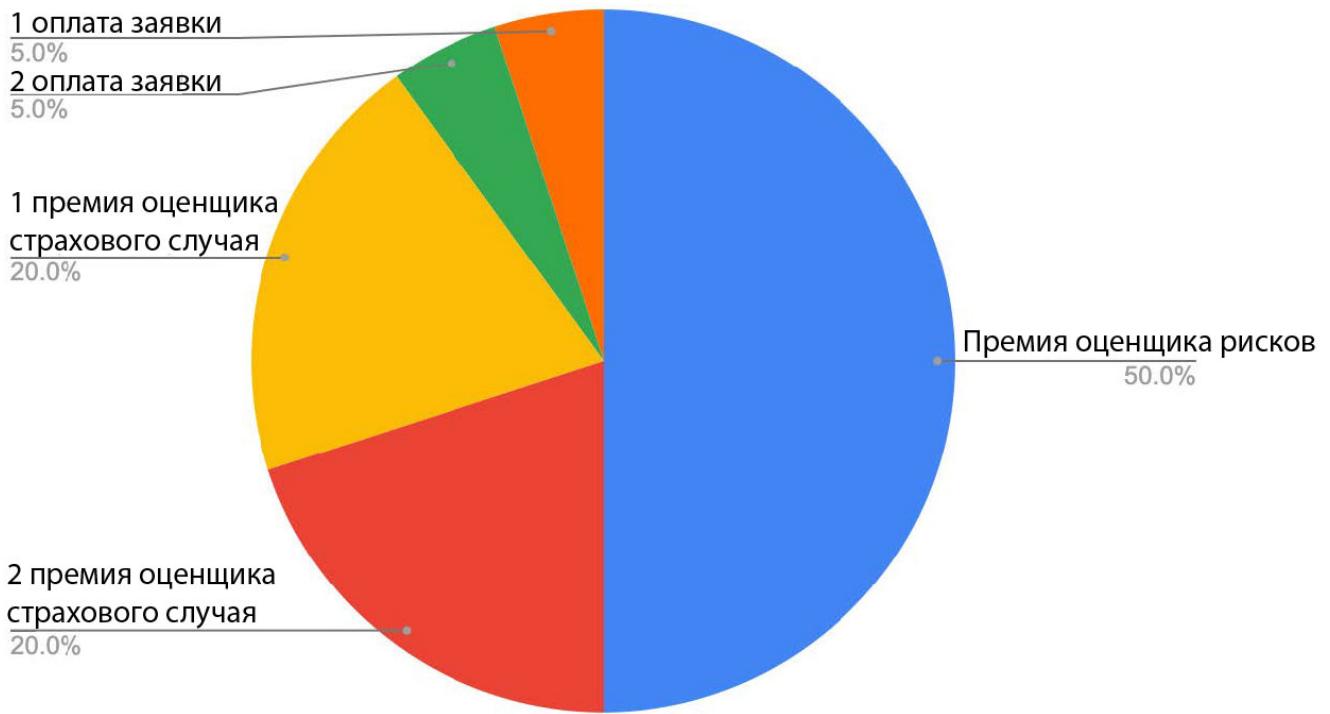
Оценка рисков

Стоимость страховки определяется суммой капитала, вложенного в конкретный протокол. Пользователи могут стейкать свои NXM в пулы протоколов, чтобы стать оценщиками рисков – чем больше NXM застейкано, тем ниже будет цена страховки.

По состоянию на апрель 2021 года для достижения минимальной базовой цены в 2% требуется 50 000 NXM. Избыточная маржа, которая установлена на уровне 30%, предназначена для покрытия затрат и создания общего профицита. Учитывая это, минимально возможная стоимость страховки составляет 2,6%.

Эксперт по оценке рисков несет убытки при страховом случае. За принятие на себя этого риска 50% премии по полису распределяется между оценщиками рисков.

Ниже приведена круговая диаграмма, показывающая, куда поступает премия:



Оплата заявки на страховой случай: сборы, уплаченные пользователем за заявку на страховой случай

Оплата оценщика страхового случая: гонорары, полученные оценщиком в случае подачи заявки на страховой случай

Если по истечении срока действия полиса не будет подано никаких заявлений, 10% премии будет возвращено оценщикам рисков, покрывающим страховку, в то время как 40% премии поступит в пул взаимного капитала.

Оценщикам рисков разрешается вкладывать доступный капитал с плечом 15x, чтобы максимизировать эффективность использования капитала. Например, если у оценщика рисков 100 NXM, он/она может застейкать 1500 NXM по нескольким протоколам, при этом максимальная ставка по любому одному протоколу составляет 100 NXM.

Здесь предполагается, что очень маловероятно, что одновременно будет взломано несколько протоколов. Эта практика согласуется с тем, как работает традиционное страхование, основанное на законе больших чисел и объединении рисков.

Если сумма требования превышает капитал, вложенный оценщиками рисков, пул взаимного капитала выплатит оставшуюся сумму.

Чтобы гарантировать, что всегда будет достаточно капитала для оплаты требований, взаимный капитал должен иметь сумму выше минимального требования к капиталу (Minimum Capital Requirement – MCR).

Обычно MCR рассчитывается на основе риска продаваемых страховок. Но из-за отсутствия данных о заявках, приходится использовать параметрами, определенным командой.

Токеномика

Токеномика (или экономика токена) NXM является важным фактором в привлечении и удержании капитала. Она использует кривую спроса для определения цены токена NXM. Формула выглядит следующим образом:

$$\text{Цена} = A + \left(\frac{MCR_{ETH}}{C} \right) \times \left(\frac{\text{Доступный капитал}}{MCR_{ETH}} \right)^4$$

где A (константа) = 0,01028

 C (константа) = 5 800 000

$\left(\frac{\text{Доступный капитал}}{MCR_{ETH}} \right)^4$ является ключевым фактором при определении цены токена NXM, поскольку в формуле цены он имеет четвертую степень. Когда люди покупают NXM через кривую спроса, доступный капитал увеличивается, что приведет к росту $\left(\frac{\text{Доступный капитал}}{MCR_{ETH}} \right)^4$, что приведет к экспоненциальному росту цены NXM.

Здесь важно отметить, что вывод токенов из кривой спроса будет остановлен, когда $\left(\frac{\text{Доступный капитал}}{MCR_{ETH}} \right)^4$ будет ниже 100%. Это делается для того, чтобы обеспечить достаточный капитал для оплаты заявок.

Wrapped NXM (wNXM)

В июле 2020 года члены сообщества Nexus Mutual выпустили wNXM, чтобы инвесторы могли получить доступ к NXM без прохождения процесса KYC. Когда вывод NXM приостановлен (когда $\left(\frac{\text{Доступный капитал}}{MCR_{ETH}}\right)^4$ опускается ниже 100%), пользователи могут завернуть свой NXM в wNXM и продать его через вторичные рынки, такие как Uniswap и Binance.

wNXM имеет много недостатков, поскольку его нельзя использовать при оценке рисков, оценке заявок и голосовании по вопросам управления. Запуск протокола Armor помогает решить вышеуказанные проблемы путем преобразования wNXM в arNXM.

Более подробную информацию можно найти ниже в разделе протокола Armor.

Доходы от протокола

Токен NXM отличается от других токенов управления тем, что цена токена определяется формулой. Таким образом, если взаимная сделка приносит прибыль, это поможет увеличить доступный капитал и повысить цену NXM.

Существует три источника прибыли:

- Собранные премии – оплаченные заявки – Траты токенов
- Спред 2,5%, когда пользователи продают NXM через кривую спроса
- Инвестиционные доходы от пула капитала

Armor Protocol



Armor Protocol делает инвестиции в DeFi максимально безопасными с помощью собственной динамической агрегации страхования. Будучи децентрализованным брокером, инновации Armor обеспечивают страхование по требованию, в режиме реального времени и с обеспечением безопасности, не связанные с блокировкой активов пользователей.

Armor Protocol состоит из четырех основных продуктов: arNXM, arNFT, arCORE и arSHIELD.

arNXM

Nexus Mutual создал wNXM, чтобы позволить инвесторам иметь доступ к NXM без выполнения KYC. Однако по мере того, как создавалось все больше wNXM, все меньше NXM становилось доступным для внутренних функций взаимного обмена, таких как размещение вкладов, оценка претензий и голосование по вопросам управления.

Armor создал arNXM, чтобы решить эту проблему, позволив инвесторам участвовать в операциях Nexus Mutual без выполнения KYC. Чтобы получить arNXM, пользователи могут вложить wNXM в Armor. Armor в свою очередь разворачивает wNXM, и NXM-токен затем стейкается на Nexus Mutual. Стейкная на Nexus Mutual, вкладчикам сигнализируют о том, что смарт-контракты безопасны, открывая больше страховых полисов для продажи.

arNXM также можно назвать хранилищем wNXM. Пользователи, которые размещают wNXM в хранилище, могут рассчитывать на получение большего количества wNXM в будущем.

arNFT

арNFT – это токенизированная форма страхования, приобретенная на Nexus Mutual. Токены arNFT позволяют пользователям покупать страховой полис без необходимости выполнять KYC. Поскольку эти страховые покрытия токенизированы, пользователи теперь могут передавать их другим пользователям или продавать на вторичном рынке. Эти токенизированные страховые полисы также обеспечивают дополнительную совместимость с другими DeFi-продуктами.

арNFT могут быть созданы для любых страховых полисов Nexus Mutual.

arCORE

арCORE – это страховой продукт с оплатой по мере использования страховки. Используя потоковую платежную систему, Armor отслеживает точное количество средств пользователей по мере их динамичного перемещения по различным протоколам и начислений каждую секунду. В основе arCORE лежат объединенные arNFT, которые разбиваются и продаются с надбавкой. arCORE обеспечивает гораздо более инновационный дизайн продукта и демонстрирует универсальную природу экосистемы DeFi.

Продукты arNFT оплачиваются с более высокой надбавкой, чтобы компенсировать стейкерам arNFT риск неполной продажи страхового полиса. По состоянию на апрель 2021 года мультипликатор составляет 161,8%, что означает, что цена будет на 61,8% выше, чем при покупке напрямую у Nexus Mutual.

В качестве дополнительного дохода, 90% возвращается стейкерам arNFT, а 10% забирает Armor в качестве административного сбора. При коэффициенте дохода 1,618 и 90%-ной доле выручки использование должно превышать 69%, чтобы это было выгодно для стейкеров arNFT. Если проданные страховые полисы составляют менее 69% от тех, которые были вложены в пул, то стейкерам придется самим покрывать расходы на страховку.

arSHIELD

арSHIELD – это застрахованное хранилище токенов провайдеров ликвидности (LP), в котором страховые взносы автоматически вычитываются из заработанных сборов за предоставление ликвидности. arSHIELD, по сути, создает застрахованные токены LP, в которых пользователям не нужно платить авансовые платежи.

арSHIELD покрывает только протокольный риск пулов ликвидности. Например, застрахованные токены Uniswap LP покрывают только риски компрометации смарт-контракта Uniswap, но не риски взлома базовых активов (например, взлома протокола базовых активов).

Таким образом, arSHIELD – это просто переупакованная версия arCORE.

Заявки на страховой случай

После того, как пользователь подаст заявку, будет запущен процесс рассмотрения и отправлен на решение в Nexus Mutual. Держатели токенов Armor также будут участвовать в процессе Nexus Mutual для утверждения заявок и выплат. Если выплата будет подтверждена, сумма будет отправлена в казначейство выплат Armor, прежде чем будет распределена среди застрахованных.

Доходы от протокола

Armor сосредоточен на создании экосистемы совместимых протоколов и продуктов для обеспечения и масштабирования массового внедрения DeFi как институционалами, так и частниками.

Ниже приведена таблица получения процентов от прибыли, обновленная по состоянию на февраль 2021 года:

Продукт	Доля прибыли вкладчиков	Доля прибыли протокола
arNXM	90%	10%
arCore	90%	10%
arNFT	0%	100%

Следует отметить, что 10% премии за каждую страховку, купленную у Nexus Mutual, зарезервировано для целей возникновения заявок. Поскольку плата за претензию составляет 5% от премии, каждый пользователь может подать заявку дважды с один и тот же полис. Если в конце периода действия полиса не будет никаких заявок, будет возвращена премия в размере 10%. Это и есть источник прибыли arNFT.

Cover Protocol



Cover Protocol был инкубирован Yearn Finance, сперва называвшийся Safe Protocol, который предлагает страхование yInsure. Но из-за некоторой ссоры между основателем Аланом и видным членом сообщества Азимом Ахмедом проект был отменен. Азим взял на себя ответственность за продукт и выпустил Armor Protocol, в то время как Алан продолжил проект под названием Cover Protocol.

Компания Yearn Finance объявила о партнерстве с Cover Protocol, чтобы застраховать все свои хранилища с помощью него. Однако Yearn Finance прекратила партнерство 5 марта 2021 года.

Типы страховок

Cover Protocol предлагает только страхование смарт-контрактов.

Давайте рассмотрим пример того, как продаются страховки. Маркетмейкеры могут внести депозит 1 DAI, и они смогут отчеканить один токен NOCLAIM и один токен CLAIM. Оба токена представляют собой только риск одного протокола. Токены действительны только в течение фиксированного срока, например, полугода.

Два сценария могут произойти через полгода:

- Если нет заявок на выплату страховки, держатели токенов NOCLAIM могут забрать 1 DAI, в то время как токены CLAIM не получат ничего.
- Если есть заявка на выплату страховки, владельцы токенов CLAIM могут забрать 1 DAI, в то время как токены NOCLAIM не получат ничего.

Это похоже на рынок прогнозов, где пользователи могут делать ставки на то, будут ли взломаны протоколы в течение определенного периода времени.

Cover Protocol ввел частичные заявки, поэтому выплата держателям токенов CLAIM при наличии действительного события претензии будет определяться комитетом по обоснованности претензий (Claim Validity Committee – CVC).

Покупка страховки

Пользователи могут купить страховку с веб-страницы Cover Protocol всего за одну транзакцию Ethereum, без необходимости регистрации или процесса KYC.

Оценка страхового случая

У пользователей есть два варианта подачи заявки на страховой случай:

1. Обычная заявка: Обычная заявка стоит 10 DAI. Держатели токенов COVER сначала проголосуют за обоснованность претензии. После подтверждения заявка перейдет в комитет CVC для принятия окончательного решения.
2. Усиленная заявка: Требование о применении такого типа заявки стоит 500 DAI. Заявка направляется непосредственно в CVC для принятия решения.

CVC состоит из внешних аудиторов смарт-контрактов. Cover Protocol возместит стоимость подачи заявки, если претензия будет одобрена.

Оценка рисков

Когда пользователи покупают страховку, используются флэш-займы для снижения стоимости газа и количества транзакций, необходимых пользователю. В этом процессе токены с CLAIM и NOCLAIM создаются с помощью заимствования DAI. Токены NOCLAIM затем продаются в пул Balancer за DAI.

В сочетании с уплаченной пользователем премией, DAI затем используются для погашения флэш-займа, и пользователи получат только токены CLAIM. Обратное произойдет, когда пользователи продадут токен CLAIM обратно в Cover Protocol.

У этой системы есть несколько преимуществ.

Ожидается, что стоимость страхования снизится, поскольку существует только один пул Balancer для фарминга. При наличии правильных стимулов маркетмейкеры будут покупать больше токенов NOCLAIM, чтобы получать прибыль от фарминга или комиссионные за торговлю, повышая цену токенов NOCLAIM. Таким образом, цена токена CLAIM снизится, так как $CLAIM = 1 - NOCLAIM$.

Ожидается, что маркетмейкер будет получать больше комиссионных, поскольку каждая покупка покрытия включала продажу токенов NOCLAIM в пул Balancer. В отличие от предыдущей системы, маркетмейкерам необходимо предоставлять ликвидность только для одного пула, а не для двух.

Ожидается, что Cover Protocol получит более высокий доход платформы, поскольку каждая покупка включает в себя создание токенов CLAIM/NOCLAIM с комиссией 0,1% во время погашения.

Цена страхования определяется спросом и предложением пула Balancer.

Доходы протокола

Комиссия в размере 0,1% будет взиматься при предъявлении CLAIM и NOCLAIM для погашения. Держатели токенов COVER имеют право голосовать за то, как использовать фонд протокола. По состоянию на апрель 2021 года обсуждается размещение токенов COVER для получения дивидендов, но детали еще не завершены.

Сравнение Nexus Mutual и Cover Protocol

Параметры	Nexus Mutual	Cover Protocol
Модель токенов	Совместное владение	Акционеры
Тип продукта	Страхование	Рынок прогнозов
Объединение рисков	Да	Нет
Эффективность использования капитала	Высокая	Низкая
Количество смарт-контрактов взаимодействующих с протоколом	72	33
Заявки	Голосования членов владения	Голосование аудиторов
KYC	Не требуется (Armor)	Не требуется
Доказательство потери	Требуется	Не требуется
Страховое покрытие	Полное	Частичное
TVL	450 млн. долларов	7 млн. долларов

По состоянию на апрель 2021 года Nexus Mutual занимает лидирующие позиции на страховом рынке, и, по-видимому, конкурентов не предвидится. Но у конкурентов есть много возможностей наверстать упущенное, поскольку уровень проникновения страхования в DeFi очень низок и составляет примерно 2% от общего объема TVL DeFi. В области, где инновации появляются каждый день, звание лидера в области страхования можно завоевать всегда.

Cover Protocol быстро внедряет инновации, даже несмотря на фиаско с Safe Protocol. Несмотря на то, что продукт еще не получил значительного распространения, инновации «от нуля к единице» никогда не бывают простыми. Мы должны помнить, что Cover Protocol действует менее года (по состоянию на апрель 2021 года).

Эффективность использования капитала

Nexus Mutual позволяет провайдерам капитала иметь 15-кратное кредитное плечо на капитал, который они размещают. Это приводит к более высокому доходу для вкладчиков. Провайдеры капитала действительно должны брать на себя больше рисков, но этот подход согласуется с тем, как традиционные страховые компании распределяют риски по нескольким различным продуктам с различными профилями рисков.

В то же время провайдеры капитала для Cover Protocol не могли использовать свой капитал с плечом, поскольку каждый пул изолирован. В результате страховки Cover Protocol стоят дороже, чем у Nexus Mutual из-за меньшей эффективности использования капитала. Например, покупка страховки для Origin Dollar обойдется в 12,91% годовых в Cover Protocol, в то время как на Nexus Mutual это обойдется всего в 2,6%. В версии 2 Cover Protocol планируется объединить различные риски вместе, но деталей пока не раскрывают.

Мы можем количественно рассчитать эффективность использования капитала, разделив сумму активного страхования на пул капитала. Nexus Mutual имеет коэффициент эффективности использования капитала до 200%, в то время как протокол покрытия, по замыслу, всегда будет меньше 100%.

Доступные страховки

Cover Protocol охватывает только 33 протокола, в то время как Nexus Mutual охватывает 72. Nexus Mutual предлагает большую гибкость в условиях страхования, когда пользователи могут решить купить страховку в любой день и иметь период страхования до одного года.

Cover Protocol предлагает только срочное страхование, то есть дата окончания должна быть определена заранее. Например, для определенной страховки срок страхования действует до конца мая. Независимо от того, когда пользователь купит эту страховку, она закончится в мае. Таким образом, со временем токен CLAIM будет сходить к 0 долларам, в то время как токен NOCLAIM будет сходить к 1 доллару.

Пользователи могут найти более разнообразные предложения от Nexus Mutual, поскольку он охватывает большинство основных протоколов DeFi. Но даже с учетом этого многие страховки распроданы из-за нехватки стейкеров. Запуск протокола Armor помог решить эту проблему, привлекая больше wNXM в arNXM, что позволяет стейкать больше NXM. В результате появляется больше страховок.

Cover Protocol можно рассматривать как конкурирующий продукт на токенах с малой ликвидностью, поскольку проекты могут быть добавлены на платформу намного быстрее и им не нужно проходить громоздкие оценки рисков со стороны протокола страхования. Это связано с тем, что каждый риск изолирован и содержится в одном пуле, в отличие от NXM, где претензия из любого отдельного протокола может попасть в пул капитала. Однако охват начальной загрузки для менее известных проектов – непростая задача. Помимо того, что они ограничены объемами, стоимость страхования часто бывает слишком высокой.

Процент выплат по страховым полисам

Компания Yearn Finance пострадала от взлома на 11 миллионов долларов в феврале 2021 года. Несмотря на то, что компания Yearn Finance решила покрыть убытки через свой фонд, страховые протоколы решили выплатить страховки, чтобы продемонстрировать, что их продукт работает так, как задумано.

Nexus Mutual приняла 14 заявок на сумму выплаты по претензиям в размере 2 410 499 долларов США (1 351 ETH и 129 660 DAI). Это привело к потере 9,57% для владельцев NXM, которые сделали стейкинг в пул по Yearn Finance. Убытки были полностью оплачены, если заявители могли доказать, что они действительно потеряли по крайней мере 20% своего фонда.

Между тем, Cover Protocol решил установить процент выплат только в размере 36% из-за того, что потеря затронула только 36% хранилища. Если у пользователей было 1000 токенов CLAIM, они получали только 360 долларов. Поскольку токены CLAIM на сумму 409 000 долларов были доступны для Yearn Finance, маркетмейкеры потеряли только 147 240 долларов.

Покупатели страховки должны понимать, что покупка страховки у Cover Protocol не гарантирует полную выплату в случае убытка. Способ определения страховых выплат больше похож на рынок прогнозов.

Сопутствующие риски

Страховые выплаты в значительной степени зависят от соглашений, заключенных между страховыми компаниями и покупателями. В толковании соглашений всегда есть нюансы, особенно в сценариях с высокими ставками, которые связаны с крупными выплатами.

Каждый протокол страхования принимает собственные решения о том, какие выплаты делать, что не обязательно может быть справедливым по отношению ко всем покупателям. Покупатели должны знать о текущих ограничениях, предлагаемых страховыми продуктами.

Быть провайдером капитала для страховых протоколов – сложная задача, и пользователи должны иметь полное представление о рисках, прежде чем принимать решение об участии в этом. Вкладчики могут понести убытки, если вероятность страховых выплат выше, чем ожидалось.

Страховые продукты, заслуживающие упоминания



Unslashed Finance

По состоянию на апрель 2021 года Unslashed Finance находится в режиме закрытого бета-тестирования. Unslashed Finance предлагает объединение рисков для провайдеров капитала. Первый продукт, названный Spartan Bucket, охватывает 24 различных контрагентов, таких как депозиты, кошельки, биржи, смарт-контракты, валидаторы и оракулы.

Lido Finance приобрела страховку на сумму 200 миллионов долларов у Unslashed Finance для своего токена stETH (стейкинг-сервис ETH 2.0), чтобы покрыть риск штрафных санкций. Риск относится к штрафам, применяемым к валидатору сети Proof of Stake (PoS), когда валидаторы не поддерживают сеть постоянно.



Nsure Network

Nsure Network привлекла начальный фонд в размере 1,4 миллиона долларов от Mechanism Capital, Caballeros Capital, 3Commas, AU21, Signal Ventures и Genblock еще в сентябре 2020 года.

Nsure Network является рынком для торговли рисками. Он основывает на стейкинге токенов NSURE, чтобы сигнализировать о степени рискованности протокола, и использует его для оценки страховки. По состоянию на апрель 2021 запускается программа страхования в тестовой сети Kovan Ethereum, чтобы понять, как будет работать оценка страхования в основном блокчейне. Участники получат токены NSURE в качестве вознаграждения.



InsurAce

InsurAce привлекло 3 миллиона долларов США от венчурных инвесторов, таких как Alameda Research, DeFiance Capital, Profit Capital, Maple Leaf Capital, Ван Цяо и Керман Коли. Он стремится стать первым протоколом страхования на основе портфеля, предлагающим как инвестиционные, так и страховые продукты для повышения эффективности капитала.

С InsurAce пользователям не нужно покупать несколько страховок, если они сталкиваются с различными протоколами фарминга, поскольку он предлагает страхование на основе портфеля активов, охватывающее все протоколы, участвующие в указанной инвестиционной стратегии. Также утверждается, что используется модель ценообразования, основанная на актуарных расчетах, вместо того, чтобы полагаться на вложения или рынок для определения цены покрытия.

По состоянию на апрель 2021 года InsurAce еще не объявило дату своего запуска. Из-за отсутствия истории страховых случаев еще предстоит выяснить, будут ли работать протокол страхования и модель ценообразования на основе страхового портфеля в пространстве DeFi.

Некоторые протоколы деривативов также предлагают интересные страховые продукты, такие как:



Hakka Finance's 3F Mutual – страхование риска отклонений от привязки DAI.



Opium Finance – страхование риска отклонений от привязки USDT.

Внедрение этих страховых продуктов, предлагаемых протоколами деривативов, до сих пор было небольшим.

В отличие от других децентрализованных бирж и протоколов кредитования/займствования, протоколам страхования, похоже, уделяется меньше внимания. Помимо того, что это более капиталоемкая операция, осведомленность о возможностях страхования не так распространена в криптоиндустрии. Мы можем увидеть, как все больше пользователей подключаются к страхованию, а новые протоколы страхования планируются к запуску в 2021 году и позже.

Вывод

Рынок страхования все еще недостаточно изучен. Согласно активной сумме страхования Nexus Mutual, страхуется только около 2% от общей заблокированной стоимости DeFi. Производные финансовые инструменты, такие как кредитный дефолтный своп и опционы, могут уменьшить необходимость покупки страховки.

Однако создание этих продуктов, как правило, является более капиталоемким, чем метод страхования с объединением рисков, что приводит к более дорогим страховкам. Кроме того, производные финансовые инструменты по определению являются более дорогостоящими, поскольку они подвержены ценовому риску.

Существует также вероятность того, что на текущем рынке DeFi доминируют лица, принимающие высокие риски, и пользователи с небольшим капиталом. Они могут не уделять особого внимания управлению рисками и, следовательно, не учитывать необходимость страхования. Рынок страхования наберет больше оборотов, когда криptoиндустрия созреет и будет больше вовлечено институционального капитала.

Основной бизнес Nexus Mutual процветает, при этом активная сумма покрытия увеличилась в десять раз с 68 миллионов долларов в январе 2021 года до 730 миллионов долларов в феврале 2021 года.

Запуск Armor Protocol стал огромным благом для Nexus Mutual, укрепив его лидерство на рынке страхования DeFi, так как токен arNXM и хранилище токенов wNXM предназначены для замены wNXM. Он привлек так много wNXM, что arNXM теперь составляет 47% от общего количества размещенных NXM. Это помогло предложить больше страховых продуктов. Между тем, на долю arNXM приходится примерно 70% от общего активного страхования.

Cover Protocol быстро внедряет инновации с помощью новых продуктов, таких как кредитный дефолтный своп, но рост их бизнеса довольно медленный. Cover Protocol предлагает меньше продуктов и обладает меньшей гибкостью в условиях страхования. Но это позволяет проектам внедряться быстрее и может обеспечить страхование с относительно меньшим капиталом.

Рекомендуемая литература

1. Почему страхование в DeFi нуждается в арбитраже, связанным с Ethereum
<https://blog.kleros.io/why-defi-insurance-needs-an-ethereum-native-claims-arbitrator/>
2. Зачем нужна страховка в DeFi и на что это похоже
<https://cryptoslate.com/why-insurance-is-needed-for-defi-and-what-it-looks-like/>
3. Nexus Mutual является самым недооцененным токеном в цифровых активах
<https://twitter.com/jdorman81/status/1376920737949184002?s=20>

ЧАСТЬ ТРЕТЬЯ: РАЗВИВАЮЩИЕСЯ КАТЕГОРИИ DEFI

ГЛАВА 9: ДЕЦЕНТРАЛИЗОВАННЫЕ ИНДЕКСЫ

Один из способов получить доступ к криптовалюте в вашем инвестиционном портфеле без постоянного мониторинга курса отдельных валют – это инвестировать в пассивно управляемые портфели, такие как децентрализованные индексы. Децентрализованные индексы работают аналогично биржевым фондам (ETF) на существующих финансовых рынках.

ETF – это тип структурированной ценной бумаги, которая может отслеживать что угодно, например, индекс S&P 500, товары (в частности, драгоценные металлы) или другие активы. Его можно купить или продать на фондовой бирже.

Исторически сложилось так, что ETF имеют лучшую доходность, чем активно управляемые стратегии, такие как ПИФы. В 2020 году глобальные ETF имели под управлением активы на сумму 7,74 трлн долларов (AUM), объем которых достиг одной трети мирового объема торговли акциями.

По состоянию на 1 апреля 2021 года сектор децентрализованных индексов быстро растет, при этом объем ETF в цепочке составляет примерно 234 миллиона долларов в AUM. Логично предположить, что эта цифра достигнет триллионов долларов в ближайшие годы.

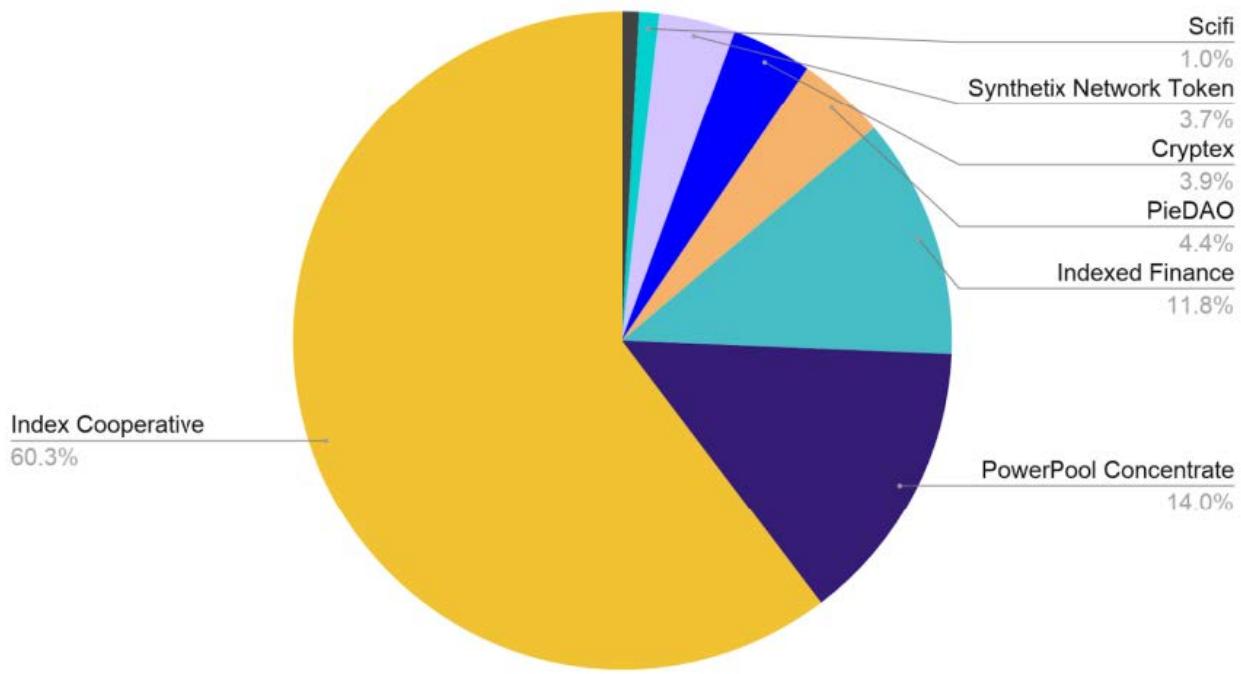
В этой главе мы сосредоточимся на децентрализованных индексах, где вы можете диверсифицировать свои портфели, не тратя слишком много времени и усилий на исследования, управление и распределение ваших инвестиций.

Протоколы индексов относятся к управляющим активами, в то время как токены индексов относятся к продуктам индексов (эквивалентным ETF). Эти индексные токены представляют вашу долю в индексном фонде и дают вам право получать прибыль от прироста капитала базовых активов. Кроме того, для некоторых протоколов существуют токены управления, дающие вам право голоса для определения направления протоколов индексов.

Во-первых, рассмотрим распределение рынка децентрализованных индексов:

Распределение ETF DeFi

\$234M Total AUM as of 1st April 2021



По состоянию на 1 апреля 2021 года, Index Cooperation имеет самую большую долю рынка с 60% децентрализованных индексов AUM. За ним следуют PowerPool (14%) и Indexed Finance (12%).

Несмотря на наличие на рынке более 20 токенов индекса DeFi, рынок децентрализованных индексов не так переполнен и конкурентоспособен, как кажется. Децентрализованные индексы AUM составляют всего 0,3% от общей заблокированной стоимости DeFi.

Давайте взглянем на 3 крупнейших протокола по индексам – Index Cooperative, PowerPool Concentrated Voting Power и Indexed Finance.

Index Cooperative (INDEX)



Index Cooperative, также известный как Index Coop, является старейшим децентрализованным протоколом индексов. Он был основан Set Labs Inc., той же компанией, которая создала Set Protocol.

Index Coop позволяет пользователям получить широкий доступ к множеству протоколов различной тематики в индустрии криптовалют. Держатели индексных токенов (не путать с держателями токенов Index) могут владеть базовыми активами, составляющими индекс, иметь доступ к ним и могут напрямую получать активы из индекса в обмен на индексные токены.

Index Coop работает с различными методологами – поставщиками данных, которые отвечают за стратегию конкретных индексов для запуска своих продуктов.

По состоянию на апрель 2021 года в разделе Index Coop доступно пять индексов:

- DeFiPulse Index (DPI)
- CoinShares Crypto Gold Index (CGI)
- ETH 2x Flexible Leverage Index (ETH2X-FLI)
- BTC 2x Flexible Leverage Index (BTC2X-FLI)
- Metaverse Index Token (MVI)

Indexed Finance (NDX)

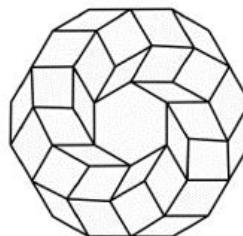


Indexed Finance – это протокол, который фокусируется на управлении портфелем. Пользователи могут создавать, обменивать или сжигать токен индексов и базовые активы, а интегрированный автоматизированный механизм маркетмейкера (AMM), форк Balancer'a, автоматически балансирует свои индексы. В Indexed Finance работают пять членов команды, один из которых является анонимным.

По состоянию на апрель 2021 года в Indexed Finance доступно семь индексов:

- Degen Index (DEGEN)
- Cryptocurrency Top 10 Tokens Index (CC10)
- Oracle Top 5 Index (ORCL5)
- DEFI Top 5 Tokens Index (DEFI5)
- NFT Platform Index (NFTP)
- 484 Fund (ERROR)
- Future Of Finance Fund (FFF)

PowerPool Concentrated Voting Power (CVP)



PowerPool

Индексы PowerPool – это интеллектуальные пулы, основанные на автоматизированном маркетмейкере (AMM) Balancer с дополнительной функциональностью. Его основная цель – объединить токены управления для кредитования, заимствования и выполнения мета-управления. Кроме того, пользователи могут напрямую менять один токен управления на другой. Анонимная команда управляет PowerPool.

В настоящее время PowerPool имеет четыре индекса:

- Power Index Pool Token (PIPT)
- Yearn Ecosystem Token Index (YETI)
- ASSY Index (ASSY)
- Yearn Lazy Ape (YLA)

Сравнение протоколов индексов

Вам, как инвестору, необходимо обратить внимание на три основных показателя:

1. Комиссии протокола
2. Стратегии протокола
3. Вес фонда

Комиссии протокола

Index Projects	Index Cooperative (INDEX)			Indexed Finance (NDX)					PowerPool Concentrated Voting Power (CVP)				
Index Funds	DPI	CGI	FLI	DEFI5	CC10	DEGEN	ORCL5	NFTP	FFF	PIPT	ASSY	YETI	YLA
Entry fee (mint)	-	-	0.10%	-	-		-	-	-	0.10%	0.10%	0.10%	0.10%
Swap fee*	-	-	-	2.00%	2.00%	2.00%	2.00%	2.00%	2.00%	0.20%	0.20%	0.20%	0.20%
Asset Manager Treasury	-	-	-	-	-	-	-	-	-	0.10%	0.10%	0.10%	0.10%
LP return	-	-	-	2.00%	2.00%	2.00%	2.00%	2.00%	2.00%	0.10%	0.10%	0.10%	0.10%
Management Fee**	0.95%	0.60%	1.95%	-	-	-	-	-	-	-	-	-	-
Asset Manager Treasury	0.65%	0.24%	1.17%	-	-	-	-	-	-	-	-	-	-
Methodologist	0.30%	0.36%	0.78%	-	-	-	-	-	-	-	-	-	-
Exit fees (Burn/Redeem)	-	-	0.10%	0.50%	0.50%	0.50%	0.50%	0.50%	0.50%	0.10%	0.10%	0.10%	0.10%

Source: CoinGecko, Index Cooperation, Indexed Finance, Powerpool, Tokensests. Taken as at 1st April 2021

* When the user swap one of the underlying assets from one to another.

** Annualized

Index Cooperative

Плата за управление каждым индексом распределяется между Index Cooperative и соответствующим методологом. Сборы следующие – DPI: 0,95%, CGI: 0,60%, FLI: 1,95%. Плата за выход для DPI и CGI не взимается. Только у FLI плата за выход составляет 0,1%.

Indexed Finance

Для покрытия непостоянных убытков взимается комиссия за обмен в размере 2% и распределяется между держателями LP в виде входного токена при любом обмене, когда вы создаете или сжигаете токен индекса. Эта комиссия в размере 2% не взимается, если при создании токена индекса вы используете все базовые активы, аналогично реализовано для возврата всех базовых активов.

Тем не менее, с вас будет взиматься фиксированная комиссия в размере 0,5% при сжигании любого токена индекса, которая распространяется обратно пользователям протокола, которые стейкуют собственный токен управления NDX.

PowerPool Concentrated Voting Power

Существует три вида комиссий: за вход, за обмен и за выход. Если бы вы создавали токен индекса, с вас бы взяли 0,1% в качестве вступительного взноса. Плата за обмен 0,2% применяется к пользователям, которые меняют один токен управления на другой. Затем комиссия за обмен равномерно распределяется между провайдерами ликвидности индексного фонда и казначейством. При выходе из индексов взимается дополнительная комиссия в размере 0,1%.

Из приведенного выше сравнения комиссий следует, что Index Coop будет получать наибольший доход, поскольку взимает самые высокие сборы. Indexed Finance имеет только один источник выручки – плата за выход в размере 0,5%. Тем временем PowerPool имеет более диверсифицированный доход от создания индексных токенов, обмена и сборов за выход.

Как инвестор фонда, вы, скорее всего, являетесь долгосрочным держателем, поэтому комиссии имеют значение.

В этом случае индексный токен PIPT был бы самым дешевым вариантом по сравнению с DPI и DEFY 5. С PIPT и DEFY 5 нет дальнейших затрат, в отличие от DPI под 0,95% годовых.

Стратегии протоколов

Важно понимать стратегии каждого протокола, чтобы осмыслить их видение и направление в отношении продуктов децентрализованных индексов.

Index Cooperative

Ниже приведем краткое описание того, как команда внедрила продукт в свой протокол:

1. Новые идеи продукта предлагаются и обсуждаются с их членами сообщества
2. Заявка на продукт подается сообществу на форуме по управлению
3. Для продвижения продукта проводится первое голосование с предложениями
4. Принятые предложения рассматриваются командой Index Coop.
5. Второе голосование проводится при выпуске продукта
6. Запуск продукта

Index Coop имеет строгий процесс и нуждается в двух этапах голосования сообщества для утверждения продукта. Например, с момента первого голосования потребовалось примерно три месяца, чтобы запустить Flexible Leveraged Index (FLI).

Indexed Finance

По сравнению с Index Coop в Indexed Finance процесс движется быстрее.

Например, ORCL5, первому индексному фонду, который был выставлен на голосование, потребовалось в общей сложности 18 дней для запуска, начиная со стадии голосования.

Powerpool Concentrated Voting Power

Последним индексным продуктом от PowerPool был Yearn Lazy Ape, который был выставлен на голосование 17 января 2021 года и был запущен только 3 марта 2021 г.

В настоящее время Index Coop и PowerPool имеют в активе четыре индексных продукта. Indexed Finance имеют семь индексов.

Хотя Indexed Finance, по-видимому, является самым быстрым при запуске индексов, команды Index Coop и PowerPool работают со своим методологом, чтобы гарантировать безопасность своих продуктов и учитывать все связанные с этим факторы и риски.

Indexed Finance могут начать двигаться медленнее с запуском их программы Sigma. Программа Sigma позволяет Indexed Finance сотрудничать с внешними партнерами, что потребует более длительного времени на принятия решений. Например, индексный фонд Degen в сотрудничестве с Redphonecrypto был анонсирован в конце декабря 2020 года и заработал только три месяца спустя.

Вес фондов

Metrics	Index Cooperative (INDEX)				Index Finance (NDX)			PowerPool Concentrated Voting Power (CVP)			
	DPI	CGI	DEFI5	CC10	ORCL5	DEGEN	PIPT	ASSY	YETI	YLA	
Fund Weighting	Market Cap-Weighted	A bi-level approach, accounting historical volatility	Sqrt of Market Cap-weighted	Equal-weighted Market Cap	Market Cap-weighted	Market Cap-Weighted	Adaptive weights proportional to vaults TVL				

В целом, существует три основных подхода к оценке токенов в децентрализованных индексных токенах:

I. Взвешенная рыночная капитализация (например, DPI)

Этот метод динамически отслеживает рыночную капитализацию каждого актива, где распределение каждого актива пропорционально их рыночной капитализации по отношению к другим активам в индексе. Индексы, использующие этот метод, будут сосредоточены на монетах с большей рыночной капитализацией по сравнению с монетами меньшего размера, что позволит индексу точно имитировать фактические показатели рынка.

II. Корень квадратный взвешенной рыночной капитализации (DEFI5)

Все индексы Indexed Finance основаны на квадратном корне взвешенной рыночной капитализации по отношению к каждому базовому активу. Такой подход снижает влияние рынка и уменьшает изменение индекса в сторону монет с большой капитализацией.

III. Равновзвешенная рыночная капитализация (например, PIPT)

Этот метод выполняет присутствие активов в равных долях. Например, в PIPT есть восемь базовых активов. Следовательно, каждый из активов имеет долю 12,5%. Равновзвешенная стратегия определяется динамикой цен и благоприятствует

монетам с меньшей рыночной капитализацией. Монетам с меньшей рыночной капитализацией придается такое же значение, как и монетам с большой рыночной капитализацией.



Сопутствующие риски

Существует три больших угрозы, когда дело доходит до инвестирования в эти протоколы и фонды индексов DeFi:

I. Код – это закон

Хотя все протоколы топ-3 индексов были проверены, инвесторы должны иметь в виду, что проверенные протоколы не являются защищенными от взлома. Несмотря на аудит, в криптопространстве произошло множество взломов, и чаще всего средства невозможно вернуть.

II. Наемный капитал

Большинство протоколов индексов содержат программы майнинга ликвидности для стимулирования провайдеров ликвидности и начальной загрузки ликвидности для токенов индекса. Однако большая часть этих капиталов обычно известна как «наемный капитал». Эти капиталы просто ищут высокую доходность и выйдут, как только появится другой протокол с более высокой доходностью. Следовательно, как только вознаграждения за добычу ликвидности иссякнут, это может привести к массовым выводам средств, что приведет к нисходящей спирали для протокола индексов.

III. Системный риск

В DeFi протоколы могут быть вложены друг в друга, как денежный конструктор lego. Однако универсальность может быть обоюдоострым мечом, поскольку она представляет системный риск. Например, Yearn Lazy APE (YLA) от PowerPool имеет десять различных источников рисков с пятью базовыми хранилищами стейблкоинов Yearn.

1. yvCurve-Compound (8.6%)	4. yUSD (27%)
2. yvCurve-3pool (36%)	5. yvCurve-BUSD (11.1%)
3. yCurve-GUSD (17.3%)	

Эти активы взаимодействуют с десятью различными протоколами и, следовательно, имеют десять различных источников рисков. Десять протоколов, задействованных в хранилище стейблкоинов Yearn:

1. Yearn	6. Circle (USDC)
2. Curve	7. Gemini (GUSD)
3. Compound (cDai и cUSD)	8. Binance (BUSD)
4. Maker (DAI)	9. TrustToken (TUSD)
5. Tether (USDT)	10. PowerPool (YLA)

Децентрализованные индексы, заслуживающие упоминания

BasketDAO – Interest Bearing DPI (BDPI)

Продукт BasketDAO, BDPI – это зарабатывающая дополнительный доход версия DPI. Разница в том, что базовые активы кладутся в кредитные протоколы, такие как Aave и Compound, для получения прибыли. В результате ожидается, что доходность от владения этим индексным фондом будет выше, чем DPI.

Cryptex Finance – Total Crypto Market Cap (TCAP)

Созданный Cryptex Finance, TCAP позволяет вам иметь доступ ко всему крипторынку. Команда также управляет Prysmatic Labs, одной из исследовательских групп ETH 2.0.

Вывод

Мы все еще находимся на очень раннем этапе развития сектора децентрализованных индексов, который, как мы ожидаем, будет бурно расти в ближайшие месяцы и годы. В качестве долгосрочного инвестора мы настоятельно рекомендуем вам изучить прошлые показатели фонда, проверить каждую взимаемую комиссию и рассмотреть используемую стратегию фонда. Также рекомендуется выбирать фонды, исходя из вашей склонности к риску, с учетом категории активов, в которой вы хотите иметь доступ.

Рекомендуемая литература

1. Пояснения по индексам DeFi

<https://newsletter.banklesshq.com/p/the-best-defi-indices-for-your-crypto>

2. Как купить индексы с помощью Argent

<https://www.argent.xyz/learn/how-to-buy-defi/>

3. Панель мониторинга индексов DeFi

<https://duneanalytics.com/0xBoxer/indices-products>

ГЛАВА 10: ДЕЦЕНТРАЛИЗОВАННЫЕ РЫНКИ ПРОГНОЗИРОВАНИЯ

Рынки прогнозирования – это рынки, созданные для того, чтобы участники делали ставки на результаты будущих событий. Отличным примером традиционных рынков прогнозирования являются платформы для ставок на спорт.

Децентрализованные рынки прогнозирования используют технологию блокчейн для создания рынков прогнозирования о чем угодно. Например, рынки прогнозов могут задаваться вопросом, когда цена биткоина превысит 100 000 долларов или кем будет следующий президент США.

Сторонники децентрализованных рынков прогнозирования считают, что централизованные платформы ставят пользователей в невыгодное положение. Стандартная практика включает высокие комиссии за транзакции, задержку вывода средств и замораживание счетов. Более того, большинство современных традиционных букмекерских платформ ориентированы на ставки на спорт, что ограничивает типы рынков прогнозов (и зачастую есть законодательные ограничения возможностью ставок только на спорт), доступных широкой публике.

Децентрализованные рыночные протоколы прогнозирования были разработаны для расширения возможностей пользователей, позволяя им создавать свои собственные.

Как работают протоколы прогнозирования?

В отличие от обычных рынков прогнозирования, протоколы прогнозирования децентрализованы и должны опираться на инновационные методы для своего функционирования. Мы можем примерно разбить выполнение процесса протокола прогнозирования на два основных раздела:

1. Маркетмейкинг
2. Разрешение

Маркетмейкинг

В маркетмейкинге в протоколах прогнозирования существует два типа долей (токенов результатов): ДА (лонг) и НЕТ (шорт). Выплата определяется в зависимости от того, произошло ли событие.

На рынке простых прогнозов одна доля Да (которая часто обозначается как 1 доллар) выплачивает 1 доллар, если происходит рассматриваемое событие, и 0 долларов, если событие не происходит. Каждая доля «Нет» выплачивает 1 доллар, если событие не происходит, и 0 долларов, если оно происходит. Рынки такого типа используют этот основной принцип, например, предлагая ставки на событие: «Превысит ли BTC 100 000 долларов к 31 декабря 2021 года?».

Другой пример вопроса: «Кто будет президентом США в 2025 году? В этом случае может быть более двух вариантов, таких как:

- A. Джо Байден
- B. Камала Харрис
- C. Дональд Трамп

Такой пример похож на стандартный протокол прогнозирования, только с тремя долями и, соответственно, с тремя вероятностями исхода. Цена доли зависит от того, сколько покупатели готовы заплатить и сколько продавцы готовы принять. Другими словами, система является автономным букмекером, ставки которого (т.е. цена) определяются взвешиванием вероятностей на рынке.

С другой стороны, рынки с большим количеством долей и связанных с ними вознаграждений будут работать по-другому. Известные как скалярные рынки, результаты варьируются в пределах определенных параметров.

Понятный способ представить себе скалярные рынки – это думать о них как о результатах, направленных на определение того, кто наиболее прав/неправ, в отличие от того, кто окончательно прав/неправ.

Давайте приведем здесь пример со следующими предположениями:

«Какова будет цена биткоина 10 ноября 2021 года?»

Точность = 10 тысяч долларов

Диапазон = \$0 – \$200 тыс.

С таким условием пользователь может выбрать \$10 тыс., \$20 тыс., \$30 тыс. и так далее.

В отличие от рынков Да/Нет и рынками множественного выбора, выплаты со скалярных рынков распределяются между всеми участниками. Каждая выплата основана на том, насколько цена попадает в диапазон относительно результата. Поэтому, если на дату закрытия цена BTC составит 198 тысяч долларов, то банк будет разделен между всеми покупателями. Однако тот, кто ближе всего ответит на цену в 200 тысяч долларов, получит наибольшую сумму выигрыша пропорционально размеру своих ставок.

Для скалярного рынка цена за долю соответствует определенной цене исполнения базового актива или тому, что прогнозируется.

Решение

Используя тот же пример, что и раньше, как определить, превысит ли биткоин 100 000 долларов к 31 декабря 2021 года? Я ссылаюсь на Coinbase или я ссылаюсь на совокупные цены всех бирж на CoinGecko? На практике маркетмейкер будет указывать источник решения до его создания. Таким образом, в этом сценарии можно установить Coinbase в качестве источника решения.

Реальная проблема заключается в том, кто предоставляет эту информацию и как эта информация проверяется? Для рынков, основанных на ценах, общедоступные API-интерфейсы могут быть созданы и получены из онлайн-источников. Также можно использовать оракулы, но они могут охватывать не все типы рынков, например, «Женится ли Виталик Бутерин до 2022 года?»

Учитывая размер и масштабы рынков прогнозирования, полагаться исключительно на технологии невозможно. Протоколы прогнозирования признают это и полагаются на людей, чтобы гарантировать точность информации.

Однако, как можно гарантировать, что плохие игроки не манипулируют рынком, предоставляя ложную информацию? В отличие от обычных рынков прогнозирования, протоколы прогнозирования децентрализованы и не располагают ресурсами для мониторинга и регулирования каждого рынка. Чтобы решить эту проблему, протоколы прогнозирования предложили различные решения. В этой главе мы рассмотрим два примера.

Протоколы рынков прогнозирования

Augur



Augur работает в сети Ethereum и использует модель решения, которая побуждает пользователей сообщать точную информацию и регулируется это с помощью вознаграждений и штрафов. После закрытия рынка начнется отчетный период, в течение которого либо создатель рынка, либо кто-либо другой (в зависимости от того, кого создатель рынка указал в качестве Назначенного Докладчика - НД) может предоставить информацию для подтверждения результатов.

В течение отчетного периода у НД будет 24 часа, чтобы представить отчет о результатах рынка. Загвоздка в том, что НД должен поставить собственный токен протокола, прежде чем сообщать о своих выводах.

Существует две версии собственных токенов: REP и REPv2. Токены REPv2 применяются только для обновленного протокола Augur v2, в то время как REP можно перенести и обменять на токены REPv2.

Ключевое отличие заключается в том, что держатели REP не могут участвовать в форке, если возникнет существенный спор по поводу результата. Однако мы будем коллективно называть их токенами REP для простоты, потому что они функционально похожи.

Какой бы исход ни выбрал НД, он становится предварительным исходом выигрыша (ПИВ). Как только НД отправляет ПИВ, результат открыт для оспоривания. Оспариваемые результаты откроют период споров на одну неделю, когда любой, у кого есть REP, может сделать ставку на ответ, который, по их мнению, является правильным. Один раунд длится одну неделю, но может достигать шестнадцати раундов.

Если спора нет, часть выигрыша используется для компенсации НД. Эта ставка вознаграждения является переменной и определяется на основе общей совокупной стоимости всех токенов REP, находящихся в обращении.

Если возникнет спор, пользователи, сделавшие ставку на выигрышный исход, получат долю REP, которая была поставлена на проигрышный исход. Это в дополнение к гонорару, который получат начавшие спор. Пользователи, которые сделали ставку на проигрышный исход, не получат никаких комиссий и потеряют все свои токены REP.

Omen



Omen – это протокол прогнозирования, разработанный DXdao и основанный на протоколе Gnosis – он работает на Ethereum и сайдчейне xDai. Gnosis позволяет пользователям Omen взаимодействовать со своей структурой токенов, классом активов на основе событий, который включает в себя основу рынков прогнозирования.

В отличие от Augur, Omen не стимулирует сообщество сообщать о рынках и решать споры. Вместо этого они полагаются на децентрализованный оракул, управляемый сообществом, известный как Reality.eth, который проверяет фактические события для смарт-контрактов.

Большинство рынков будут решены в соответствии с Reality.eth, где члены сообщества будут принимать решения на основе комиссий. Пользователи на Reality.eth размещают залог для выбранных ими исходов, но им может быть брошен вызов, если кто-то опубликует другой исход и удвоит залог. Это может происходить в течение нескольких циклов, пока спор не прекратится, где ответ определяется последним человеком, разместившим свой залог.

Когда Reality.eth выполнила свои обязательства по решению исхода, они предоставляют результаты на соответствующий рынок Omen. Если пользователь Omen недоволен результатами, он может (через Reality.eth) обратиться к внешнему арбитру, Kleros.

Клерос случайным образом выбирает присяжных из определенного пула и предлагает вознаграждения, основанное на теории игр, чтобы обеспечить достижение консенсуса анонимными голосами. Те, кто делает ставку на правильные результаты, получают деньги от тех, кто сделал ставку на неправильные результаты (очень похоже на Augur).

Примечательно, что DXdao, самоуправляющаяся организация, стоящая за Omen, также может принять решение действовать в качестве компетентного арбитра в будущем.

Каковы еще ключевые различия между Augur и Omen?

Как мы только что обсуждали, и у Augur, и у Omen очень разные подходы к процессу урегулирования споров. Augur решает проблему оракула, создавая экосистему вознаграждений и штрафов, которые регулируют надежность отчетной информации. Omen же передает свои потребности в отчетности на аутсорсинг внешнему DAO (используя там те же принципы, что и Augur). В этом смысле Augur более самодостаточен.

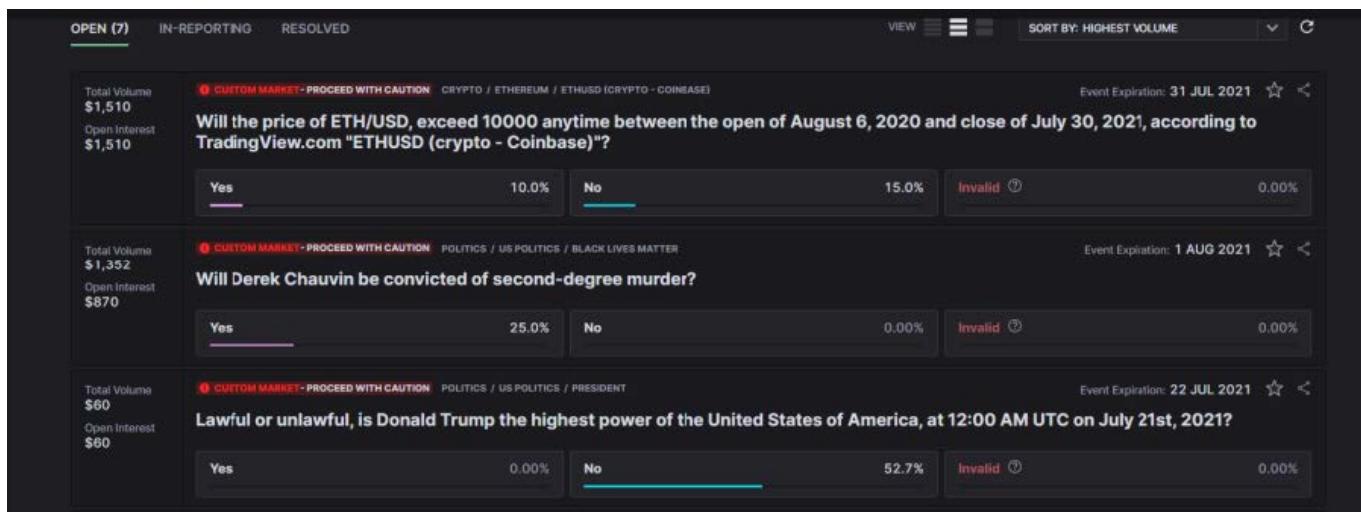
С точки зрения ликвидности рынки на Augur v2 используют внеблокчейновую книгу ордеров, а реализуются данные ордеры уже в блокчейне. Напротив, автоматизированные маркетмейкеры Omen работают аналогично DEX, такой как Uniswap, которая создает большие пулы ликвидности для пар токенов.

Хотя оба токена результата используют стандарт ERC-1155, токены Omen могут быть обернуты в стандарт ERC-20 и доступны за пределами их сети – это позволяет Omen получать доступ к DEX и подключаться к более крупным пулам ликвидности. В отличие от такого решения, токены результатов Augur ограничены только внутренними пулами ликвидности их протокола.

Для краткого сравнения Augur и Omen вы можете обратиться к таблице ниже:

Параметры	Augur	Omen
Система проверки информации	Использование внутренних вознаграждений и штрафов для арбитража	Передано на аутсорсинг внешним арбитрам DAO
Ликвидность	Традиционная книга ордеров + протокол в блокчейне для децентрализованного исполнения	Автоматизированный маркетмейкер
Управление	Уничтоженный ключ администратора означает невозможность каких-либо обновлений	DAO
Токены	REP (REP + REPv2)	
Токены исхода	ERC-1155	ERC-1155, но могут быть обернуты в ERC-20 для доступа к пулам ликвидности сторонних DEXs
Рыночные пары	DAI	30 пар
Поддерживаемые блокчейны	Ethereum	Ethereum, xDai

У нас нет доступа к рыночным данным ни одного из протоколов, но сканирование (проведенное 28 апреля 2021 года) веб-сайтов обоих протоколов показывает, что происходит очень мало активности.



Для Augur создано всего семь рынков. Только первые три имеют фактический объем торгов, который в совокупности составляет всего около 3000 долларов.

What will Joe Biden's Presidential Job Approval Rating be after 100 days in office? (Source: Gallup)

★ 54.00 % | 6 days remaining | 3.25K xDAI - Liquidity

What will the average USD price of CTX be on May 1st, 2021? (REF: most liquid of Uniswap, Sushiswap, or Swapr pools)

★ 18.50 USD | 5 days remaining | 2.19K xDAI - Liquidity

Will Compound Chain be launched and usable by the end of Q2 2021?

★ No (73.40%) | 2 months remaining | 1.63K xDAI - Liquidity

Will EIP-1559 be deployed on Mainnet before August 2021?

★ Yes (75.33%) | 3 months remaining | 1.13K xDAI - Liquidity

А что касается Omen, то есть только четыре рынка, но общий объем торгов составляет примерно 7200 долларов США (нет на изображении, но показано на другой веб-странице).

Сопутствующие риски

Самая большая проблема на рынках прогнозирования – это надежность данных. Хотя существует множество стимулов, основанных на прибыли для минимизации манипулирования данными, всё-таки нерациональные действия некоторых пользователей могут поставить под угрозу корректность результатов. Кроме того, оспариваемые результаты могут привести к ситуациям, которые отнимают много времени и будут дорогостоящими.

Протоколы рынков прогнозирования, заслуживающие упоминания



По состоянию на апрель 2021 года на Polymarket есть продукт в бета-стадии, который работает на Ethereum. Официальных документов для протокола еще не опубликовано, но они, похоже, представляют собой гибрид между централизованными и децентрализованными структурами. Протокол кажется гораздо более популярным, чем Augur или Omen – наше быстрое сканирование 28 апреля 2021 года показало бурный рост рыночной активности на более чем шестидесяти рынках предсказаний. Только на самом популярном рынке объем торгов составил около 2 миллионов долларов.

Вывод

Рынки прогнозов – интересное финансовое поле, потому что есть ситуации, выходящие за рамки ставок, – это позволяет пользователям хеджировать различные риски. Традиционные деривативы позволяют покупателям и продавцам хеджировать определенные результаты, сохраняя за собой право торговать конкретным товаром в будущем по определенной цене. Например, фермер, выращивающий рис, может заключить дериватив на продажу 1000 килограммов риса 31 декабря 2021 года за 5000 долларов, если он ожидает, что цена будет ниже в течение этого времени.

Рынки прогнозирования могут основываться на чем угодно, а не только на рисе. Вместо того чтобы хеджировать цены на рис, рисовод может решить вместо этого застраховаться от погоды. Другими словами, рынки прогнозирования позволяют пользователям хеджировать более конкретные риски.

Протоколы прогнозирования предоставляют платформу для любого, кто может застраховаться от чего угодно. К слову, сами рынки прогнозирования также могут выступать в качестве опросов «де-факто». Участники протоколов прогнозирования эффективно делятся своими мнениями по различным вопросам, которые могут быть экстраполированы для получения общей информации по широкому кругу тем.

Будущее протоколов прогнозирования захватывающе, потому что их принципы могут стать основой для реальных случаев использования. Можно было бы представить себе использование аналогичных систем разрешения споров для включения юридических контрактов в блокчейн, поскольку методы арбитража функционируют очень похоже на систему правосудия, основанную на присяжных заседателях. Однако в ближайшей перспективе мы ожидаем, что большее количество протоколов будет использовать возможности протоколов прогнозирования и использовать их для создания инновационных инструментов хеджирования.

Рекомендуемая литература

1. Основы рынков прогнозирования

<https://augur.net/blog/prediction-markets>

2. Оценки в рынках прогнозирования

<https://medium.com/veil-blog/a-guide-to-augur-market-economics-16c66d956b6c>

3. Как рынки прогнозирования сопротивляются с недобросовестными манипуляциями

<https://blog.gnosis.pm/how-manipulation-resistant-are-prediction-markets-710e14033d62>

4. Ключевые отличия Augur и Omen

<https://blog.gnosis.pm/omen-and-the-next-generation-of-prediction-markets-2e7a2dd604e>

ГЛАВА 11: ДЕЦЕНТРАЛИЗОВАННЫЕ ПРОТОКОЛЫ С ФИКСИРОВАННОЙ ПРОЦЕНТНОЙ СТАВКОЙ

Если мы посмотрим на традиционные финансы, где проживает большинство финансовых потребителей, глобализация привела к росту спроса на стабильные финансовые экосистемы. Действительно, прошло более 20 лет с тех пор, как Европарламент впервые признал необходимость большей стабильности цен в своем документе, озаглавленном «Определение процентных ставок»:

«Интеграция мировых финансовых рынков усиливает давление внешних факторов при определении внутренней денежно-кредитной политики. Кроме того, хотя и подходы крупнейших центральных банков мира к проведению денежно-кредитной политики различаются в деталях, существует широкое согласие по основным вопросам: стремление к стабильности цен и стабильности финансовых рынков».

Ключевым моментом здесь является интеграция. Аналогично тому, как работает криptoиндустрия, пространство созрело до такой степени, что DeFi стал отраслевым стандартом для протоколов. Часто называемая финансовым LEGO, технология блокчейна позволила разработчикам интегрироваться с другими протоколами и создавать инновационные финансовые продукты. Однако такой прогресс не меняет того факта, что криptoиндустрия непредсказуема и крайне изменчива.

Стабильные процентные ставки являются важным аспектом любой финансовой экосистемы. Хотя существует множество протоколов кредитования и агрегаторов доходности, которые предлагают процентные ставки кредиторам в криptoиндустрии, относительно немногие из них предлагают фиксированные процентные ставки.

В связи с растущей популярностью фарминга и спросом на более стабильные ставки кредитования и займов, несколько протоколов DeFi попытались удовлетворить постоянно растущий спрос на стабильные процентные ставки и стали отличительной чертой надежности. Это породило новый класс протоколов, известных как Протоколы с фиксированной процентной ставкой (FIRP).

По сравнению с традиционными финансами, где фиксированные процентные ставки предоставляются в форме фиксированных депозитов (или облигаций), FIRP использует базовую структуру токеномики и предлагает различные стимулы для поддержания своих процентных ставок. На данный момент экосистему FIRP можно в целом разделить на две категории:

1. Кредитование/Заемствование
2. Агрегаторы доходности

Даже в соответствии с этой общей классификацией, FIRP бывают разных форм и размеров. Каждый протокол имеет свой метод «фиксации» процентных ставок, что приводит к различным вариантам использования. Некоторые предлагают «фиксированную процентную ставку» или «фиксированный процентный коэффициент доходности». Более того, некоторые FIRP вообще не предлагают фиксированных процентных ставок, а скорее создают условия, способствующие фиксированным процентным ставкам.

В этой главе мы рассмотрим три примера.

Обзор Протоколов с фиксированными процентными ставками

Yield



Yield – это децентрализованная система кредитования, которая предлагает рынки кредитования с фиксированной ставкой и процентными ставками доходности с использованием нового вида токенов под названием «fyTokens». Текущая итерация (версия 1) включает в себя fyTokens для стейблкоина DAI. Этот новый класс токенов, называемый «fyDai», позволяет полностью обеспечивать займы и кредиты с фиксированной ставкой в DAI.

Токены fyDai – это токены на основе Ethereum (ERC20), которые можно обменять на DAI после заранее определенной даты погашения. fyDai аналогичны облигациям с нулевым купоном или дисконтом.

Чтобы создать или продать fyDai, заемщикам придется предоставить обеспечение ETH, которое в настоящее время соответствует тому же коэффициенту обеспечения, что и MakerDAO (150%). Кредиторы покупают fyDai, цена которого, как правило, будет снижена по сравнению с DAI. Разница между дисконтированной стоимостью и 1 DAI (стоимостью при погашении) представляет собой кредитную ставку кредитора или ставку заимствования заемщика.

Хотя стоимость fyDai отражает процентную ставку по кредитованию/заимствованию, он также может быть продан на рынке в качестве самостоятельного облигационного инструмента. Это возможно, потому что существует несколько «серий» fyDai, каждая из которых имеет разную дату погашения.

Система тесно интегрирована и дополняет Maker. Пользователи Maker могут «перенести» свои хранилища DAI в хранилища fyDai, зафиксировав процентную

ставку на определенный период и конвертировав обратно в хранилище Maker после погашения.

Процентные ставки определяются рыночной оценкой fyDai (при этом каждая серия имеет свою собственную дату погашения). Для кредиторов более высокая оценка fyDai снизит процентные ставки, полученные по достижении срока погашения.

И наоборот, более высокая оценка fyDai снизит ставку заимствования, поскольку он будет продан для покупки соответствующего стейблкоина (например, DAI). Это означает, что в зависимости от времени покупки токенов fyDai как заемщики, так и кредиторы могут определять процентную ставку по займам/кредитам.

Пример

Предположим, что заемщик вносит 1,5 ETH в качестве залога и намерен занять 900 DAI по годовой ставке заимствования 10%. После исполнения заемщик получит 1000 fyDai со стоимостью 900 DAI – они будут автоматически проданы протоколом на рынке, и заемщик получит 900 DAI. В конце годичного срока погашения заемщик должен будет погасить 990 DAI, если он пожелает отозвать свое обеспечение.

Для кредиторов предположим, что он предоставляет 1000 DAI. Взамен кредитор получает 1000 fyDai, которые будут накапливаться по мере приближения срока погашения. Первоначально 1 полученный fyDai стоит 1 DAI, но по истечении одного года 1 fyDai будет стоить 1,1 DAI. Затем кредитор может продать свои 1000 fyDai за 1100 DAI. Это эффективно определяет процентную ставку по кредиту в 10%.

На практике пользователи могут выбирать только серии fyDai, которые были предварительно запрограммированы Yield. Это похоже на то, как функционируют обычные облигационные инструменты, где существуют различные ставки по облигациям и сроки погашения.

В 1 квартале 2021 года Yield предложила интеграцию с протоколом MakerDAO, который позволил бы MakerDAO быть кредитором DAI с фиксированной ставкой для получения заемщиков. Это предложение было принято руководством MakerDAO и находится в процессе интеграции в протокол MakerDAO.

Yield также ожидает запуска версии 2 своего протокола летом 2021 года. Он будет включать новые типы обеспечения и позволит заимствовать активы кроме DAI, такие как USDC и Tether.

А вы знали?

В январе 2021 года анонимное физическое лицо погасило свой ипотечный кредит в банке и теперь выплачивает свой рефинансированный ипотечный кредит с помощью Defi протокола под названием «Notional Finance». Notional обладает аналогичными функциями по доходности, поскольку они также используют систему облигаций с нулевым купоном благодаря внедрению нового финансового примитива под названием fCash.

Saffron.Finance



Saffron Finance является децентрализованным агрегатором доходности для провайдеров ликвидности и был одним из первых протоколов, использующих систему, основанную на траншах. Транш – это сегменты, созданные из пулов ликвидности, которые разделены по риску, сроку погашения или другим характеристикам, чтобы быть доступными для разных инвесторов.

С помощью различных траншей пользователи Saffron Finance могут выбирать различные портфели в зависимости от их предпочтительного отношения к риску. Что еще более важно, экосистема Saffron Finance создает внутреннюю систему страхования, в которой инвесторы в траншах с более высоким риском страхуют инвесторов в траншах с более низким риском.

Собственный токен Saffron Finance, SFI, в основном используется в качестве токена для доступа к траншу А с наиболее высоким доходом. Тем не менее, SFI также можно вложить в протокол, чтобы получить вознаграждение в пуле и иметь возможность голосовать в процессе управления протоколом.

Система траншей позволяет распределять доходы и создавать разные ставки для разных пулов. В случае с Saffron Finance транш А в десять раз превышает прибыль транша АА. Транш S предлагает переменную процентную ставку, которая уравновешивает транши А и АА. Они всегда находятся в идеальном равновесии, чтобы поддерживать десятикратное соотношение прибыли с фиксированным процентом между траншем А и траншем АА.

Пример

Если транш AA заработает 100 DAI:

1) Транш A будет зарабатывать 1000 DAI

2) Транш S будет зарабатывать DAI со скоростью, которая гарантирует, что транш A выплатит в 10 раз больше, чем транш AA

Однако, даже если и существует риск платформы (например, событие черного лебедя), Транш AA получит свои депонированные активы и прибыль в первую очередь – это берется из основной суммы и процентных доходов Транша A.

Horizon Finance



В отличие от обычных агрегаторов доходности, Horizon позволяет пользователям создавать свои собственные рынки, основанные на принципах теории игр. Теория игр предполагает пространство, в котором существуют только рациональные действующие лица. В такой гипотетической ситуации покупатели и продавцы будут принимать оптимальные решения на основе имеющейся информации.

Horizon позволяет пользователям вносить свое обеспечение в пул ликвидности, который затем предоставляется в протоколы кредитования, такие как Compound. Чтобы предоставить пользователям фиксированные процентные ставки, Horizon предлагает пользователям отправлять свои закрытые заявки на фиксированные процентные ставки (действующие как ограничения доходности) или плавающие процентные ставки в каждом раунде

Ставки раскрываются после каждого раунда, создавая таким образом книгу ордеров. Протокол ранжирует ставки от самой низкой процентной ставки до самой высокой процентной ставки. Переменная прибыль по протоколу кредитования затем распределяется от ставок с самой низкой процентной ставкой до ставок с самой высокой процентной ставкой, при этом любой избыточный доход переходит в плавающий пул.

Одной из примечательных особенностей является то, что все ставки будут отображаться на веб-сайте Horizon. Отображаемые ставки позволяют пользователям активно конкурировать и определять, какие процентные ставки являются наиболее популярными. Кроме того, пользователи могут свободно изменять свои ставки, в том числе переходить на плавающую ставку. Horizon, по сути, работая как протокол прогнозирования доходности.

Пример

Чтобы проиллюстрировать это, предположим, что раунд для пула X длится с 1 мая 2021 года по 14 мая 2021 года:

1 мая

- Участник А вносит 100 000 DAI и выбирает ставку 20%.
- Участник В вносит 100 000 DAI и выбирает плавающую ставку.

7 мая

- Участник С вносит 100 000 DAI и выбирает ставку 10%.

На данный момент Участник А пересматривает свою заявку, поскольку Участник С подал гораздо более низкую ставку. Если Пул X зарабатывает слишком мало, он может вообще ничего не получить.

13 мая,

- Участник А изменяет свою ставку до 5% процентной ставки.

После окончания раунда, допустим, 300 000 DAI в пуле X смогли заработать процентную ставку в размере 4% на общую сумму 461 DAI, таким образом:

- Участник А выполняет свою заявку и получает 192 DAI, получая процентную ставку 5%.
- Участник С частично завершает свою заявку и получает оставшиеся 269 DAI, что составляет 7% процентной ставки. Его первоначальная ставка в размере 10%, если бы она была полностью выполнена, принесла бы 383 DAI в течение двухнедельного периода, если бы Пул X заработал достаточный процент.
- Участник В не выполняет свою заявку и ничего не получает.

Как вы заметили, здесь задействовано множество игр интеллекта! Более того, процентные ставки технически не являются фиксированными. Однако система вознаграждает пользователей, которые могут оценить сумму процентов, которую они должны получить от своих ставок. Это стимулирует пользователей соответствовать «безопасной» ставке, если они не уверены в сумме, которую они могли бы заработать. Слишком высокие ставки или ставки с плавающей ставкой могут привести к меньшей прибыли или вообще к нулю. Таким образом, «безопасные» ставки фактически становятся фиксированной процентной ставкой с течением времени.

Какой FIRP лучше использовать?

FIRP нельзя складывать в одну кучу и сравнивать друг с другом. Во-первых, протоколы кредитования сильно отличаются от агрегаторов доходности.

Прежде чем рассматривать более ориентированные на прибыль показатели, такие как конкурентоспособность процентных ставок, мы должны рассмотреть способность FIRP поддерживать свою «фиксированную процентную ставку», которая фактически является их основной функцией. И если бы мы проанализировали, как работают FIRP, то, по сути, было бы три определяющих характеристики, которые врачаются вокруг фиксированных процентных ставок:

I. Что они предлагают?

Разные протоколы предлагают различные условия. Например, Saffron Finance обещает, что, если вы примете участие в транше A, вы заработаете в 10 раз больше, чем в транше AA. Horizon же не дает никаких обещаний относительно того, сколько вы заработаете. Понимание данных обещаний позволяет пользователям решать, какой протокол предлагает лучший продукт.

II. Как они намерены выполнить свои обещания?

Для каждого обещания требуется своя методология. Например, Saffron Finance предлагает страхование пользователям транша AA, предоставляя прибыль в первую очередь им в случае дефицита. Понимание того, как выполняется каждое обещание, позволяет пользователям определить, какой протокол является более надежным.

III. Насколько протоколы зависят от внешних факторов?

Разработка механизмов протоколов, влияющих на поведение пользователей, имеет важное значение для всех FIRP. Например, доходность требует относительно равномерных соотношений кредиторов и заемщиков для поддержания фиксированных процентных ставок. Выявление таких особенностей позволяет пользователям

определить, насколько обещание протокола подвержено влиянию факторов, находящихся вне их прямого контроля.

Если мы рассмотрим эти критерии, то невозможно сказать, какой из них лучше всего подойдет вам. В конечном счете, это сводится к предпочтению каждого человека к риску, типу требуемого финансового инструмента и вере в механизмы, лежащие в основе протокола. И, возможно, что еще более важно, отрасль все еще зарождается, потому что многие протоколы все еще создаются – им еще предстоит проявить себя, особенно в сложных рыночных условиях, которые угрожают их способности предлагать фиксированные процентные ставки.

Сопутствующие риски

Одним из наиболее существенных рисков является способность FIRP предоставлять фиксированные процентные ставки. Большинство из этих протоколов полагаются на внешних агентов или других пользователей, которые активно участвуют в протоколе для обеспечения функциональности рынка.

Если существует неактивное сообщество или непропорционально большое количество профилей пользователей и ликвидности (например, больше кредиторов, чем заемщиков по доходности, или больше участников в транше A, чем в транше AA для Saffron Finance), FIRP могут не иметь возможности поддерживать свои фиксированные процентные ставки.

Протоколы с фиксированной ставкой, заслуживающие упоминания



Notional облегчает кредитование с фиксированной ставкой, срочное кредитование и заимствование криptoактивов. Как и Yield Protocol, оба протокола имеют очень схожие функциональные возможности, поскольку в Notional создается система облигаций с нулевым купоном за счет внедрения нового финансового примитива под названием fCash. Однако есть некоторые ключевые различия. В частности, Notional использует другой автоматизированный маркетмейкер и другие варианты обеспечения.



BarnBridge использует систему траншей (аналогично Saffron Finance) для продуктов, основанных на доходности. Тем не менее, у BarnBridge также есть другой продукт (SMART Alpha), который предлагает оказывать влияние на рыночные цены с помощью деривативов на волатильности самих траншей.



88mph

88mph – это агрегатор доходности, который предлагает фиксированные процентные ставки. Они способны поддерживать свои ставки за счет введения облигаций с плавающей ставкой и уникальной структуры токеномики, которая помогает влиять на поведение рынка.



Pendle

Pendle – это новый протокол, который позволяет пользователям токенизировать будущую доходность, которую затем можно продать за предоплату. По сути, Pendle рассчитывает вашу ожидаемую доходность, эффективно фиксируя ваши процентные ставки.

Вывод

FIRP это новый набор протоколов, которые обязательно станут основным элементом в DeFi. Мы выделили три примера, потому что они являются инновационными и способны продемонстрировать потенциал DeFi в сочетании с традиционными инструментами с фиксированным доходом.

В этом пространстве есть много интересных разработок, которые предлагают уникальные продукты и услуги. У нас уже есть протоколы, сочетающие прогнозирование цен и агрегирование доходности; представьте, что банк предложил бы рынок ставок на фиксированную доходность депозитов? Мы даже не обсуждали протоколы, которые токенизируют будущую доходность, что, по сути, позволяет любому создавать свои собственные облигации и продавать их за предоплату.

По мере дальнейшего развития этой области мы ожидаем роста институционального интереса к продуктам FIRP. Инструменты с фиксированным доходом всегда были обычным явлением в традиционных финансах. Однако, поскольку совокупный уровень долга и инфляция продолжают расти, а стоимость доллара США продолжает падать, FIRP могут предлагать более надежную доходность.

Рекомендуемая литература

1. Отчет по кредитованию в DeFi на основе траншей

<https://consensys.net/blog/codefi/how-tranche-lending-will-bring-fixed-interest-rates-to-defi/>

2. Обзоры протоколов с фиксированной доходностью

<https://messari.io/article/fixed-income-protocols-the-next-wave-of-defi-innovation>

3. Почему протоколы с фиксированной доходностью так важны

<https://medium.com/notional-finance/why-fixed-rates-matter-1b03991275d6>

ГЛАВА 12: ДЕЦЕНТРАЛИЗОВАННЫЕ АГРЕГАТОРЫ ДОХОДНОСТИ

Криптография породила деятельность по фармингу, где пользователи могут получать доход, просто выделяя капитал в протоколах DeFi. Многие крипто-аборигены с тех пор стали фермерами, в поисках наиболее привлекательных доходов.

Криптовалюты породили деятельность по фармингу, где пользователи могут получать доход, просто размещая капитал в протоколах DeFi. Многие крипто-аборигены с тех пор стали фермерами, в поисках наиболее привлекательных доходов.

Из-за огромного количества новых ферм, выпускаемых каждый день, ни один человек не может знать о каждой возможности. При огромных процентах дивидендов, потенциальная стоимость упущеной выгоды при пропуске нового фарминга увеличилась значительно.

Протоколы агрегаторов доходности

Yearn Finance



ABOUT
yearn.finance
yearn.finance defi made simple

Yearn Finance начался как проект Андре Кронье, основанный только на энтузиазме, по автоматизации переноса капитала между кредитными платформами DeFi для поиска наилучшей доходности. Это необходимо, поскольку большинство кредитных платформ DeFi предоставляют плавающие, а не фиксированные ставки. Средства автоматически переводятся между dYdX, Aave и Compound при изменении процентных ставок между этими протоколами.

Услуга включает в себя основные стейблкоины в долларах США, такие как DAI, USDT, USDC и TUSD. Например, если пользователь вносит DAI в Yearn Finance, он получит взамен токен yDAI, собирающий доход.

Позже Yearn Finance стала сотрудничать с Curve Finance, чтобы выпустить пул токенов USD, приносящий доход, под названием yUSD. Curve Finance – это децентрализованная биржа, которая фокусируется на торговле активами схожей стоимости, такими как стейблкоины в долларах США. yUSD – это пул ликвидности, включающий четыре у-токена: yDAI, yUSDT, yUSDC и yTUSD.

Имея yUSD, пользователь имеет 5 возможных источников дохода:

1. Кредитование DAI
2. Кредитование USDT
3. Кредитование USDC
4. Кредитование TUSD
5. Комиссии за своп, за счет предоставления ликвидности Curve Finance

Таким образом, yUSD продвигается как превосходный стейблкоин доллара США, чем просто хранение базовых стейблкоинов.

Хранилища

Компания Yearn Finance презентовала функцию хранилища после запуска токена, вызвав ажиотаж вокруг автоматизированного ведения фарминга, и считается инициатором категории агрегаторов фарминга. Хранилища помогают пользователям получать вознаграждение за добычу ликвидности и продавать собственные токены протокола за базовые активы.

Хранилища приносят доход пользователям за счет снижения затрат на газ, автоматизации процесса получения прибыли и ребалансировки, а также автоматического перемещения капитала по мере возникновения новых возможностей. Пользователям также не нужно обладать глубокими знаниями о соответствующих базовых протоколах. Таким образом, хранилища представляют собой стратегию пассивного инвестирования для пользователей. Это сродни криpto-хедж-фонду, где цель состоит в том, чтобы увеличить количество активов, которые пользователи депонировали.

Помимо простого фарминга, Yearn Finance также интегрировала различные новые стратегии, чтобы помочь увеличить доходность хранилищ. Например, она может использовать любые активы в качестве залога для заимствования стейблкоинов и использовать эти стейблкоины в хранилище стейблкоинов. Любые последующие доходы затем используются для выкупа актива.

Версия 2 Yearn была запущена 18 января 2021 года. 73 хранилища версии 2 могут использовать несколько стратегий для каждого хранилища (до 20 стратегий одновременно), в отличие от хранилищ версии 1, в которых используется только одна стратегия для каждого хранилища.

Стратегии

Будучи агрегатором доходности, Yearn Finance в максимально возможной степени использовала функцию совместимости различных продуктов на Ethereum. Ниже мы рассмотрим, какую роль играет программа добычи ликвидности Curve Finance в стратегии хранилища Yearn Finance.

Curve Finance – это децентрализованная биржа, которая фокусируется на парах стейблкоинов. Она использует довольно сложную систему управления – veCRV используется для измерения права голоса в управлении, которое пользователи могут получить, заблокировав свои токены CRV.

- 1 CRV, заблокированный на 4 года = 1 veCRV
- 1 CRV, заблокированный на 3 года = 0,75 veCRV
- 1 CRV, заблокированный на 2 года = 0,5 veCRV
- 1 CRV, заблокированный на 1 год = 0,25 veCRV

veCRV можно использовать для голосования за листинг новых пар и принятия решения о том, какое вознаграждение за фарминг CRV будет предоставлено каждой паре. Что еще более важно, veCRV используется для определения вознаграждения за повышение доходности, доступного провайдерам ликвидности.

Pool	Base APY ▼	Rewards APY
 y USD yDAI+yUSDC+yUSDT+yTUSD	22.91%	+8.68% → 21.69% CRV

Ссылаясь на изображение выше, yUSD представляет собой пул стейблкоинов, приносящих доход. Пользователи могут внести yUSD в Curve Finance, чтобы получить yCRV, где награды CRV будут собраны и проданы, чтобы получить больше yUSD.

«Базовая годовая процентная доходность» (Base APY) связана с комиссией за обмен, получаемой за то, что вы являетесь провайдером ликвидности пула Curve. «Награды APY» (Rewards APY) связаны с вознаграждениями за программу майнинга ликвидности в виде токенов CRV. При использовании veCRV вознаграждение в размере 8,68% может быть увеличено до 21,69%, или в 2,5 раза по сравнению с базовыми. В общей сложности ожидаемая доходность составляет примерно от 31,59% до 44,60%.

Внося стейблкоины доллара США в Yearn Finance, вы получите максимальную выгоду от повышения доходности в 2,5 раза вместо того, чтобы блокировать свои CRV, чтобы получить повышение доходности.

Партнерства Yearn Finance

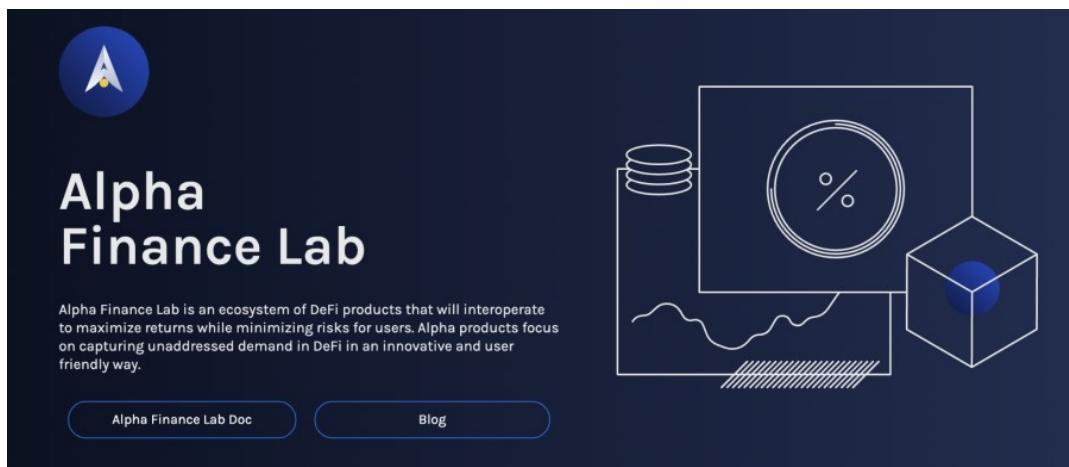
С 24 ноября 2020 года по 3 декабря 2020 года Yearn Finance объявила о серии партнерских отношений (называемых слияниями и поглощениями) по нескольким протоколам, по сути, образуя альянс, основанный на YFI.

- Sushi Swap присоединился в качестве своего автоматизированного маркетмейкера (AMM)
- Cover присоединился в качестве платформы страхования
- CREAM присоединился в качестве своей платформы кредитования
- Akropolis присоединился в качестве провайдера институциональных услуг для хранилищ и будущих кредитных продуктов
- Pickle присоединился в качестве одного из стратегов

Затем Yearn Finance решила прекратить партнерство с Cover Protocol 5 марта 2021 года.

Версия 2 Yearn Finance также стимулирует взносы сообщества, распределяя процент прибыли между стратегами сообщества. Yearn Finance также создала партнерскую программу с другими протоколами, которые готовы формировать синергетические отношения, в результате чего протоколы могут получать до 50% от получаемого дохода. Другими словами, Yearn Finance превратилась в большую экосистему, предлагающую широкий спектр продуктов и услуг для фарминга.

Alpha Finance



Alpha Finance внедрила фарминг с использованием заемных средств с помощью своего первого продукта Alpha Homora, что позволило пользователям использовать заемный капитал для увеличения их участия в фарминге. По сути, он действует как протокол агрегатора кредитов и доходов.

В версии 2 Alpha Homora пользователи могут кредитовать (для получения процентной ставки по кредиту) и занимать многие активы (для повышения своей доходности), включая ETH, DAI, USDT, USDC, YFI, SNX, sUSD, DPI, UNI, SUSHI, LINK и WBTC.

Пример

Используя пример пары SUSHI/ETH, как упоминалось в главе 2, вместо того, чтобы заниматься фармингом с капиталом всего в 1000 долларов с помощью Alpha Homora, теперь вы можете использовать в два раза больший капитал, заимствуя ETH на сумму 1000 долларов.

Заняв 1000 долларов, вы теперь будете участвовать в выращивании урожая, предоставив ETH на сумму 1000 долларов и SUSHI на сумму 1000 долларов, в общем на 2000 долларов. Эта стратегия принесет прибыль только в том случае, если сборы за обмен и вознаграждение за фарминг будут больше, чем стоимость заимствования на Alpha Homora.

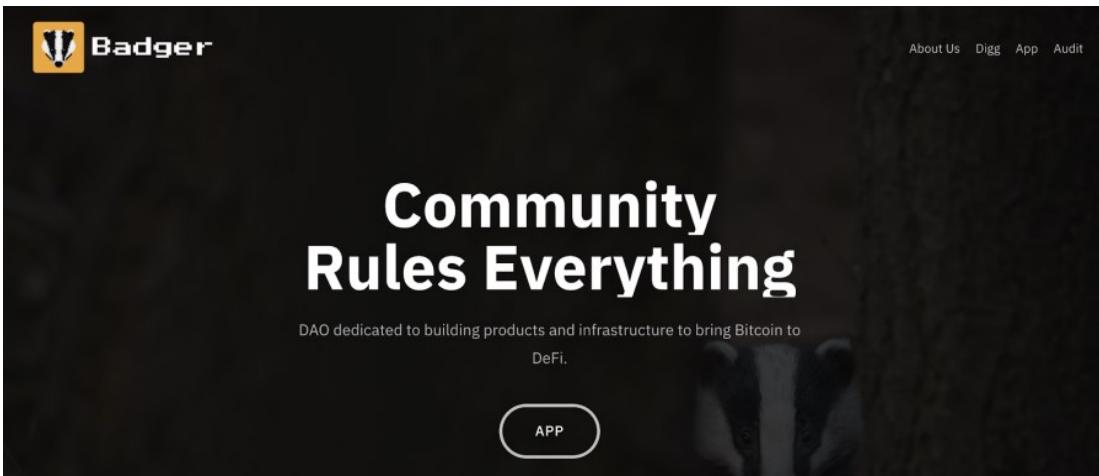
Кроме того, обратите внимание, что, поскольку ETH и SUSHI доступны в качестве заемных активов, вы можете фармить с использованием кредитного плеча заимствуя и ETH и SUSHI одновременно, чтобы минимизировать плату за обмен.

Стоимость заимствования на Alpha Homora рассчитывается по переменной ставке, зависящей от спроса и предложения. Если стоимость заимствования внезапно вырастет из-за увеличения объема заимствований, позиция с привлечением заемных средств может понести убытки. Другой риск заключается в том, что заемный актив вырос в цене по сравнению с доходностью позиции фарминга. Используя приведенный выше пример, если ETH быстро растет в цене, в то время как SUSHI падают в цене, позиция с привлечением заемных средств может быть ликвидирована.

Помимо получения более высокой прибыли, наличие позиции с кредитным плечом на фермах с высокой доходностью также подвергнет пользователей более высоким непостоянным потерям. Полученная прибыль в значительной степени зависит от выбора актива, заимствованного для фарминга. Например, заимствование ETH по сравнению со стейблкоинами в долларах США приведет к совершенно иному профилю возврата. Для получения более подробной информации о непостоянных потерях можно обратиться к ГЛАВЕ 5.

Alpha Homora версии 2 также поддерживает токены провайдера ликвидности (LP) в качестве обеспечения. Например, пользователи с ликвидностью, предоставляющей позицию в пуле ETH/SUSHI на Sushiswap, смогут внести токен ETH/SUSHI LP в качестве залога на Alpha Homora версии 2 и заимствовать больше токенов ETH и SUSHI для повышения доходности.

Badger Finance



Badger DAO стремится создать экосистему продуктов DeFi с конечной целью внедрения биткоина в Ethereum. Это первый проект DeFi, который решил сосредоточиться на биткоине в качестве основного резервного актива, а не на использовании Эфириума.

Sett – это агрегатор доходности, ориентированный на токенизированные BTC. Sett можно разделить на три основные категории:

- a) Токенизированные хранилища BTC
 - Вдохновленные хранилищами Yearn Finance, первоначальные продукты включают хранилища биткоинов, в которых фармят токены CRV, такие как SBTCCURVE, RENBTCCURVE и метапул TBTC/SBTCCURVE.
 - Они также сотрудничают с протоколом Harvest для фарминга токенов CRV и FARM с помощью RENBTCCURVE, депонированных в самом Harvest.
- b) Хранилища LP
 - Чтобы привлечь больше пользователей, существует Sett для WBTC/ETH, с помощью которого можно фармить SUSHI.
 - Кроме этого, существует четыре агрегатора Sett для начальной загрузки ликвидности для BADGER и DIGG.
 1. WBTC/BADGER UNI LP
 2. WBTC/DIGG UNI LP
 3. WBTC/BADGER SUSHI LP
 4. WBTC/DIGG SUSHI LP
- c) Хранилища Протоколов
 - Пользователи, во избежание непостоянных потерь и рисков токенизации BTC, могут просто разместить собственные токены BADGER и DIGG в хранилищах bBADGER и bDIGG, получая плату за протокол и вознаграждение за фарминг.

Интересно (на самом деле не очень-то), что слово Sett (в переводе – нора) выбрано так, как оно связано с домом барсука (badger).

Harvest Finance

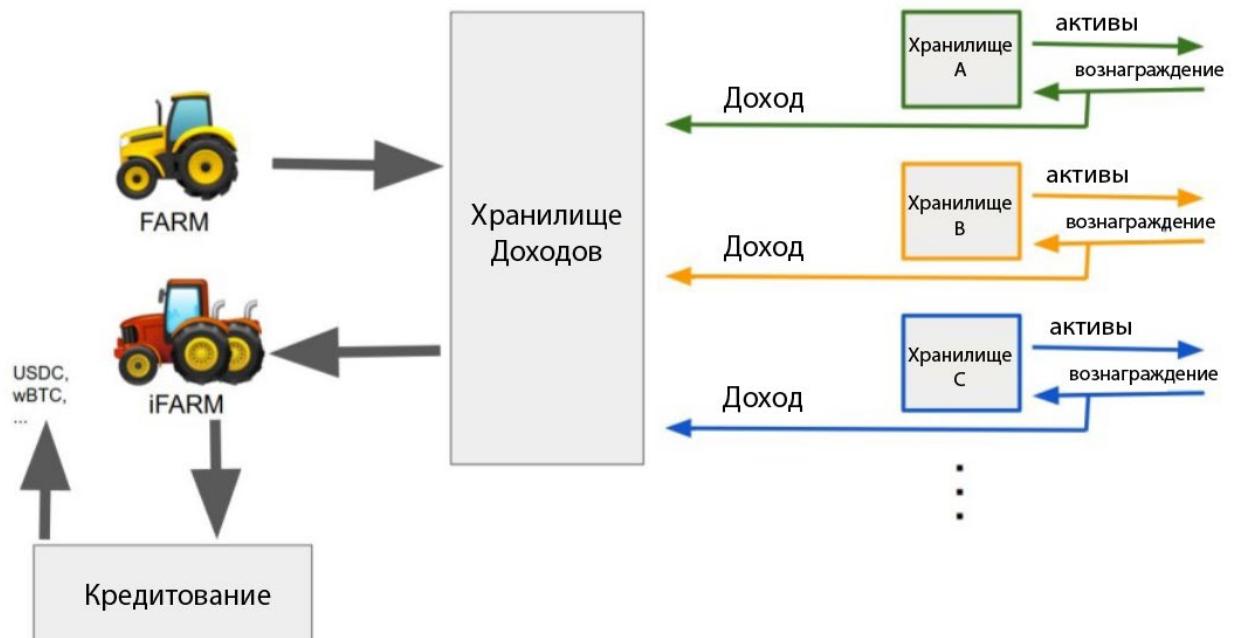


Начиная своё происхождение от форка Yearn Finance, Harvest Finance с тех пор приняла стратегию быстрого продвижения. Она выпускает новые стратегии быстрее, чем другие протоколы агрегаторов доходности, даже те, которые считаются высокорискованными.

По состоянию на апрель 2021 года она поддерживает аж 63 различных фермы только в Ethereum, с категориями, охватывающими стейблкоины, SushiSwap, ETH 2.0, BTC, NFT, 1inch, алгоритмические стейблкоины и активы mAssets от Mirror Protocol.

Он также недавно расширился до Binance Smart Chain, предлагая фермы на Ellipsis, Venus, Popsicle Finance, PancakeSwap, Goose Finance и bDollar.

Команда Harvest Finance выпустила токен FARM (iFARM), в котором пользователи могут вкладывать свои FARM, чтобы получать комиссии с протокола.



Источник: <https://mbroome02.medium.com/harvest-101-understanding-ifarm-and-its-potential-54d9cf305e5>

Сравнения агрегаторов доходности

	Yearn Finance	Alpha Finance	Badger DAO	Harvest Finance
Комиссия за управление	2 %	-	-	-
Комиссия с дохода	20 %	-	20 %	30 %
Комиссия за заимствования	-	10 % / 20 %	-	-

Одним из важных факторов, который следует учитывать при принятии решения о том, какие агрегаторы доходности использовать, является взимаемая комиссия. Yearn Finance следует стандартной модели хедж-фонда, где он взимает плату за управление в размере 2% и процент с дохода в размере 20%. Badger DAO и Harvest Finance взимают только процент с дохода в размере 20% и 30% соответственно. Alpha Homora v1 (от Alpha Finance) на Ethereum и BSC собирает 10% от суммы, заимствованной для кредитного плеча, и собирает 20% на Alpha Homora V2.

Структура комиссии предполагает, что пользователям, возможно, придется платить самые высокие сборы, инвестируя в Yearn Finance – 2% от инвестированной суммы ежегодно платится независимо от того, приносят ли стратегии прибыль или нет.

Взимание комиссии с доходов можно считать более справедливым, поскольку это просто означает меньшую отдачу для пользователей. Yearn Finance может взимать комиссию из-за своего лидирующего положения в отрасли, поскольку многие его хранилища интегрированы с другими протоколами, такими как Alchemix, Powerpool и Inverse Finance

	Yearn Finance	Alpha Finance	Badger DAO	Harvest Finance
TVL (млн. долларов)	2 000	936	1140	527
Капитализация (млн. долларов)	1 305	434	287	113
Разбавленная капитализация (млн. долларов)	1 348	1 810	975	180
Капитализация/TVL	0,65	0,46	0,25	0,21
Разбавленная капитализация/TVL	0,67	1,93	0,86	0,34

* – данные на 1 апреля 2021 года

Yearn Finance по-прежнему сохраняет лидерство с точки зрения общей заблокированной стоимости (TVL), в то время как Harvest Finance, по-видимому, является наиболее недооцененным среди агрегаторов доходности. Между тем, Alpha Finance является наиболее переоцененной, основываясь на соотношении разбавленной капитализации к общей заблокированной стоимости (FDV/TVL).

Сопутствующие риски

Агрегаторы доходности подвержены высокому риску взломов из-за того, что они стремятся получить высокую доходность по более рискованным протоколам. Из четырех протоколов только Badger DAO еще не взламывали (по состоянию на апрель 2021 года).

Интеграция со страховыми протоколами все еще слаба, что может быть главным препятствием для дальнейшего роста общей стоимости заблокированных средств в секторе. С запуском большего количества протоколов страхования мы можем увидеть запуск застрахованного агрегатора доходности в будущем.

Агрегаторы доходности, заслуживающие упоминания



Pancake Bunny

Pancake Bunny – крупнейший агрегатор доходности в экосистеме Binance Smart Chain. Он предоставляет только фермы, основанные на PancakeSwap. Низкая плата за газ в Binance Smart Chain позволяет использовать более частую стратегию повторного вложения, тем самым повышая доходность и приводя к повышению % годовых. Предлагаемые фермы стабильно обеспечивают доход, превышающий 100%.



AutoFarm

Auto Farm – это кроссплатформенный агрегатор доходности, поддерживающий Binance Smart Chain и Huobi ECO Chain. Как и Pancake Bunny, AutoFarm предлагает более высокую частоту повторного вложения и, следовательно, более высокий APY для своих ферм. Это второй по величине агрегатор доходности в экосистеме Binance Smart Chain.

Вывод

Агрегаторы доходности выполняют ту же роль, что и активно управляемые фонды или хедж-фонды. Их работа состоит в том, чтобы находить лучшие инвестиционные возможности и получать от них доход.

В DeFi программы майнинга ликвидности породили специализированный способ получения прибыли. Поскольку совместимость продуктов DeFi используется все более творческими способами, мы прогнозируем, что стратегии, используемые агрегаторами доходности, будут усложняться.

Большинство программ по выращиванию урожая действуют всего три-четыре месяца и могут быть изменены в любое время руководством. Агрегаторы урожайности помогают пользователям находить высокоурожайные фермы, но новые фермы обычно имеют повышенный риск взлома. Сложно сбалансировать поиск высокой доходности с рисками.

Существует также опасение, что высокая доходность, предлагаемая агрегаторами доходности, может оказаться неустойчивой. По состоянию на апрель 2021 года высокая доходность частично поддерживается спекулятивной рыночной конъюнктурой. Например, высокая цена токена CRV приводит к высокодоходным вознаграждениям за фарминг. Никто точно не знает, как может вести себя доходность на медвежьем рынке, но есть высокая вероятность снижения ее до нуля. Это плохо скажется на агрегаторах доходности.

Рекомендуемая литература

1. Предложения по улучшению Yearn (YIP 56) – байбэк и укрепление
<https://gov.yearn.finance/t/yip-56-buyback-and-build/8929>
2. Предложения по улучшению Yearn (YIP 61): Управление 2.0
<https://gov.yearn.finance/t/yip-61-governance-2-0/10460>
3. Предстоящий перезапуск Alpha Homora V2! Что изменилось?
<https://blog.alphafinance.io/upcoming-alpha-homora-v2-relaunch-what-is-included/>

ЧАСТЬ ЧЕТВЕРТАЯ: ТЕХНОЛОГИИ, ОПРЕДЕЛЯЮЩИЕ DEFI

ГЛАВА 13: ОРАКУЛЫ И АГРЕГАТОРЫ ДАННЫХ

DeFi работает на основе смарт-контрактов. Иногда входные данные, необходимые для получения выходных данных, состоят из реальных данных, не хранящихся в блокчейне, таких как погодные условия или информация о дорожном движении. Существует необходимость в протоколах для преодоления этого разрыва путем передачи данных в блокчейн в смарт-контракты.

Информация вне блокчейна является неотъемлемой частью DeFi и всегда должна быть достоверной и точной. Наличие ложных данных полностью искажает представление конкретного проекта и создает серьезные проблемы для DeFi. Однако, как мы можем гарантировать, что предоставленные данные всегда точны и им можно доверять?

Некоторые протоколы направлены на достижение этой цели путем передачи и трансляции данных в блокчейн без манипуляций или вмешательства. Обычно это делается с помощью механизма голосования или консенсуса, когда проверяющие соглашаются с наиболее точными данными. Без оракулов или агрегаторов данных в качестве основного «источника истины» нехорошие люди могут использовать ложную информацию, чтобы воспользоваться преимуществами ничего не подозревающих пользователей.

В этой главе мы подробнее рассмотрим некоторые из доступных оракулов и агрегаторов данных, таких как Chainlink, Band Protocol, Graph Protocol и Covalent. Мы рассмотрим, как эти оракулы и агрегаторы данных преодолевают разрыв между блокчейнами и реальными данными.

Протоколы оракулов

Оракулы действуют в качестве моста между данными вне блокчейна и блокчейном или между протоколами, которые не имеют внутренних каналов данных для ссылки на данные внутри блокчейна. Эти оракулы проверяют и передают внешнюю информацию в блокчейн для выполнения с помощью её смарт-контрактов или приложений в экосистеме DeFi.

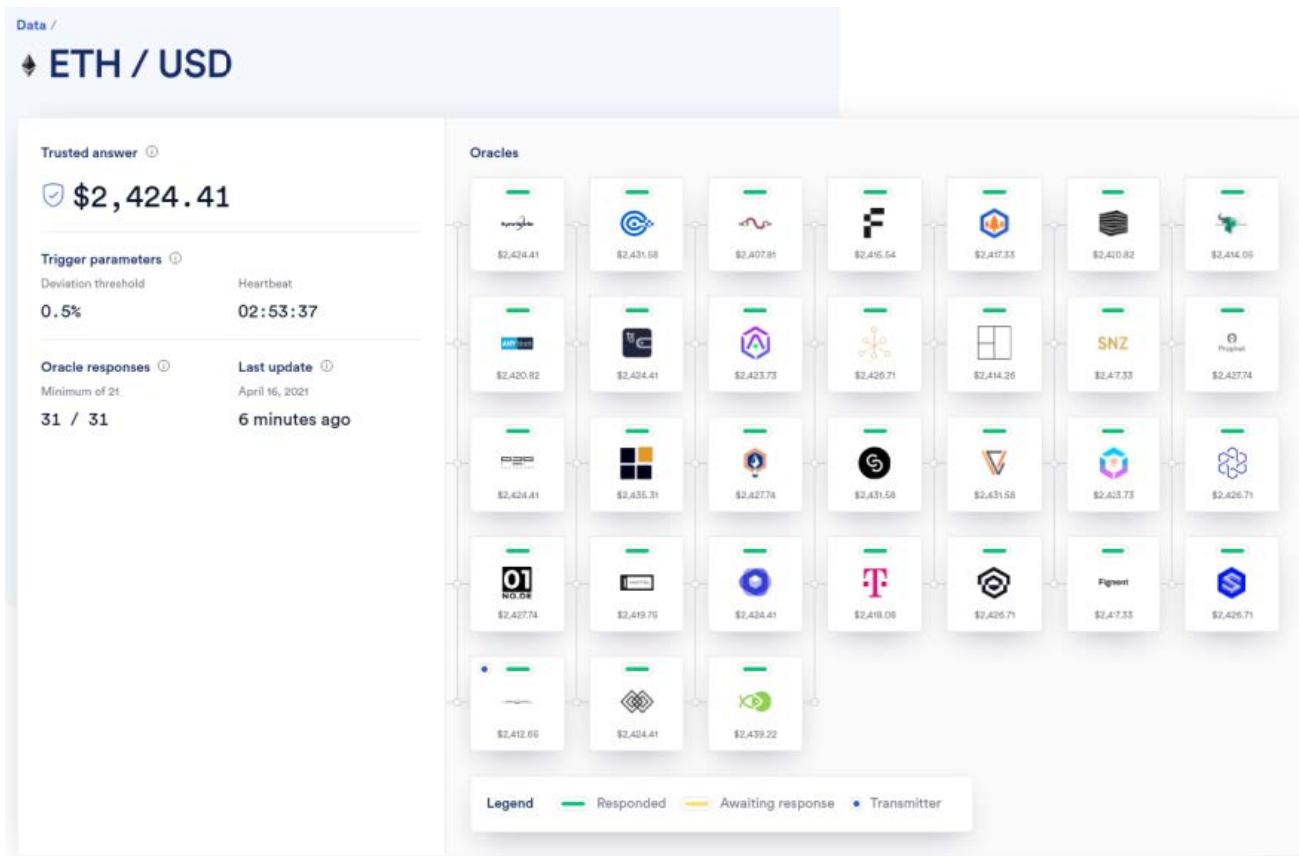
Chainlink



Chainlink – это платформа и инфраструктура для создания децентрализованных сетей оракулов, которые соединяют безопасно смарт-контракты в любом блокчейне с внешними ресурсами данных и автономными вычислениями. Каждая сеть оракула защищена независимыми и устойчивыми к Атакам Сивиллы операторами узлов (вид атаки, в результате которой пользователь подключается только к узлам, контролируемым злоумышленником), которые получают данные от множества сторонних провайдеров данных, объединяют информацию в единое значение и передают в блокчейн для исполнения с помощью ее смарт-контрактов.

Одной из основных функций Chainlink является предоставление наиболее точных цен на активы через каналы цен, которые могут быть интегрированы в протоколы блокчейна для конкретного использования. Например, цены на активы очень важны при расчете опционов и фьючерсных контрактов по истечении срока погашения и когда активы используются в качестве обеспечения по кредитам. Услуги Chainlink также включают в себя справку «подтверждения резервирования» для токенов с другого блокчейна и «проверяемую случайную функцию» для игр на блокчейне.

Чтобы глубже погрузиться в то, как Chainlink взаимодействует с данными и обрабатывает их, рассмотрим некоторые методы, используемые оракулами Chainlink для передачи реальных данных в блокчейн.



Наиболее распространенным методом, который оракулы Chainlink используют для передачи внешних данных в блокчейн, является Децентрализованная Модель Данных – постоянно обновляемый смарт-контракт в блокчейне, представляющий определенную часть данных (например, цену ETH против BTC), которые могут быть запрошены за одну транзакцию.



Базовая модель запроса и получения – это еще один метод, при котором пользовательский смарт-контракт запрашивает данные непосредственно у одного или нескольких узлов Chainlink, и сообщенное значение принимается в следующей транзакции. Эта модель используется для выборки случайных значений или более уникальных наборов данных. Узлы Chainlink оплачиваются токенами LINK за свои услуги в обеих этих сетевых моделях оракула.

Любой желающий может стать оператором узла Chainlink и начать предоставлять данные в сеть. Сети передачи стоимостей Chainlink защищены узлами, управляемыми несколькими традиционными предприятиями, такими как Deutsche Telekom's T-systems, поставщиками данных и профессиональными DevOps (development & operations) фирмами. Поставщики данных, которые управляют собственным узлом Chainlink, криптографически подписывают свои данные непосредственно у источника, предоставляя смарт-контракты с большими гарантиями безопасности.

В апреле 2021 года был выпущен технический документ Chainlink 2.0, в котором была представлена новая архитектура для децентрализованных сетей оракулов. Децентрализованные сети оракулов функционируют аналогично решениям уровня-2, значительно повышают скорость доставки данных и повышают безопасность. Кроме того, Chainlink представила свою суперлинейную модель стейкинга, механизм криптоэкономической безопасности, который стимулирует узлы предоставлять точные отчеты оракула и значительно усложняет возможность атаки для злоумышленников.

Это краткий обзор сетей Chainlink и децентрализованных сетей оракулов! Возможно, вы заметили, что некоторые из лучших протоколов DeFi, представленных в этой книге, такие как Synthetix и Aave, также работают с Chainlink.

Band Protocol



Подобно Chainlink, Band Protocol представляет собой кросчейн платформу оракулов, которая соединяет смарт-контракты с внешними данными и API. Децентрализованные приложения, интегрированные с Band Protocol, получают данные от смарт-контрактов Band Protocol, а не напрямую от сторонних оракулов.

Уникальным аспектом Band Protocol является то, что они используют BandChain, отдельный блокчейн для обработки и передачи информации, который может обрабатывать тысячи транзакций. Данные могут быть отправлены в другие блокчейны по протоколу Cosmos Inter-Blockchain Communication (IBC).

Данные, полученные из Band Protocol, контролируются и проверяются сообществом, гарантуя, что они достаточно надежны, чтобы на них могли ссылаться как пользователи децентрализованных приложений, так и разработчики. Эти источники данных могут быть агрегированы из различных каналов и агрегаторов данных в блокчейне с использованием различных

статистических методов, таких как среднее значение, медиана или мода (это статистическая, а не высокая), а также любых дополнительных методов уточнения данных, таких как нормализация или средневзвешенное среднее по времени.

Для извлечения данных из Band Protocol, запрашивающему необходимо указать несколько параметров: идентификатор скрипта необходимого оракула, параметры скрипта оракула и необходимое количество валидаторов. Как только запрос будет сделан и проверен в BandChain, скрипт оракула начнет первый этап выполнения, именуемый как фаза подготовки, путем предоставления источников данных, необходимых для выполнения запроса.

Валидаторы будут выбраны для обработки запроса на основе рандомизированного алгоритма, зависящего от веса стейка валидатора. Валидаторы попытаются получить запрошенные данные из всех указанных источников и отправят результаты с чистыми данными в BandChain для подтверждения.

Как только минимальное количество валидаторов успешно представят свои отчеты, BandChain перейдет ко второму этапу, именуемому как фаза агрегирования. Все собранные отчеты собираются в единый результат, хранящийся в BandChain, к которому можно получить доступ и отправить в другие BandChain для дальнейшего использования.



Сеть BandChain опирается на множество участников, наиболее важными из которых являются валидаторы и делегаты. Топ-100 валидаторов с наибольшим количеством застейканных токенов BAND отвечают за создание и подтверждение новых блоков в сети BandChain. С другой стороны, делегаты могут делегировать свои токены BAND любым валидаторам для получения вознаграждений за блок.

По запросу валидаторы в BandChain обязаны получать данные от указанных поставщиков данных. Валидаторы экономически заинтересованы в предоставлении точных данных, поскольку предоставление ложных данных приведет к урезанию или конфискации застейканных токенов BAND. Предоставление ложных данных также приведет к снижению показателей доверия и количества пользователей, что еще больше снизит стоимость застейканных токенов и усугубит убытки валидатора.

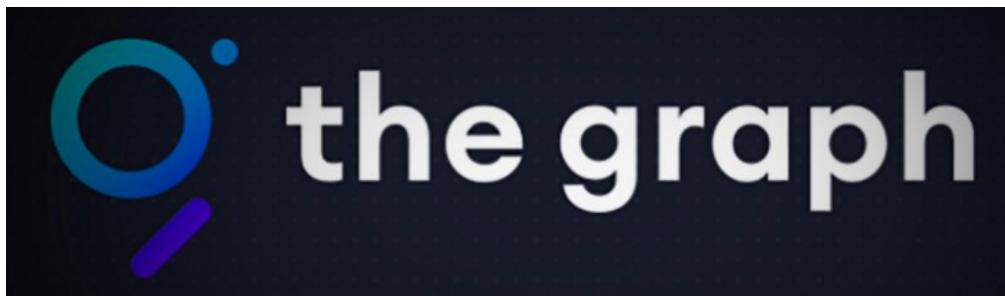
Кроме того, процесс запроса данных, выполняемый валидатором является общедоступным для всех, что еще больше снижает риск передачи ложных или сфальсифицированных данных. Валидаторы обслужили около 4,3 миллиона запросов данных за первые шесть месяцев с тех пор, как функция оракула заработала в основной сети BandChain в октябре 2020 года.

Чтобы стать валидатором в BandChain, вам нужно будет владеть определенным количеством токенов BAND или попросить других пользователей делегировать вам токены BAND. Валидаторы выбираются случайным образом с использованием взвешенного по стейку алгоритма, основанного на их доле токенов в стейке. Чем больше доля, тем выше шансы быть выбранным.

Агрегаторы данных

Если оракулы связывают реальные данные с блокчейном, то агрегаторы данных помогают пользователям их читать. Эти протоколы собирают данные блокчейна в упрощенный формат, облегчая проектам и отдельным пользователям создание своей аналитической панели.

Graph Protocol

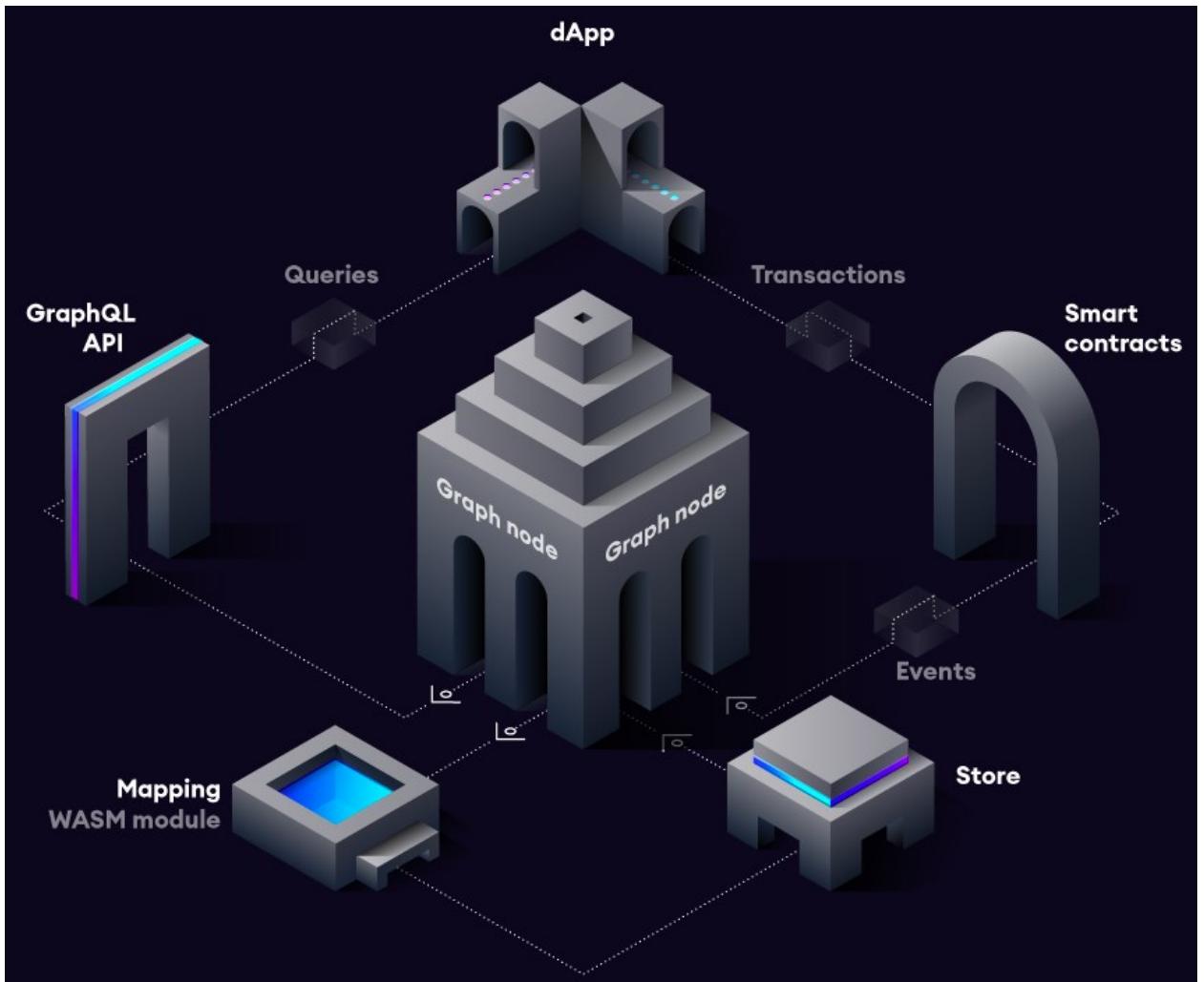


Graph представляет собой децентрализованный протокол для запроса и получения данных из блокчейнов, таких как Ethereum, Polkadot и Solana. Хотя довольно просто отвечать на запросы, полученные непосредственно путем считывания адреса контракта в блокчейне, гораздо сложнее найти специфические данные с более высокой детализацией. Graph решает эту проблему путем индексирования данных блокчейна в «подграфы» или открытые API, которые можно запрашивать с помощью стандартного API GraphQL.

Graph работает с помощью сильно индексированных различных типов данных на основе описания подграфа, также именуемого как манифест подграфа. Манифести определяют соответствующие смарт-контракты и ключевые события контракта, на которых следует сосредоточиться. Он также определяет, как сопоставить данные о событиях с данными, хранящимися в базе данных Graph.

Как только манифест подграфа создан, интерфейс Graph сохраняет его в файловой системе InterPlanetary File System (IPFS), децентрализованном решении для хранения данных, и начинает индексировать информацию для этого подграфа.

Вот основной поток информации при поиске и хранении данных узлами Graph:



1. Децентрализованные приложения (Dapps) добавляют данные из транзакции смарт-контракта в блокчейн.
2. Смарт-контракт имеет новые события (Events) во время обработки транзакции.
3. Узлы Graph непрерывно сканируют блокчейн в поисках новых блоков и данных для манифестов подграфов.
4. Узлы Graph находят события и запускают предоставленные обработчики отображения. Модуль WASM генерирует и обновляет данные, хранящиеся в узлах.
5. Dapps запрашивает узлы графа для индексированных данных с помощью GraphQL.
6. Запросы GraphQL преобразуются узлами в удобное для пользователя представление до того, как они будут получены DApp.

7. DApp отображает эти данные через свой пользовательский интерфейс, чтобы использовать их в качестве основания при выдаче новых транзакций в блокчейне.

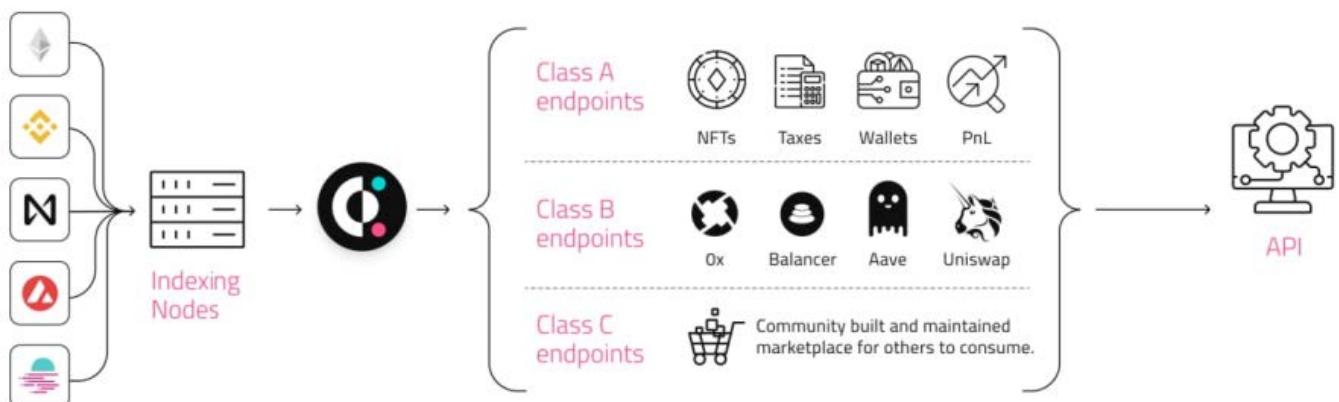
Graph используется многими децентрализованными приложениями в пространстве DeFi и Web3, включая Uniswap, Aave, Balancer и Synthetic. Он обеспечивает надлежащую инфраструктуру для обслуживания протоколов с интенсивным использованием данных. По состоянию на 1 квартал 2021 года около 16 000 разработчиков развернули более 10 000 подграфов и обработали более 100 миллиардов запросов менее чем за год.

Covalent



Covalent – это поставщик данных блокчейна, который предоставляет единый API для доступа к, казалось бы, бесконечным рядам данных в блокчейне. Подробную информацию о балансах токенов и активности кошельков из различных блокчейнов можно получить с помощью единого API, что значительно облегчает разработчикам создание аналитических панелей или сбор информации о деятельности блокчейна.

Функции Covalent могут показаться довольно похожими на Graph, но он отличается некоторыми моментами. Например, для Graph требуется, чтобы подмножество данных было преобразовано в подграф, прежде чем его можно будет запросить. А Covalent будет индексировать блокчейн полностью, что приведет к увеличению объема детализированных данных для пользователей. Кроме того, Covalent вышел за рамки Ethereum. По состоянию на апрель 2021 года Covalent поддерживает данные из четырех других блокчейнов, в том числе Fantom, Binance Smart Chain, Polygon и Avalanche.



Чтобы получить доступ к API Covalent, вам сначала нужно будет получить бесплатный ключ API, создав учетную запись на Covalent. Существует два класса API Covalent – класс А и класс В.

Вы можете использовать точки выхода класса А для извлечения данных блокчейна, которые не зависят от сети. Короче говоря, это общие данные, которые применимы ко всем сетям, таким как балансы, транзакции и держатели токенов. С другой стороны, вы можете использовать точки выхода класса В для получения значений из протоколов на нужном вам блокчейне. Например, вы можете запросить данные у Uniswap или PancakeSwap, хотя обе децентрализованные биржи изолированы в соответствующих сетях.

Get token balances for address real-time

GET /v1/{chain_id}/address/{address}/balances_v2/

Return a list of all ERC20 and NFT token balances along with their current spot prices.

REQUEST

PATH PARAMETERS

- *`chain_id` string Chain ID of the Blockchain being queried. Currently supports `1` for Ethereum Mainnet, `137` for Polygon/Matic Mainnet, `80901` for Polygon/Native Mumbai Testnet, `56` for Binance Smart Chain, `43114` for Avalanche C-Chain Mainnet, `43113` for Fuji C-Chain Testnet, and `258` for Fantom Opera Mainnet.
- *`address` string Passing in an `EIP` resolves automatically.

QUERY-STRING PARAMETERS

- `nft` boolean Set to `true` to return ERC721 and ERC1155 assets. Defaults to `false`.
- `no-nft-fetch` boolean Set to `true` to skip fetching NFT metadata, which can result in faster responses. Defaults to `false` and only applies when `nft=true`.
- `format` string If `format=csv`, return a flat CSV instead of JSON responses.

TRY

Оракулы и агрегаторы данных, заслуживающие упоминания



DIA

DIA, сокращение от Децентрализованного Информационного Актива, представляет собой оракул с открытым исходным кодом, который предоставляет данные для многих приложений DeFi. Они предоставляют ценовые каналы для популярных DEX, таких как Uniswap и Sushiswap, в других сетях, таких как Binance Smart Chain и Polygon.



API3

API3 предоставляет информацию проектам через децентрализованные API или dAPI. Потоки данных контролируются DAO, в состав которого входят партнеры по проекту и отраслевые эксперты. Они также позволяют пользователям dAPI получать страховку в случае, если API не отработает должным образом.

Сопутствующие риски

Поскольку все больше протоколов начинают полагаться на давно зарекомендовавшие себя продукты, прошедшие испытания в самых суровых условиях, важно также помнить, что эти продукты могут быть не полностью надежными. Если бы произошли события черного лебедя, оракулы, возможно, не смогли бы эффективно предоставлять данные, что привело бы к принятию неточных решений.

В марте 2020 года, иначе известном как Черный Четверг, оракулы, такие как Chainlink и «Medianizer» MakerDAO, не смогли достаточно быстро обновить свои ценовые каналы, что привело к совершенно неверным ценам. Ценовой провал MakerDAO привел к цепочке катастрофических событий, в результате которых владельцы CDP потеряли залог ETH на сумму более 8 миллионов долларов.

Вывод

Оракулы и агрегаторы данных составляют основу многих протоколов DeFi. Необходимость в скорости и точности при запросе и передаче данных имеет первостепенное значение для будущих проектов, направленных на изменение процесса предоставления данных. В настоящее время Chainlink доминирует в пространстве с более чем 400 интеграциями, включая более 200 проектов DeFi.

Тем не менее, DeFi постоянно находится на острие инноваций, и на регулярной основе в действие вступают более совершенные механизмы оракулов и сбора данных. В конечном счете, цель DeFi состоит в том, чтобы иметь надежную, внутренне безопасную и хорошо защищенную от негативных внешних факторов службу оракулов. Кроме того, надежные протоколы индексирования, которые были созданы и постоянно совершенствуются, будут способствовать большей ясности и пониманию поведения пользователей в блокчейне, позволяя проектам предоставлять более качественные продукты и услуги с большим соответствием рынку продуктов.

Рекомендуемая литература

1. Документация и дополнительная информация по Chainlink

<https://docs.chain.link/docs>

2. Официальные документы Chainlink

<https://link.smartcontract.com/whitepaper>

3. Что такое Chainlink и почему он очень важен в криптоиндустрии?

<https://finance.yahoo.com/news/chainlink-why-important-world-cryptocurrency-110020729.html>

4. Документация по Band Protocol

<https://docs.bandchain.org/>

5. Что такое Band Protocol и как купить токен BAND

<https://decrypt.co/resources/what-is-band-protocol-defi-oracle>

6. Документация по The Graph Protocol

<https://thegraph.com/docs/>

7. The Graph - Google блокчейна?

<https://finematics.com/the-graph-explained/>

8. Документация по Covalent API

<https://www.covalenthq.com/docs/api/#overview>

9. Небольшой обзор о роли «Covalent API в блокчейне»

<https://newspi.site/heres-a-quick-look-at-the-role-of-covalent-blockchain-data-api-in-terms-of-data-gathering-e-hacking-news/>

10. Сообщение о запуске сети Covalent

<https://www.covalenthq.com/blog/covalent-network-blog/>

ГЛАВА 14: МУЛЬТИЧЕЙН ПРОТОКОЛЫ И КРОССЧЕЙН МОСТЫ

Ethereum, несомненно, является домом для многих проектов DeFi. Однако резкие скачки платы за газ из-за высокого уровня использования и увеличения цены эфира до рекордно высокого уровня послужили тревожным сигналом для пользователей и разработчиков изучить другие блокчейны с более низкими транзакционными сборами.

Многие проекты DeFi нашли второй дом в других блокчейн-сетях, чтобы обслуживать еще больше пользователей и более эффективно масштабироваться. Хотя биржи обычно предоставляют пользователям возможность легко переходить между различными блокчейнами, это все равно может ограничить движение средств.

Из-за этой дилеммы выросло несколько проектов, таких как Ren, THORChain и Anyswap, которые позволяют пользователям легко подключаться и перемещать средства между блокчейнами без необходимости доверия кому-либо. Централизованные биржи, такие как Binance, также попытались объединить Ethereum и другие блокчейны, введя Binance Bridge.

Обзоры протоколов и мостов

Ren Project



Ren Project – это протокол, с которым каждый может работать без необходимости получать какое-либо разрешение, который позволяет пользователям анонимно взаимодействовать и передавать токены между блокчейнами. Ren Project делает это через RenBridge, работающее на виртуальной машине Ren (RenVM).

RenBridge позволяет легко представлять криптовалюты одной сети в других сетях. Например, биткоин может быть представлен в сети Ethereum в виде токена ERC-20, если его завернуть в renBTC. Используя RenVM, активы преобразуются в соответствии с форматом сети назначения в соотношении 1:1, гарантируя, что завернутые версии всегда полностью поддерживаются базовым активом.

В то время как вы используете в других блокчейнах новые обернутые токены, RenVM действует как децентрализованный хранитель ваших первоначальных активов, при этом стоимость связанного REN поддерживается в три раза выше общей стоимости заблокированных активов путем их формирования и сжигания. Узлы Darknodes постоянно перетасовываются для обеспечения бесперебойной работы RenVM, а дополнительные уровни безопасности, такие как реализация алгоритма RPZ MPC и алгоритмически скорректированные комиссии, делают атаку хакеров чрезвычайно сложной задачей. В маловероятном случае, если произойдет атака, RenVM может восстановить украденные средства.

RenVM работает в децентрализованной сети компьютеров, известной как Darknodes, которые помогают проверять транзакции и поддерживать безопасность сети Ren. Чтобы управлять Darknode, пользователям необходимо застелить 100 000 токенов REN в качестве залога, что составляет примерно 103 000 долларов США (7 мая 2021 года).

Darknodes собирают часть торговых комиссий с транзакций RenVM в виде завернутых активов.

Виртуальная машина Ren поддерживает три типа транзакций между цепочками:

- блокировка и формирование актива
- сжигание и высвобождение актива
- сжигание и формирование актива

Блокировка и формирование актива

Блокировка и формирование актива происходит, когда пользователь отправляет средства из исходной сети в сеть назначения. Токены, отправленные в RenVM, становятся «заблокированными». Как только будет подтверждено, что активы заблокированы, RenVM предоставит пользователю подпись формирования актива, которая позволит пользователю создать токенизированную версию актива 1:1 в сети назначения. Сформированные активы могут быть погашены в любое время в любом количестве.

Сжигание и высвобождение актива

В дополнение к первой транзакции функция сжигания и высвобождения актива позволяет пользователям отправлять свои токены из блокчейна назначения обратно в исходную сеть, записывая токенизированную версию актива в сети назначения и получая заблокированные активы по выбранному адресу. Как следует из названия, привязанные токены «сжигаются», в то время как RenVM «высвобождает» равное количество базового актива в исходной сети блокчейна.

Сжигание и формирование актива

Сжигание и формирование актива объединяет обе вышеуказанные транзакции. Пользователи могут напрямую перемещать свои активы между основными блокчейнами, сжигая привязанные активы из одной сети и формируя такое же количество привязанных активов в другой основной сети. Однако для этого потребуется несколько платежей и подтверждений через RenVM, что делает этот процесс медленным и дорогостоящим.

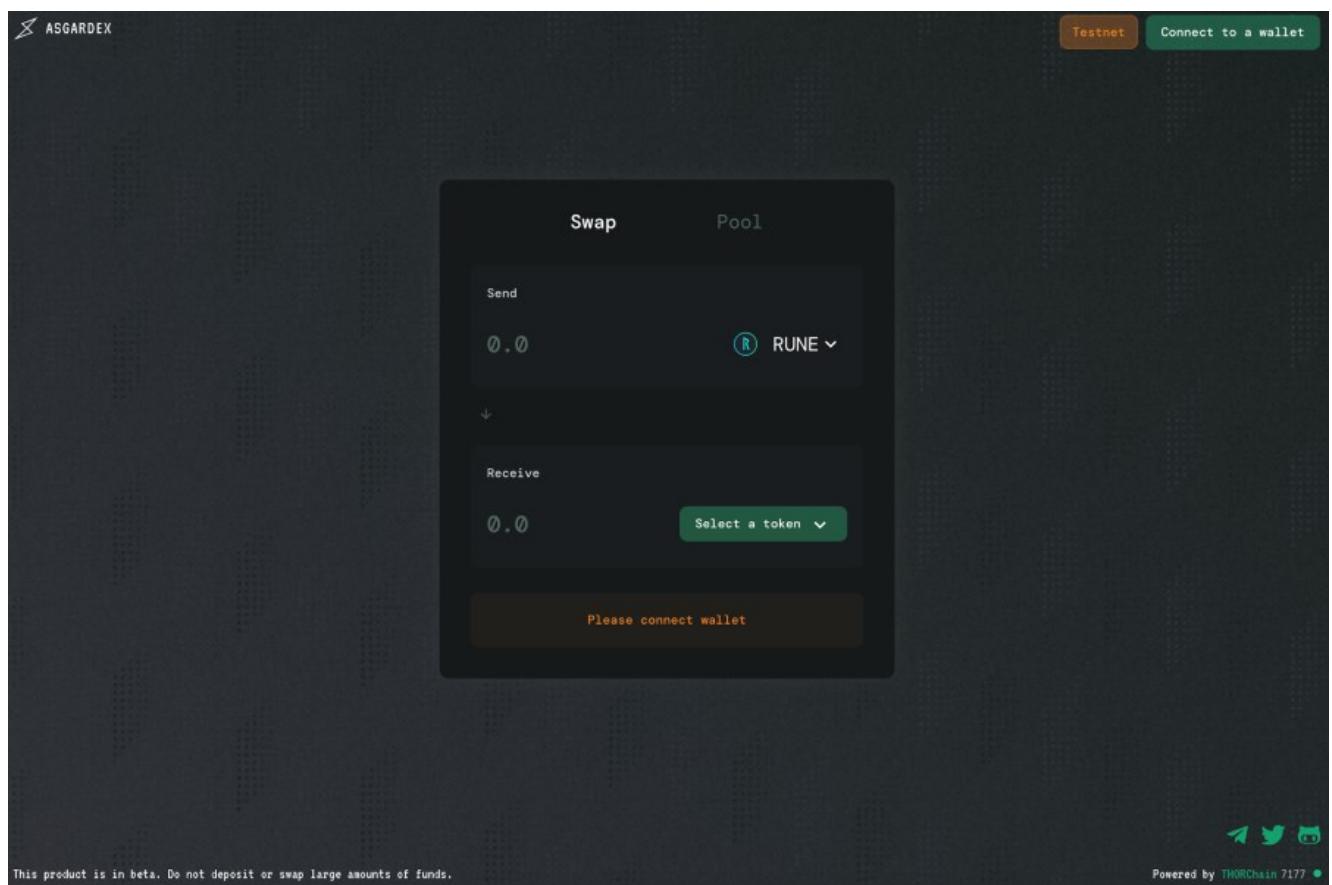
ThorChain



ThorChain – это децентрализованная сеть ликвидности с совместимым блокчейном, который позволяет осуществлять обмен токенами между блокчейнами без блокировки и доступа к вашим активам. Она не привязывает и не переносит активы, но позволяет пользователям обмениваться токенами между различными блокчейнами уровня 1. Например, трейдеры на ThorChain могут легко перемещать свои активы из биткоина в Эфириум без регистрации или прохождения процесса KYC централизованной биржи.

Привлекательность ThorChain заключается в том, что его функция, не зависящая от конкретного блокчейна, позволяет ему обмениваться активами без какого-либо преобразования. В отличие от Ren, где завернутый биткоин (renBTC) выпускается в пропорции 1:1 для дальнейших действий. Вместо этого с помощью Thorchain можно обменивать ETH на реальный биткоин. Это важная веха, так как ранее самое близкое представление биткоина в DeFi было в качестве завернутого токена. Таким образом, ThorChain значительно приближает биткоин к основам экосистемы DeFi.

Кроме того, по мере роста числа новых платформ смарт-контрактов, таких как Solana и Polkadot, разнообразие проектов и протоколов, существующих в этих блокчейнах, продолжит расширяться экспоненциально. Разнообразие блокчейнов вызывает необходимость в минимизации доверия и децентрализованном способе обмена токенами между различными блокчейнами.



ThorChain использует механизм Proof-of-Stake. Он построен на Tendermint, где требуются валидаторы или узлы для привязки собственного токена RUNE. RUNE представляет собой модель токена, ценность которого возрастает по мере роста использования сети. Это означает, что по мере того, как в пулы ликвидности ThorChain будет вкладываться больше ликвидности, RUNE станет более дорогим.

RUNE нужна по двум фундаментальным причинам:

- I. В пулах ликвидности RUNE действует как базовая пара, где для размещения вкладов требуется в соотношении 1:1 АКТИВ:RUNE (например, BNB-RUNE или ETH-RUNE). ThorChain не работает путем прямой передачи активов; вместо этого ему нужна RUNE для перехода от одного актива к другому. RUNE также необходима для активации протокола Bifrost ThorChain, который действует как мост, обеспечивающий мультичейн подключение. Протокол также отслеживает соотношение RUNE к активам в их общих пулах ликвидности (CLP – Continuous Liquidity Pools), означающее, что они также наследуют надежное значение стоимости для цифровых активов, не полагаясь на сторонние оракулы.
- II. RUNE используется в качестве залога операторами узлов, чтобы снизить интерес к атакам злоумышленниками, следя соотношению залога и использования 2:1. RUNE не предназначена для управления. ThorChain управляет аналогично биткоину, где операторы узлов могут определять его будущее направление. Это также означает, что ThorChain не ограничивается только трейдерами, но также используется провайдерами ликвидности и операторами узлов.

При соотношении залога и использования 2:1 в сочетании с соотношением долей пула ликвидности 1:1 необходимое количество RUNE будет в три раза превышать количество заблокированных активов. Другими словами, это соотношение 3:1 представляет собой внутреннее или минимальное количество токенов RUNE, необходимых для работы протокола.

Пользователи, которые используют кроссчейн сервисы ThorChain для переноса активов между пулами, должны будут платить фиксированную сетевую комиссию и переменную комиссию за проскальзывание, чтобы покрыть плату за газ внешних сервисов и быстрое исполнение. Помимо предоставления услуг трейдерам, пользователи также могут стать провайдерами ликвидности на ThorChain.

Провайдеры ликвидности на ThorChain могут добавлять ликвидность в различные пулы, которые привязаны к RUNE в отдельном хранилище. Пулы ликвидности стимулируют любого участника ThorChain предоставлять ликвидность в обмен на вознаграждение RUNE, равное удвоенному количеству используемого газа.

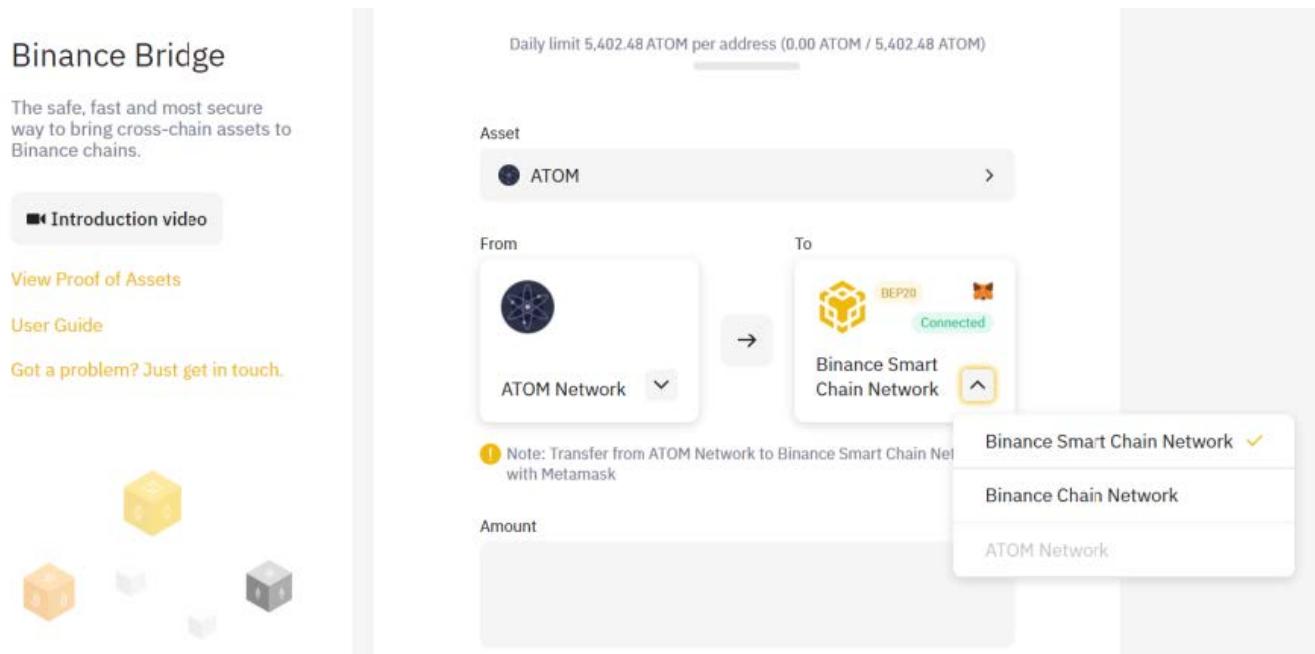
Как указано на веб-сайте ThorChain, «ликвидность обеспечивается вложениями, которые получают комиссионные за обмены, превращая свои непродуктивные активы в продуктивные, способом, не связанным с блокированием и потерей доступа к средствам. Рыночные цены поддерживаются за счет соотношения активов в пуле, которое трейдеры могут использовать в арбитраже для восстановления правильных рыночных цен».

Что отличает ThorChain, так это его функция кросчейна – она позволяет пользователям обменивать любой актив и создавать для него пул ликвидности, открывая совершенно новый мир возможностей для экосистемы DeFi.

По состоянию на 13 апреля 2021 года работает мультичейн сеть Chaosnet от ThorChain, а также их децентрализованная биржа Asgardex. Пользователи могут совершать транзакции в пяти активных блокчейнах – Bitcoin, Bitcoin Cash, Litecoin, Ethereum и Binance Chain.

Binance Bridge

Используя Binance Bridge, пользователи могут переводить средства в различные блокчейны, такие как Ethereum, Tron и Binance Smart Chain (BSC). Для каждого конкретного актива поддерживаются только определенные блокчейны. Например, собственные токены для других блокчейнов, таких как Cosmos (ATOM) и Ontology (ONT), ограничены передачей между Binance Smart Chain, Binance Chain или их собственной сетью. Существует ежедневный лимит на сумму, которую вы можете перевести для каждого актива.



Если вы перемещаете активы в сеть Binance Smart Chain, вы также можете обменять их на некоторое количество Binance Coin (BNB). Аналогично тому, как ETH используется для оплаты комиссий за транзакции в сети Ethereum, BNB используется для оплаты комиссий за транзакции в сети Binance Smart Chain. Таким образом, желательно обменять некоторое количество активов на BNB, особенно если вы новичок в Binance Smart Chain.

Amount

10

I want to swap some BNB gas in this order
Please select the amount of swapping BNB

0.5 BNB 1 BNB 2 BNB

You will receive ≈ ⚡ 9.83857302 ETH BEP20 + 1 BNB
The final price will depend on the market condition at the time of execution.

Anyswap

Anyswap – это децентрализованная кросчейн биржа, которая поддерживает восемь различных блокчейнов, таких как Ethereum, Binance Smart Chain и Fantom. Она предлагает универсальную платформу для пользователей, позволяющую обменивать или конвертировать свои активы в другие блокчейны. Пользователи могут выбрать обычный метод депонирования своих активов для создания обернутых токенов или напрямую выполнить кросчейн обмен, чтобы обменять свои токены на другой токен в другом блокчейне.

The screenshot shows the Anyswap dashboard. On the left, there's a sidebar with icons for Swap, Pool, Bridge, Farms, Markets, Governance, Network, and Documents. The 'Swap' icon is highlighted. The main area is titled 'Dashboard' and contains a 'My Balance' section. It lists three tokens: BNB (Binance-Peg Binance), ANY (Anyswap-BEP20), and CYC (CyCoin). Each token entry includes its logo, name, price, balance, liquidity, total balance, and a 'Swap' button. A search bar at the top right allows users to search by token name, symbol, or address. At the bottom of the balance table, there's a 'Show More' button.

Для каждого блокчейна биржа Anyswap поддерживает различные пары токенов, которые, начиная с версии 1, всегда спарены с базовым токеном сети. Например, в сети Fantom токены соединяются с токеном FTM.

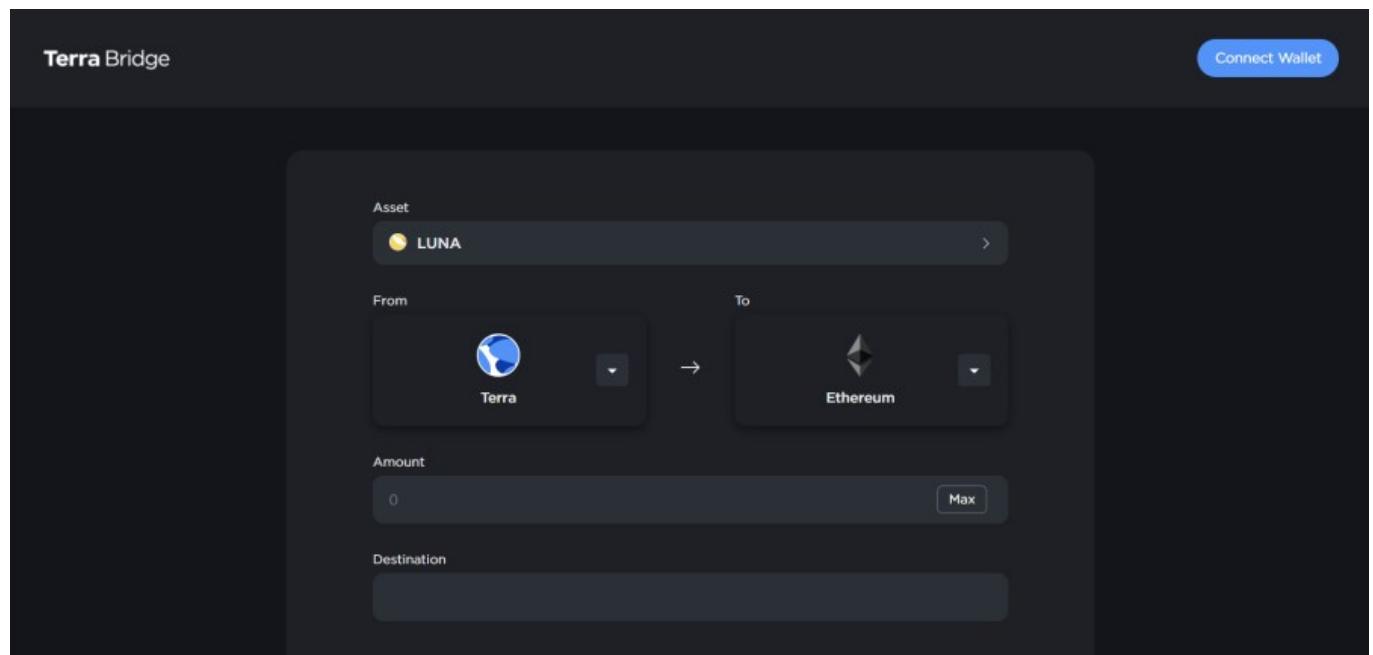
Сборы, взимаемые за использование биржи, варьируются в зависимости от количества используемого газа и типа активов, используемых при обмене. По сути, пользователи платят комиссию за обмен 0,4% в дополнение к комиссии за

транзакции в сети. 75% сборов идет провайдерам ликвидности, а остальная часть отправляется в Anyswap. С пользователей, которые совершают транзакцию между любыми двумя неродными активами, дважды взимается комиссия в размере 0,4%.

Популярность Anyswap возросла с тех пор, как Андре Кронье поделился своими интересами и восхищением проектом кроссчейна. С общей стоимостью заблокированных средств (TVL) более 620 миллионов долларов в поддерживаемых биржей блокчейнах (по состоянию на май 2021 года), у протокола все еще есть много возможностей для роста, поскольку все больше пользователей готовы использовать и исследовать другие сети. Вдохновленный Anyswap, Андре Кронье также выпустил multichain.xyz, свой кроссчейн протокол, который работает аналогично с индивидуальными парами для каждой сети.

Terra Bridge

Terra Bridge – это приложение для пользователей, позволяющее отправлять поддерживаемые активы Terra в блокчейне Terra между сетями Ethereum и Binance Smart Chain. Среди этих активов- LUNA (собственный токен Terra), стейблкоины Terra, такие как UST (Terra USD), и зеркальные активы, такие как mTSLA (Tesla) и mAAPL (Apple Inc.).



Мультичейн и кросчейн платформы, заслуживающие упоминания



Multichain.xyz

Поддерживая 10 различных блокчейнов, Multichain.xyz позволяет вам обмениваться различными активами, такими как BNB, ETH и USDC. По состоянию на 24 мая 2021 года его общая заблокированная стоимость составляет более 200 миллионов долларов и поддерживает более 280 токенов.



Matic Bridge

Matic Web Wallet Bridge позволяет пользователям переводить средства в сеть Polygon и из нее с помощью моста Plasma или моста Proof-of-Stake (PoS). В зависимости от используемого моста могут быть переданы только определенные активы. При этом, время вывода средств может быть различным.



APYSwap

APYSwap - это децентрализованный протокол для обмена активами между различными блокчейнами с уникальной функцией - он также работает для блокчейнов, не совместимых с EVM, позволяя пользователям переводить средства между Ethereum, Binance Smart Chain и Huobi ECO Chain в Solana и обратно.

Сопутствующие риски

Хотя мосты и кросчейн протоколы становятся жизненно важным шагом в улучшении связи между различными сетями, пользователи также должны знать о существующих проблемах, которые могут возникнуть при взаимодействии с этими протоколами.

Помимо неотъемлемых рисков, связанных с природой смарт-контрактов и их подверженностью ошибочному коду и экспloitам, пользователи должны убедиться, что их исходные активы действительно заблокированы в исходной сети, прежде чем формировать связанные активы в других блокчейнах. Если бы исходные токены можно было свободно разблокировать и использовать другими, сформированные активы станут бесполезными, так как они не могут быть использованы для возврата в исходную сеть.

Пользователи также должны быть осведомлены о различных смарт-контрактах токенов для разных сетей. Хотя большинство токенов имеют один и тот же адрес контракта в нескольких блокчейнах, все равно важно проверить, действительно ли вы получаете одну и ту же версию токена или некий эквивалент, когда пытаетесь выполнить переводы или кросчейн депозиты.

Вывод

По мере того, как альтернативные сети начинают приобретать все большее и большее значение, мосты и мультичейн протоколы становятся более важными, чем когда-либо прежде. Будь то через прокси-токены или обмен между собственными токенами, очевидно, что все больше пользователей будут продолжать экспериментировать и переходить в блокчейны, которые могут предлагать различные услуги или меньшую комиссию. Таким образом, повышение безопасности и удобства использования этих протоколов имеет решающее значение для того, чтобы DeFi действительно был доступен для всех в каждой сети.

Рекомендуемая литература

1. Обзор Ren Protocol

<https://defirate.com/ren-protocol/>

2. Углубленное пособие по пулам ликвидности в Thorchain.

<https://medium.com/thorchain/an-in-depth-guide-to-thorchains-liquidity-pools-c4ea7829e1bf>

3. Документация по Binance Bridge v2

<https://docs.binance.org/smart-chain/guides/bridge-v2.html>

4. Руководство пользователя по бирже Anyswap

<https://anyswap-faq.readthedocs.io/en/latest/>

5. Руководство пользователя по переводам в Terra's Shuttle Bridge

<https://docs.anchorprotocol.com/user-guide/interchain-transfers>

6. Руководство по использованию Matic Bridge в Matic Network

<https://blog.matic.network/deposits-and-withdrawals-on-pos-bridge/>

7. Как добавить сеть в браузер, используя Chainlist.org

<https://metamask.zendesk.com/hc/en-us/articles/360058992772-Add-Network-Custom-RPC-using-Chainlist-in-the-browser-extension>

ГЛАВА 15: ВЗЛОМЫ DEFI

Использование DeFi рискованно; взломы смарт-контрактов происходят постоянно. Только в 2020 году было совершено по меньшей мере 12 громких взломов DeFi, в результате которых из протоколов DeFi было выведено не менее 121 миллиона долларов средств.



Никто - даже лучшие аудиторы смарт-контрактов - не могут полностью предсказать, что произойдет с работающими смарт-контрактами. Имея миллиарды долларов средств, вложенных в смарт-контракты, вы можете быть уверены, что самые блестящие хакеры постоянно стремятся использовать слабые места в системе безопасности и извлечь из них выгоду.

Большой риск для DeFi заключается в том, что по мере того, как проекты используют совместимость проектов DeFi и строятся друг на друге, сложность приложений DeFi возрастает экспоненциально, что затрудняет выявление слабых мест аудиторами смарт-контрактов. Разработчики приложений должны обеспечить, чтобы аудиторы кибербезопасности постоянно проверяли их коды, чтобы уменьшить любую возможность эксплойтов, поскольку последствия ошибок приведут к огромным финансовым потерям.

В этой главе мы рассмотрим причины взломов, флэш-займы, потенциальные решения для снижения потерь от взломов и некоторые советы для частных лиц, чтобы избежать потери средств в результате эксплойтов DeFi.

Причины взломов

Ниже мы рассмотрим некоторые распространенные причины взломов. Этот список безусловно не может быть исчерпывающим.

1. Экономические взломы/флэш-займы

Флэш-займы позволяют пользователям использовать практически неограниченный капитал для осуществления финансовой транзакции до тех пор, пока заемщик погашает кредит в рамках одной и той же транзакции. Это мощный инструмент, позволяющий выполнять экономические атаки, требующие ранее много капитала. В случае с флэш-займами наличие правильной стратегии является единственным требованием для использования эксплойтов.

Почти все взломы DeFi использовали флэш-займы. Мы рассмотрим это более подробно в следующем разделе.

2. Культура использования кода

Многие проекты DeFi, возглавляемые Андре Кронье, основателем Yearn Finance, следуют принципам тестирования кода непосредственно в производстве для ускорения темпов разработки продукта вместо того, чтобы максимизировать безопасность и выполнять предварительное тестирование. Проведение аудита каждого релиза значительно увеличит время, необходимое для вывода любых обновлений продукта на рынок.

Одним из главных конкурентных преимуществ DeFi является то, что разработчики могут выполнять итерации намного быстрее, расширяя границы финансовых инноваций. Однако не каждый проект может позволить себе проведение аудита, особенно когда проект еще не набрал оборотов. Несмотря на проведение многочисленных аудитов, хакерам все еще удается взламывать некоторые проекты, предполагая, что проведения аудитов может быть недостаточно для предотвращения всех взломов.

3. Небрежное кодирование и недостаточный аудит

На бычьем рынке многие проектные команды чувствуют необходимость действовать быстро и использовать короткие пути, чтобы быстрее выпускать свои продукты. Некоторые могут решить вообще пропустить аудит, чтобы получить преимущество первопроходца, и проводить аудит только через несколько месяцев после запуска продуктов.

Существует также множество «форков» – новых проектов, которые используют тот же код, что и другие устоявшиеся проекты. Запущенные без полного понимания того, как работает код, создатели рассматривают их как быстрое получение денег, что приводит ко многим эксплойтам.

4. Выдергивание ковра (инсайдерская работа)

В пространстве DeFi нередко проекты запускаются анонимными командами. Некоторые делают это, чтобы избежать пристального внимания регулирующих органов из-за неопределенного нормативного климата. Однако другие предпочитали оставаться анонимными, поскольку у них плохие намерения. Было много случаев, когда анонимные команды проводили инсайдерскую работу и намеренно оставляли ошибку, которая использовалась для кражи у ничего не подозревающих пользователей.

Криптообщество не отчуждает проекты, запущенные анонимными основателями, видя, как первая криптовалюта, биткоин, также была основана неизвестным человеком. Пользователи оценивают проекты на основе созданного кода, а не того, кто или откуда разработчики. Это согласуется с принципами децентрализации открытого программного обеспечения.

Но если забыть об идеалах и принципах, то при эксплойте протокола, запущенного анонимной командой, шансы невозврата средств высоки, поскольку трудно определить личность разработчиков в реальном мире.

5. Атака оракула

Протоколы DeFi должны знать цены активов, чтобы правильно функционировать. Например, протокол кредитования должен знать цену актива, чтобы решить, следует ли ликвидировать позицию заемщика.

Поэтому, являясь неотъемлемой частью инфраструктуры DeFi, оракулы могут подвергаться серьезным манипуляциям. Например, в главе 12 мы упоминали, как эксплойт хранилища MakerDAO привел к ликвидации займов, которые не было необходимости ликвидировать, а убытки от этого действия составили более 8 миллионов долларов.

6. Атака на Metamask

Как основной интерфейс для каждого приложения Ethereum, неудивительно, что Metamask стал основной целью атаки. Команда ConsenSys тщательно следила за безопасностью, и на сегодняшний день не было никаких широко распространенных эксплойтов.

Тем не менее, было несколько громких атак:

- убыток в размере 59 миллионов долларов через учетную запись Metamask администратора проекта EasyFi.
- убытки в размере 8 миллионов долларов через личный кошелек основателя Nexus Mutual.

Флэш-займы

Что такое флэш-займы?

Флэш-займы – это займы, по которым пользователи могут занимать средства без какого-либо обеспечения, если пользователь возвращает заем в той же транзакции. Если пользователь не погасит флэш-заем в той же транзакции, транзакция автоматически завершится неудачей, что приведет к потере комиссии за транзакцию и гарантирует, что флэш-заем не будет выдан. Флэш-займы предлагаются различными протоколами DeFi, такими как Aave и dYdX.

Флэш-займы имеют три основные характеристики, которые выделяют их по сравнению с обычным кредитом:

- Отсутствие риска невозврата: Флэш-займы погашаются в рамках одной и той же транзакции. Поэтому нет никакого риска не получить возврат средств.
- Отсутствие залога: Заемщики могут взять кредит без предоставления какого-либо залога или проверки кредитоспособности, если они могут погасить кредит в течение одной транзакции.
- Неограниченный размер кредита: Пользователи могут занимать любую сумму вплоть до общей ликвидности, доступной по протоколам DeFi.

По состоянию на апрель 2021 года работа с флэш-займами не удобна для обычного пользователя, так как вы должны выполнить его, написав код смарт-контракта. Таким образом, он более доступен программистам, чем среднестатистическому обывателю.

Действительно, некоторые программисты часто используют этот фактор и запускают то, что мы называем «флэш-заем-атакой», особенно когда обеспечение не требуется. Одна из самых известных флэш-заем-атак произошла в Harvest Finance, в результате чего был нанесен ущерб в размере 24 миллионов долларов.

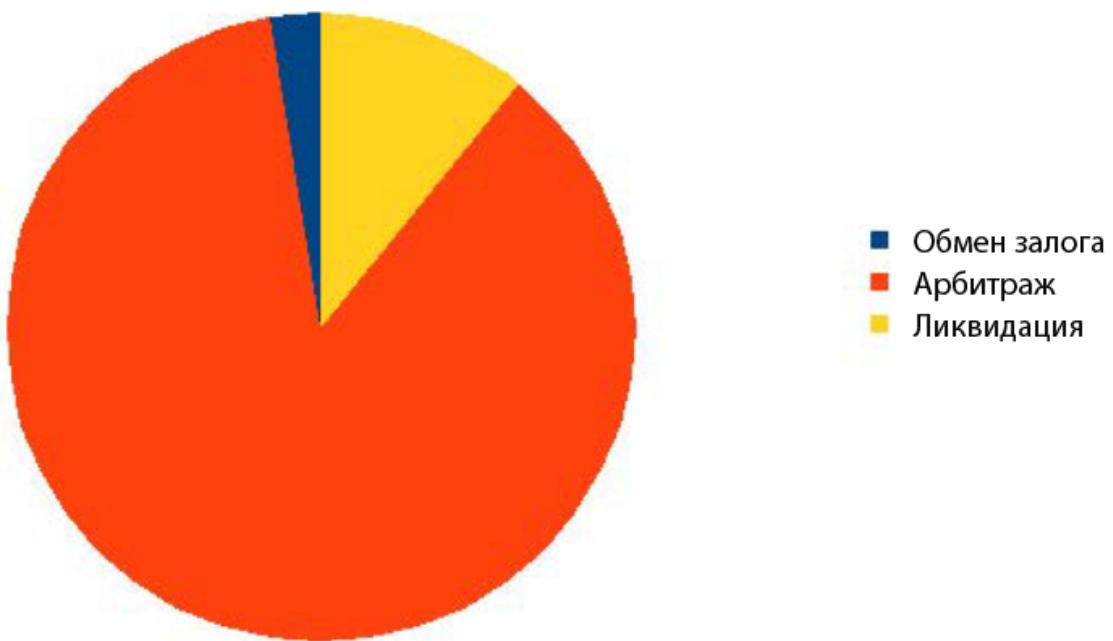
В таблице ниже показаны комиссии, которые вы заплатите по основным протоколам, предлагающим флэш-займы:

Протокол	Комиссия за флэш-заем
Aave	0,09 %
dYdY	1 Wei (10^{-18} ETH)
bZx	Бесплатно
Uniswap v2	0,3 %

Использование флэш-займа

На следующей диаграмме показана структура использования всех флэш-займов от Aave:

Использование флэш-кредитов



Мы видим, что флэш-займы в основном используются в арбитражных целях. Арбитраж – это акт использования разницы в ценах между рынками для получения прибыли. Например, предположим, что мы обнаружили значительную разницу в ценах на WBTC на двух разных децентрализованных биржах. Мы можем использовать флаш-заем для заимствования значительной суммы WBTC без какого-либо обеспечения, чтобы получить прибыль от разницы в цене.

Второе использование флаш-займов – это ликвидация кредитов. Обычно для заемщиков существует штраф, если они позволяют протоколу ликвидировать их позицию. Когда на рынке происходят существенные ценовые изменения, заемщики могут выбрать получение флаш-займов и самоликвидацию своих позиций, избегая штрафных санкций.

Давайте рассмотрим пример, когда мы занимаем DAI из протокола Maker с ETH в качестве залога. Когда цена ETH значительно упадет, она может приблизиться к уровню ликвидации нашего кредита DAI. У нас может не быть ETH для увеличения наших залогов или DAI для погашения кредита. Что мы можем сделать, так это взять флаш-заем DAI, чтобы погасить кредит в Maker. Затем мы можем обменять часть снятого обеспечения ETH на DAI, чтобы мгновенно погасить флаш-заем. Используя этот метод, мы сохраним оставшиеся ETH без уплаты штрафа за ликвидацию.

Наконец, флэш-займы также могут быть использованы для выполнения обмена залога. Например, если у нас есть кредит DAI в сочетании с ETH в качестве обеспечения, мы можем обменять обеспечение ETH на обеспечение WBTC, используя флэш-заем. Это позволяет нам легко изменять наши профили рисков без необходимости делать несколько транзакций.

Выполнение флэш-займов по-прежнему требует значительных технических знаний и имеет высокие барьеры для входа для тех, кто не знает, как писать код. Однако существует стороннее приложение, которое делает оформление флэш-займов доступным для обычных пользователей – эта платформа называется Furucombo.

Протокол флэш-займов: Furucombo

Furucombo – это платформа, которая позволяет любому создавать арбитражные стратегии с использованием флэш-займов. Благодаря инструменту drag-and-drop, который позволяет конечным пользователям создавать и настраивать различные комбинации DeFi, снижаются барьеры для входа при сборке MONEY-LEGO. Обратите внимание, что Furucombo не ищет для вас арбитражных возможностей.

Чтобы использовать Furucombo, пользователям необходимо настроить ввод/вывод и порядок транзакций, и он объединит все кубики в одну транзакцию для выполнения. Пример того, как может быть осуществлена арбитражная сделка, показан ниже:



1. Получите флэш-заем в размере 15 000 DAI от Aave.
2. Обменяйте DAI на yCRV, используя 1inch.
3. Обменяйте yCRV обратно на DAI, используя Curve. Из-за разницы в ценах между 1inch и Curve вы получаете 15 431 DAI.
4. Сумма займа в размере 15 013 DAI, включая плату за флэш-заем Aave, возвращается Aave. Пользователь остается с прибылью в размере 418 DAI. Все эти шаги выполняются в рамках одной транзакции.

Furucombo не требует никаких авансовых средств и не взимает плату с пользователей за создание «комбо» и совершение арбитражных сделок с использованием флаш-займов на платформе. Все что вам нужно – это деньги в вашем кошельке, чтобы оплатить газ.

Пользователям рекомендуется торговать на свой страх и риск, так как возможности арбитража не всегда доступны на Furucombo и комбинация может не сработать, если разница в цене больше не существует. Пользователи сталкиваются с риском оплаты комиссий за транзакции независимо от результата.

Тематическое исследование: Взлом флаш-займов bZx

15 февраля 2020 года состоялась транзакция на блокчейне Ethereum, которая в то время считалась уникальной. Прибыль в размере примерно 360 000 долларов была получена в рамках одного блока и одной транзакции меньше чем за минуту.

Эта транзакция привлекла внимание криптообщества и была подробно проанализирована. Прибыль был достигнута за счет первоначального почти безрискового займа в форме флаш-займа, за которым последовала серия арбитражных сделок между различными децентрализованными биржами.



1. Получение флэш-займа

Первое, у dYdX был взят флэш-заем в размере 10 000 ETH.

2. На хранение

Половина из этих ETH (5500 ETH) была заложена в качестве обеспечения в сочетании с займом 112 WBTC.

3. Накачка цены с плечом

1300 ETH депонируются в bZx, чтобы использовать ETH для получения WBTC с использованием 5x кредитного плеча. 5637 ETH, предоставленных в bZx, были использованы для обмена на 51 BTC с помощью KyberSwap. Согласно алгоритму KyberSwap, лучшая цена была предложена Uniswap. Однако из-за низкой ликвидности обмен повысил обменный курс 1 WBTC примерно до 109,8 WETH, что примерно втрое превышало нормальный курс конвертации в тот период.

4. Продажа

Злоумышленник продал заимствованные 112 WBTC в Uniswap после повышения цены, получив 6 871 ETH с коэффициентом конвертации 1 WBTC = 61,2 WETH.

5. Возврат флэш-займа

С неиспользованными 3200 ETH и полученными 6871 ETH от продажи злоумышленник вернул флэш-заем в размере 10 000 ETH с прибылью в размере 71 ETH.

Протокол	Количество	Актив	Тип операции
dYdX	-10,000	ETH/WETH	Кредит
Compound	+5,500	ETH/WETH	Обеспечение
Compound	-112	WBTC	Кредит
bZx	+1,300	ETH/WETH	Обеспечение
bZx	-5,637	ETH/WETH	Кредит
bZx	+51	WBTC	Обеспечение

Протокол	Количество	Актив	Тип операции
-	+3,200	ETH/WETH	Баланс
-	+6,871	ETH/WETH	Баланс

6. Конечная прибыль

Позиция в Compound все еще была прибыльной. Поскольку средняя рыночная цена 1 WBTC составляла 38,5 WETH, злоумышленник мог получить 112 WBTC примерно за 4300 ETH. В общей сложности злоумышленник получил

$$71 \text{ WETH} + 5500 \text{ WETH} - 4300 \text{ ETH} = 1271 \text{ ETH}$$

что примерно составляло 355 880 долларов США (в тот момент цена ETH составляла 280 долларов США).

Описанное выше событие не только демонстрирует возможность экстремального прироста капитала за счет манипулирования ценой других активов, но и то, что для заемщика не было никаких других затрат, кроме относительно низкой платы за протокол. Единственным условием, с которым столкнулся заемщик, было то, что кредит должен был быть погашен в рамках одной и той же транзакции. Таким образом, сама концепция необеспеченных кредитов открывает широкий спектр возможностей в криптовалютном пространстве.

Заключение по флэш-займам

Флэш-займы могут быть обоюдоострым мечом. С одной стороны, их использование в смарт-контрактах обеспечивает удобство и прогресс в экосистеме DeFi – трейдеры без большого капитала могут запускать стратегии арбитража и ликвидации с помощью флэш-займов без необходимости в большой базе капитала.

С другой стороны, хакеры могут использовать флэш-займы для запуска флэш-заем-атак, что значительно увеличивает их прибыль, поскольку залог не требуется. Как и любой инструмент, флэш-займы можно использовать как в хороших, так и в плохих целях.

На наш взгляд, атаки с использованием флэш-займов, используемые в недобрых целях, укрепили всю экосистему DeFi, поскольку проекты улучшают свою инфраструктуру, чтобы предотвратить будущие атаки. Поскольку флэш-займы все еще находятся на стадии зарождения, атаки можно рассматривать как положительный момент, который смягчает перегибы в экосистеме DeFi и делает ее более крепкой.

Решения

Одного аудита смарт-контрактов недостаточно для предотвращения эксплойтов. Проектам необходимо сделать больше, и сейчас они ищут альтернативы для обеспечения сохранности средств, внесенных в их протоколы. Ниже приведены некоторые из возможных решений:

Фонд внутреннего страхования

Несколько проектов решили использовать свой собственный токен в качестве защиты от рисков. Примеры включают:

- Maker напечатал токены MKR в Черный Четверг, чтобы покрыть нехватку средств для обеспечения DAI из-за быстрого падения курса.
- Aave развернула stAAVE, чтобы покрыть любую потенциальную нехватку средств для вкладчиков.
- YFI обеспечила залог своим токеном и одолжила DAI для возврата потерянных при взломе средств.

Страхование

Будучи одним из новичков в блокчейне, Unslashed Finance предлагал своим пользователям покрытия на уровне протоколов для LIDO и Paraswap. Это открывает возможность для протоколов покупать страховку для своих пользователей.

Вознаграждения за выявление ошибок

Проекты все чаще используют Immunefi для перечисления вознаграждений за нахождение ошибок, поощряя хакеров брать вознаграждения за обнаружение ошибок, а не за их использование. Самые высокие награды предлагают до 1,5 миллионов долларов. Однако, учитывая более высокие потенциальные выгоды от взлома, будет ли это сдерживать хакеров, еще предстоит выяснить.

Другие возможные решения

- Глобальный страховой пул

Можно создать глобальный страховой пул, в котором каждый участвующий протокол DeFi вносит часть своих доходов или платит фиксированную плату. В таком случае пул выплатит претензии, когда один из участников столкнется со взломом. Это похоже на идею Федеральной корпорации по страхованию вкладов (FDIC).

- Аудиторам иметь «шкуру в игре»

В рамках этой идеи аудиторам предлагается стейкать собственные средства в страховые платформы DeFi, такие как Nexus Mutual. Если протоколы будут взломаны, то аудиторы в качестве стейкеров понесут убытки. Считается, что эта реализация позволит согласовать интересы аудиторов и проекта.

Советы для частных лиц

Помимо взломов смарт-контрактов, вы также можете подвергнуться различным попыткам взлома. Ниже приведены некоторые шаги, которые вы можете предпринять, чтобы минимизировать риски и снизить вероятность взлома.

Не предоставляйте смарт-контрактам неограниченное одобрение

Взаимодействие с протоколами DeFi обычно требует от вас предоставления доступа к смарт-контрактам и согласия на расходование средств вашего кошелька. Обычно в целях удобства протоколы DeFi запрашивают по умолчанию бесконечный доступ, что означает, что протокол имеет неограниченный доступ к одобренному активу на вашем кошельке.

Предоставление неограниченного разрешения на использование одобренных активов в вашем кошельке обычно является плохой идеей, потому что вредоносный смарт-контракт может использовать это для вывода средств из вашего кошелька.

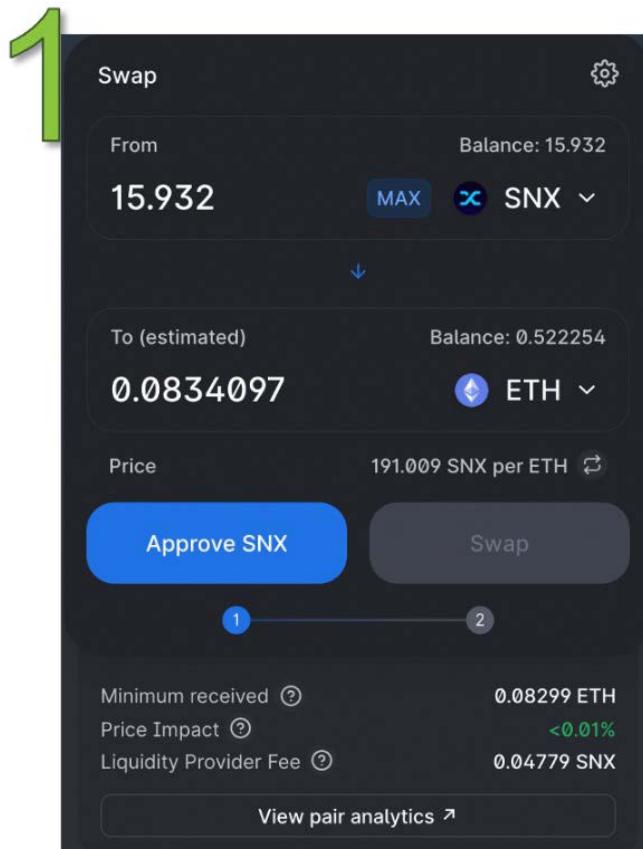
27 февраля 2021 года хакер использовал поддельный смарт-контракт и обманул Furucombo, заставив его думать, что Aave v2 имеет новую реализацию. Атака использовала крупные кошельки с неограниченным количеством одобренных токенов и истощила эти кошельки, переведя средства на адрес, контролируемый хакерами.

В результате этой атаки пользователи Furucombo понесли убытки на общую сумму до 15 миллионов долларов. Даже протокол кредитования Cream Finance допустил ошибку, имея неограниченные разрешения, и потерял 1,1 миллиона долларов из своего хранилища в результате этой атаки.

Таким образом, рекомендуется вручную изменять одобренную сумму для каждой транзакции, чтобы предотвратить предоставление протоколам DeFi неограниченного разрешения на расходы во время одобрения токенов. Даже несмотря на то, что это приведет к дополнительной транзакции для каждого последующего взаимодействия DeFi и повлечет за собой более высокие комиссионные за транзакции, вы можете снизить риск истощения кошельков в результате атаки с использованием смарт-контрактов.

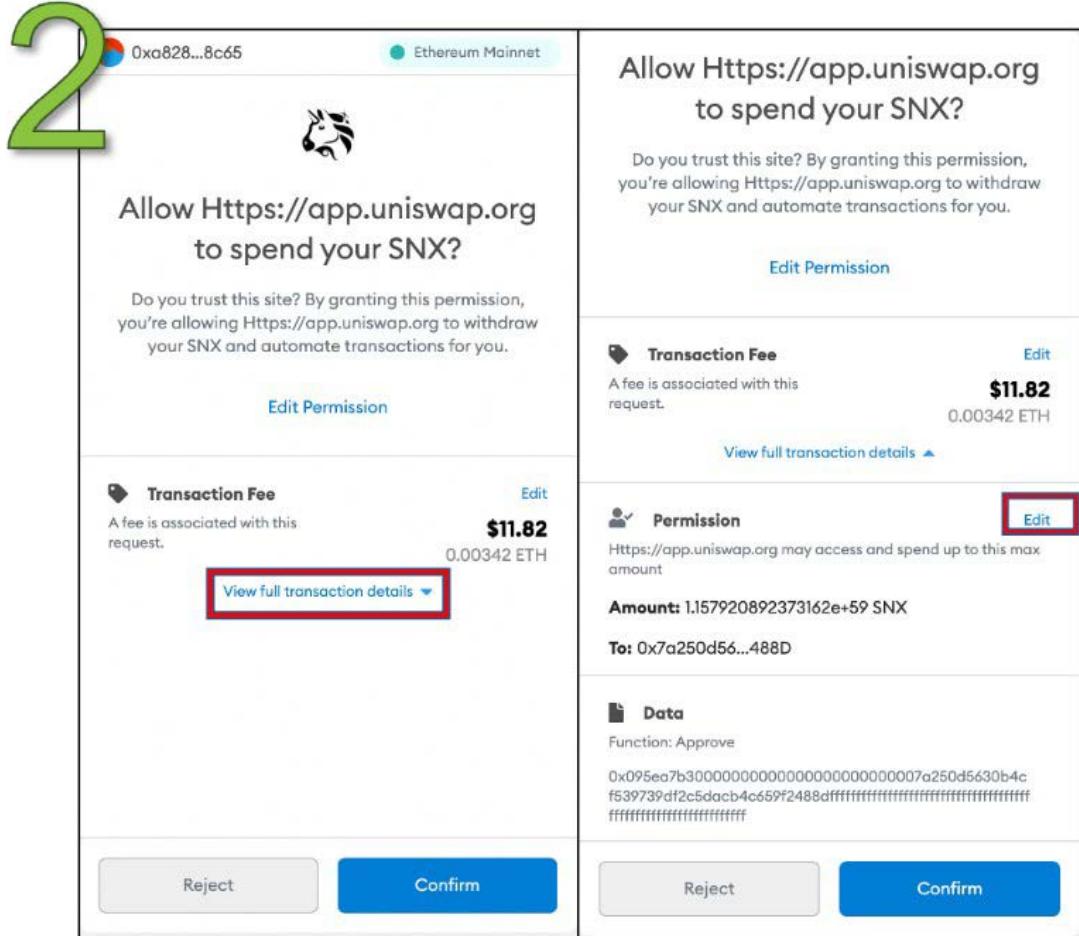
Чтобы вручную изменить одобренную сумму, следуйте приведенному ниже пошаговому руководству.

Не предоставляйте смарт-контрактам неограниченное одобрение: Руководство



Шаг 1

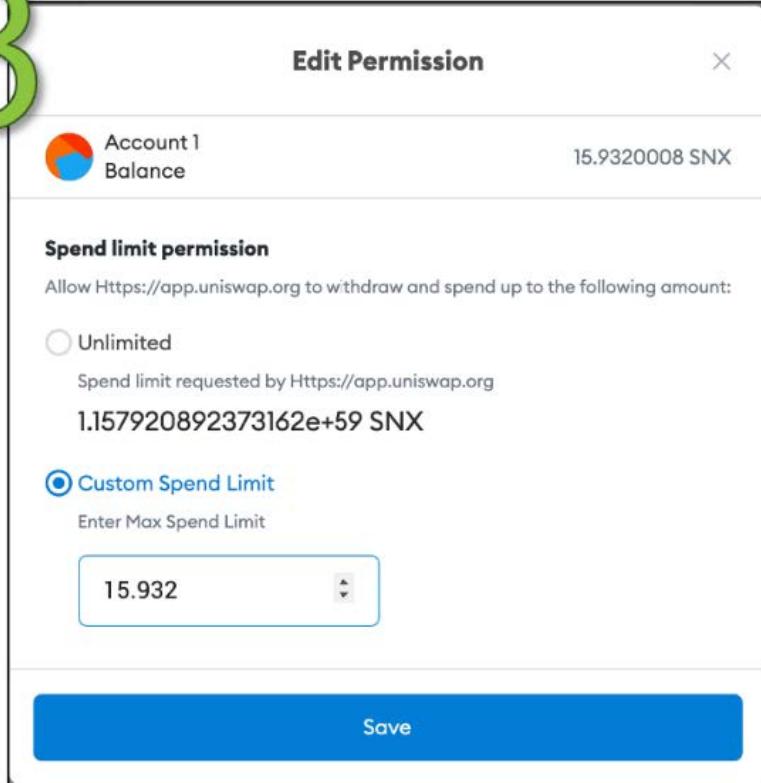
- Одним из наиболее распространенных случаев, требующих подтверждения, является обмен токенов.
- В примере мы планируем обменять 15,932 SNX на 0,0834 ETH на Uniswap.
- Нажимаем «Одобрить SNX» (Approve SNX).



Шаг 2

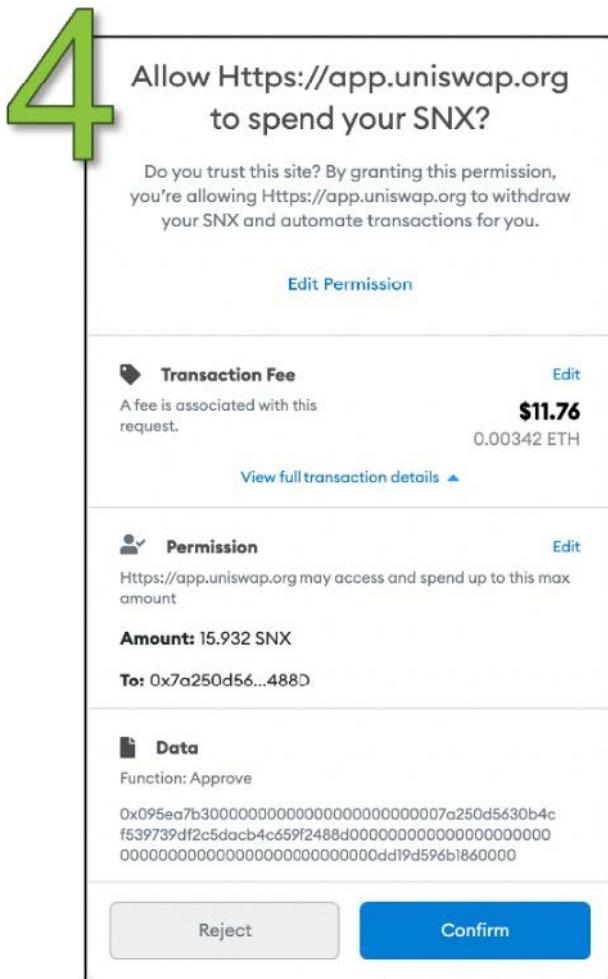
- Левое изображение – это окно по умолчанию, которое мы видим.
- Нажимаем «Просмотреть полную информацию о транзакции».
- Затем нам будет представлено изображение справа. Нажимаем «Изменить» (Edit).

3



Шаг 3

- Выбираем «Пользовательский лимит расходов» (Custom Spend Limit).
- Многие приложения по умолчанию выбирают опцию «Без ограничений».
- Введите сумму, которую мы хотим потратить, в этом примере это 15,932 SNX.



Шаг 4

- В разделе «Разрешение» (Permission) видим, что одобренное число было обновлено.
- Нажимаем «Подтвердить» (Confirm) и оплачиваем комиссию за транзакцию.

Отзыв неограниченных разрешений от смарт-контрактов

Если вы ранее давали протоколам DeFi неограниченные разрешения на расходы, у вас есть два варианта. Более простой вариант – перевести все свои средства на новый адрес Ethereum, и вы получите новый перезапуск без каких-либо рисков, связанных с вашим предыдущим адресом Ethereum.

Однако, если перевод средств с вашего существующего адреса Ethereum невозможен, вы можете проверить список всех предыдущих одобрений, используя инструмент проверки одобрения токенов, предоставляемый Etherscan.

Contract	Approved Spender	Approved Amount	Last Updated (UTC)	Revoke
Compound Dai	[REDACTED]	Unlimited cDAI	2021-01-27 02:37:43	

На этой странице вы можете просмотреть все одобрения, которые вы ранее предоставили смарт-контрактам. Вы должны отозвать все одобрения с неограниченными одобренными суммами, особенно протоколы, с которыми вы больше не взаимодействуете. Обратите внимание, что отзыв каждого одобрения требует самого взаимодействия с смарт-контрактом и повлечет за собой транзакционные комиссии.

Использование аппаратного кошелька

Аппаратный кошелек – это физическое устройство, используемое исключительно для хранения криптовалют. Аппаратные кошельки хранят закрытые ключи отдельно от устройств, подключенных к Интернету, что снижает вероятность взлома вашего кошелька.

В аппаратных кошельках закрытые ключи хранятся в безопасной автономной среде, даже если аппаратный кошелек подключен к компьютеру, зараженному вредоносными программами. Хотя аппаратные кошельки могут быть физически украдены, они бесполезны, если вор не знает ваш код доступа. В случае, если ваш аппаратный кошелек поврежден или украден, вы все равно сможете восстановить свои средства, если вы создали секретный код резервной копии до потери.

Ведущими производителями аппаратных кошельков являются Ledger и Trezor, хотя в отрасль приходит все больше производителей.

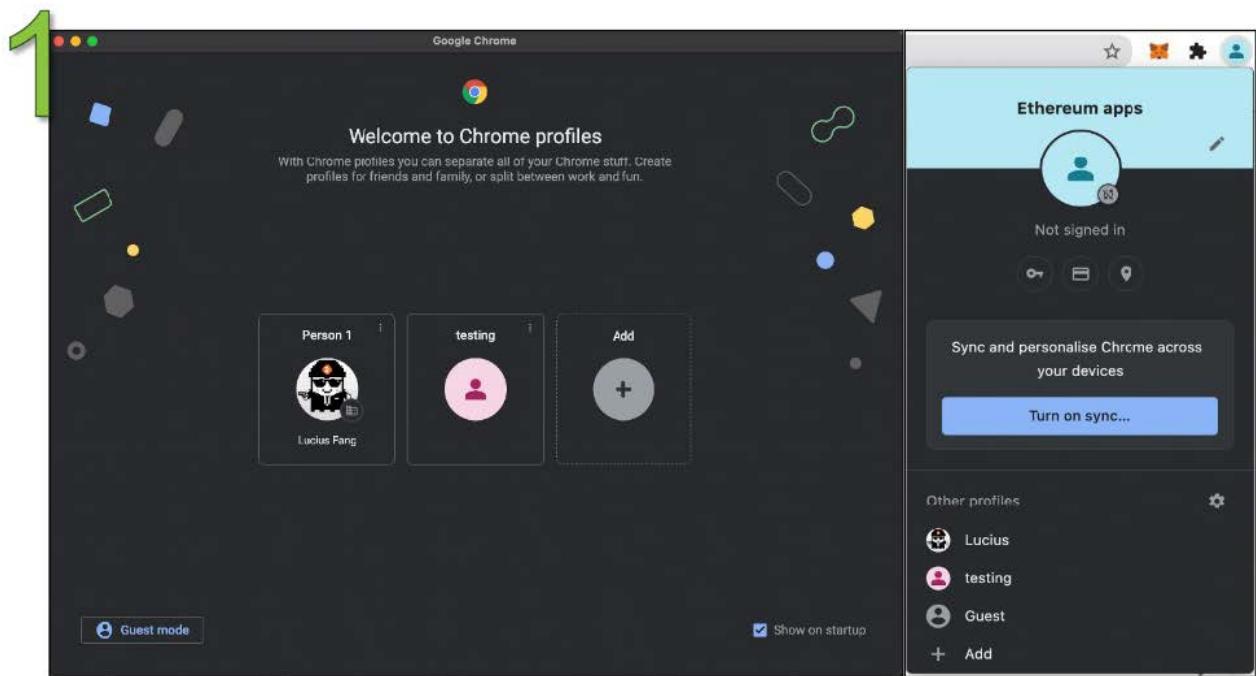
Использование отдельного профиля браузера

Хотя расширения браузера полезны и делают вашу работу более эффективной и продуктивной, вам всегда следует беспокоиться о том, что вредоносные расширения браузера могут вызвать проблемы с вашей криптовалютой.

Если вы случайно установили вредоносное расширение браузера, оно может проникнуть в ваши ключи Metamask и стать вектором атаки на ваши средства. Одним из способов повышения вашей безопасности является создание отдельного профиля браузера в вашем браузере Google Chrome или Brave. В этом новом профиле браузера установите только расширение Metamask. Поступая таким образом, вы снижаете риск того, что вредоносное расширение браузера выведет средства из вашего кошелька.

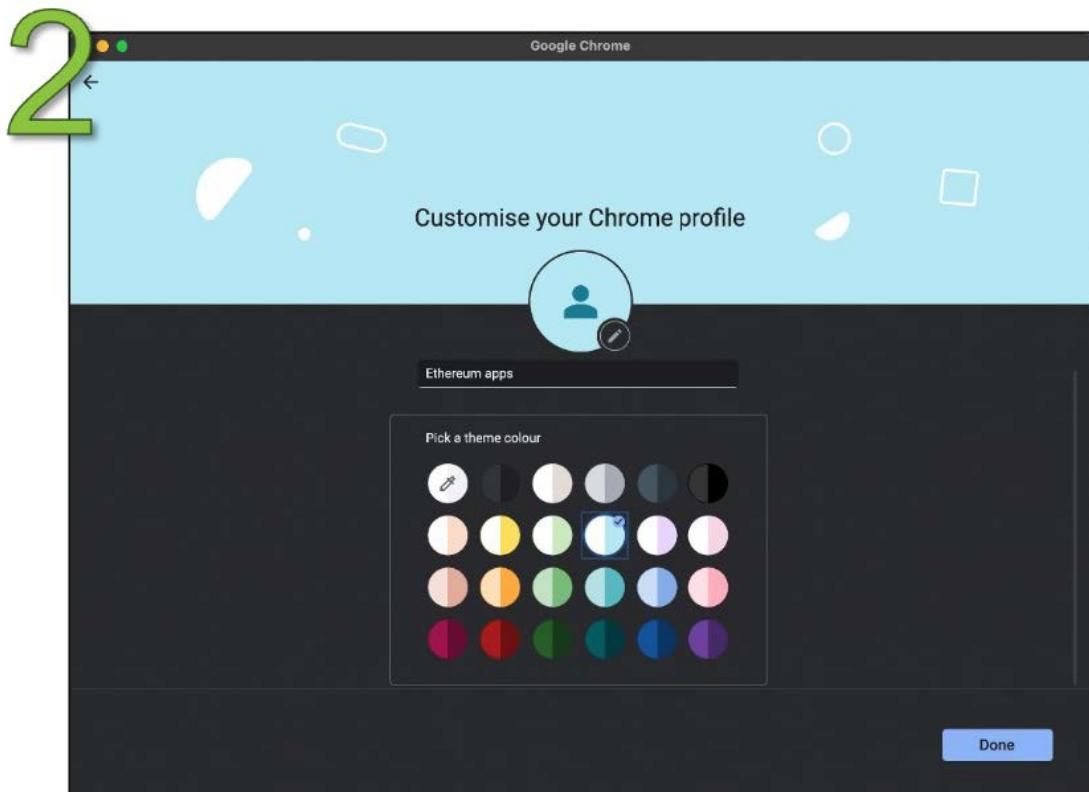
Вот пошаговое руководство по созданию нового профиля браузера в Google Chrome.

Отдельный профиль браузера: Пошаговое руководство



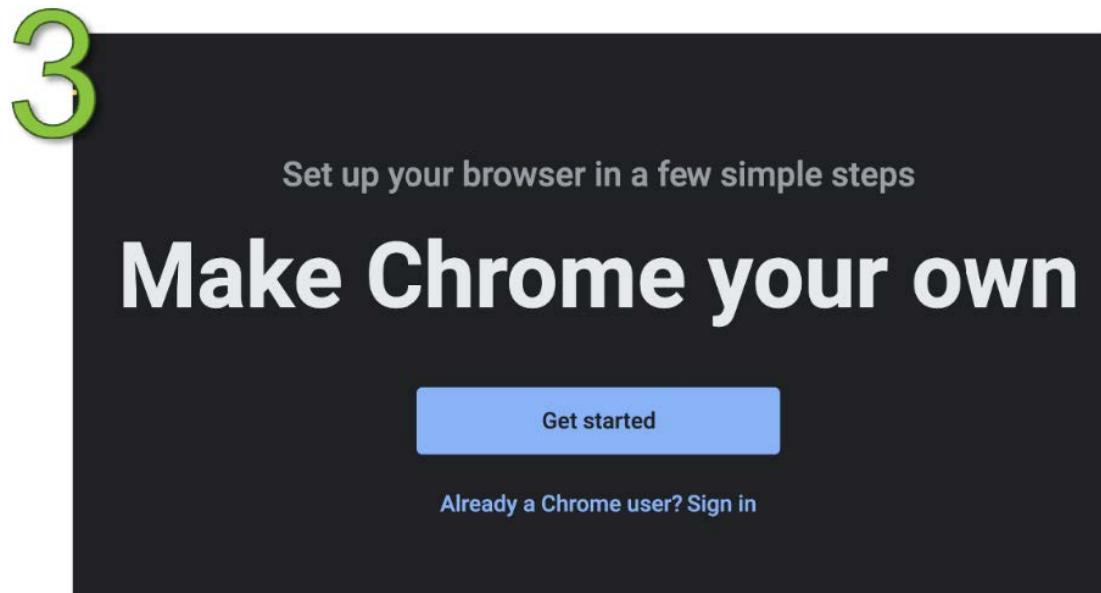
Шаг 1

- Откройте браузер Chrome на указанной выше странице с профилями. Нажмите «Добавить» (Add).
- В качестве альтернативы вы можете перейти в правый верхний угол и нажать на значок профиля. Нажмите «+ Добавить» (Add) в самом низу.



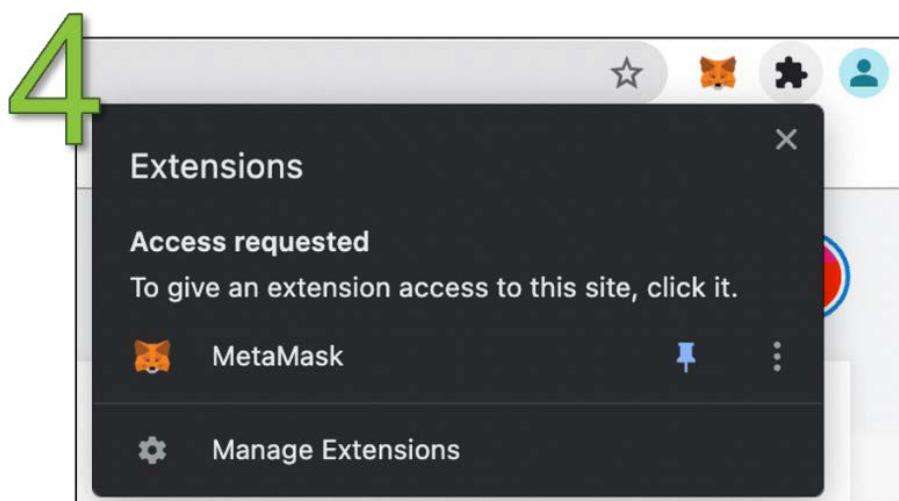
Шаг 2

- Выберите название и цвет. Затем нажмите «Готово» (Done).



Шаг 3

- Войдите в другую учетную запись Chrome, если она у вас есть. Если нет, просто нажмите «Начать» (Get started).



Шаг 4

- Загрузите расширение Metamask и сделайте его единственным расширением в этом профиле.

Вывод

Пространство DeFi по-прежнему является экспериментальной площадкой для различных финансовых инноваций. Таким образом, все может пойти не так. Имейте в виду риски использования новых приложений DeFi, особенно тех, которые не прошли боевую проверку.

Всегда проводите свои исследования, прежде чем использовать какие-либо протоколы DeFi. В большинстве случаев, как только происходит ошибка, нет возможности возместить понесенные убытки. Даже в случае возмещения средств от протокола убытки обычно превышают сумму полученной компенсации.

Тем не менее, из-за связанных с этим рисков, отдача от участия в деятельности DeFi высока. Чтобы не упустить высокую доходность, предлагаемую DeFi, вы можете застраховать некоторые риски, купив страховку или опционы.

Пространство DeFi все еще растет. По мере продвижения мы ожидаем, что будет запущено больше протоколов DeFi с улучшенными гарантиями и страховыми фондами,ключенными в их операционные модели.

Рекомендуемая литература

1. Быть своим собственным банком с Metamask

<https://consensys.net/blog/metamask/metamask-secret-seed-phrase-and-password-management/>

2. Как (не) оказаться в заднице – Объяснение взломов DeFi

<https://finematics.com/defi-hacks-explained/>

3. Безопасность DeFi: С таким количеством взломов будет ли это когда-нибудь безопасно?

<https://unchainedpodcast.com/defi-security-with-so-many-hacks-will-it-ever-be-safe/>

4. Новости о взломах и эксплойтах

<https://www.rekt.news/>

ГЛАВА 16: БУДУЩЕЕ ФИНАНСОВ

Миссия DeFi ясна: переосмысление инфраструктуры и интерфейса традиционных финансов с большей прозрачностью, доступностью, эффективностью, удобством и совместимостью.

По состоянию на апрель 2021 года общая стоимость заблокированных (TVL) приложений DeFi достигла 86 миллиардов долларов – в 86 раз больше с тех пор, как мы в последний раз публиковали наше руководство по DeFi: для начинающих (Первое издание) в марте 2020 года. В то время TVL в DeFi только что достиг 1 миллиарда долларов.

Вот краткое резюме основных этапов DeFi:

- 2018: TVL увеличился в 5 раз с 50 миллионов долларов до 275 миллионов долларов
- 2019: TVL увеличился в 2,4 раза до 667 миллионов долларов
- 2020: TVL увеличился в 23,5 раза до 15,7 миллиарда долларов
- 2021 год: TVL увеличился в 5,5 раза до 86,05 миллиарда долларов (по состоянию на апрель 2021 года)

Из обеих наших книг вы можете видеть, что DeFi сам по себе переосмысливает то, как работают глобальные финансовые системы. Как мы рассказывали во всех наших главах, различные финансовые примитивы уже существуют, такие как децентрализованные биржи, кредитование, страхование и производные финансовые инструменты. Независимо от местоположения и статуса, DeFi позволила любому человеку в мире получить доступ к финансовым услугам, если у него есть доступ в Интернет.

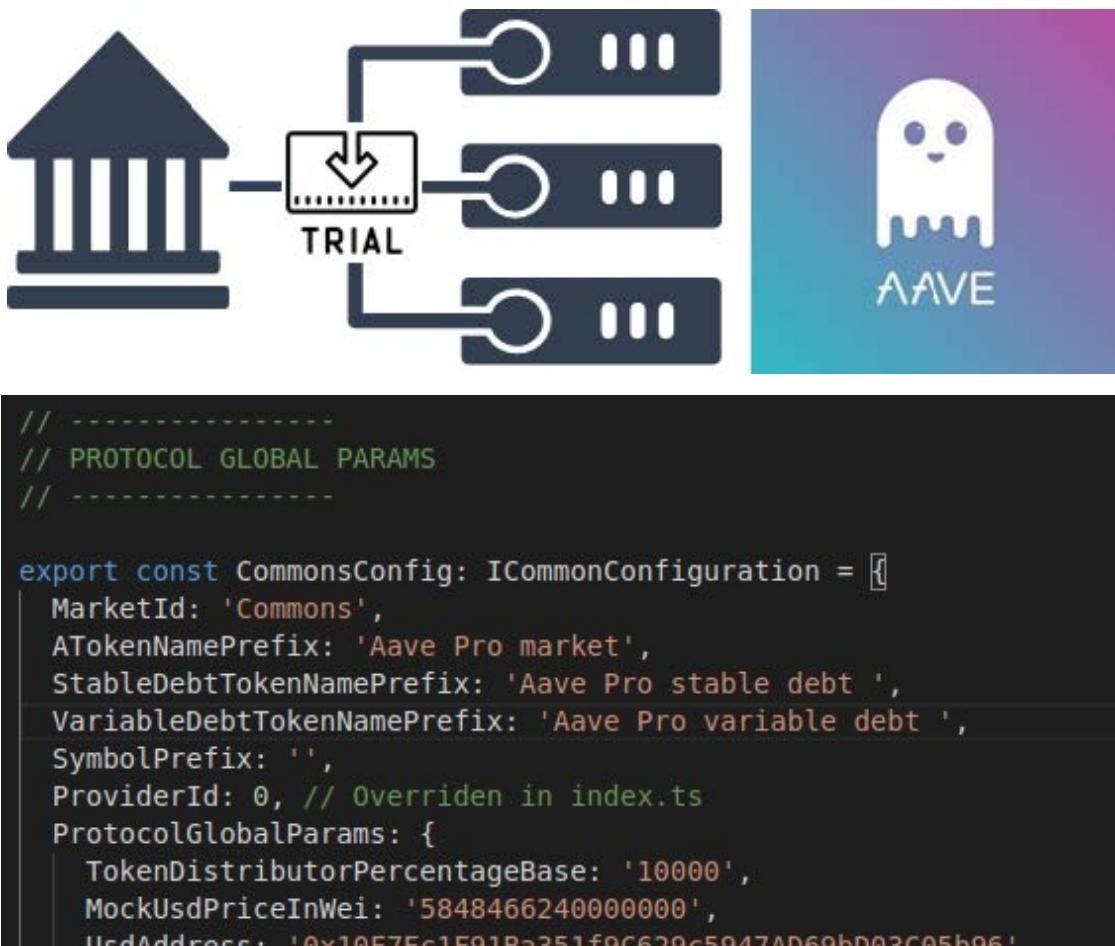
Хотя большинство протоколов DeFi, которые мы рассмотрели, являются уроженцами Ethereum, мы уже видим экспоненциальный рост пользователей и проектов в других блокчейн-сетях, таких как Binance Smart Chain, Solana, Polygon и Fantom.

Переосмысление унаследованных финанс – это нечто большее, чем просто технология. Это также означает переосмысление культуры. В своей основе DeFi представляет собой прозрачное и открытое движение с чрезвычайно мощной культурой, которое продолжает свою миссию по созданию стоимости в десятки триллионов долларов. Эта культура – то, что помогает сформировать и узаконить DeFi.

Великие умы собрались вместе и попытались решить некоторые из наиболее насущных проблем, которые беспокоят традиционные финансы. Результат сочетает в себе традиционные финансовые принципы, инновации и технологию блокчейна, предлагая при этом превосходные финансовые продукты и услуги.

Сколько времени пройдет до того, как институты будут опираться на эти сети?

Мы уже видели примеры институтов, построенных на DeFi. Например, Visa объявила в первом квартале 2021 года, что вскоре начнет проводить расчеты с USDC на Ethereum. В мае 2021 года Aave построила частный пул для учреждений в качестве площадки для практики, прежде чем войти в экосистему DeFi. Оба являются отличными примерами совместного обучения между двумя финансовыми системами и выступают в качестве предшественника прямого участия институционалов в DeFi.



Скриншот строк кода смарт-контракта Aave Pro.

К чему это приведет нас в ближайшие 5-10 лет?

Трудно сказать, как все будет в будущем, но мы хотели бы думать о DeFi как о технологическом движении, которое бросает вызов статус-кво традиционных финанс. Подобно тому, как Интернет сделал многие изобретения устаревшими, революционизировав способ нашего общения и обмена информацией, DeFi сделает то же самое для финансов и воспользуется преимуществами глобальной сети для создания более прозрачной и эффективной финансовой системы.

Разработка требует времени, но темпы инноваций в DeFi развиваются с головокружительной скоростью. По состоянию на апрель 2021 года общая стоимость средств, заблокированных в DeFi, выросла более чем в 1700 раз по сравнению с тем, что было четыре года назад в 2018 году.

Одна из главных причин, по которой мы пришли сюда, заключается в том, что разработчики и сообщество DeFi неустанно строят, строят и строят, несмотря на конкурентную среду в криптовалютном пространстве. За это мы хотим сказать всем вам спасибо за то, что сделали возможным открытые финансы.

Заключение

Поздравляю вас с тем, что вы добрались так далеко! От текущего состояния DeFi до децентрализованных обменов и эксплойтов наше путешествие по DeFi в этой книге подошло к концу. Однако это еще не конец, так как всегда будут новые вещи, которые нужно изучить, и новые протоколы для изучения.

К настоящему времени у вас должно быть более глубокое понимание DeFi и того, как оно работает. Вы должны знать, что DeFi движется очень быстро и бесконечно усложняется. К тому времени, когда мы опубликуем эту книгу, часть информации уже устареет!

Тем не менее, мы надеемся, что «Что такое DeFi: Продвинутый курс» станет основным ориентиром в вашем путешествии в DeFi. Пусть это поможет вам в ваших нескончаемых поисках и исследований множества кроличьих нор.

Приложения

Рекомендации CoinGecko

Аналитика

Defillama - <https://defillama.com/home>

DeBank - <https://debank.com/>

DeFi Prime - <https://defiprime.com/>

DeFi Pulse - <https://defipulse.com/>

Dune Analytics - <https://duneanalytics.com/home>

LoanScan - <http://loanscan.io/>

Nansen - <https://www.nansen.ai/>

Token Terminal - <https://www.tokenterminal.com/>

The Block Dashboard - <https://www.theblockcrypto.com/data>

Новые сайты

CoinDesk - <https://www.coindesk.com/>

CoinTelegraph - <https://cointelegraph.com/>

Decrypt - <https://decrypt.co/>

The Block - <https://www.theblockcrypto.com/>

Crypto Briefing - <https://cryptobriefing.com/>

Почтовые рассылки

CoinGecko - <https://landing.coingecko.com/newsletter/>

Bankless - <https://bankless.substack.com/>

DeFi Tutorials - <https://defitutorials.substack.com/>

DeFi Weekly - <https://defiweekly.substack.com/>

DeFi Pulse Farmer - <https://yieldfarmer.substack.com/>

Delphi Digital - <https://www.delphidigital.io/research/>

Dose of DeFi - <https://doseofdefi.substack.com/>

Ethhub - <https://ethhub.substack.com/>

Deribit Insight - <https://insights.deribit.com/>

My Two Gwei - <https://mytwogwei.substack.com/>

Messari - <https://messari.io/>

The Defiant - <https://thedefiant.substack.com/>

Week in Ethereum News - <https://www.weekinethereumnews.com/>

Подкасты

CoinGecko - <https://podcast.coingecko.com/>

BlockCrunch - <https://castbox.fm/channel/Blockcrunch%3A-Crypto-Deep-Dives-id1182347>

Chain Reaction - <https://fiftyonepercent.podbean.com/>

Into the Ether - Ethhub - <https://podcast.ethhub.io/>

PoV Crypto - <https://povcryptopod.libsyn.com/>

Uncommon Core - <http://uncommoncore.co/podcast/>

Unchained Podcast - <https://unchainedpodcast.com/>

Wyre Podcast - <https://blog.sendwyre.com/wyretalks/home>

Youtube

Bankless - <https://www.youtube.com/channel/UCAI9Ld79qaZxp9JzEOwd3aA>

Chris Blec - <https://www.youtube.com/c/chrisblec>

DeFi Dad - <https://www.youtube.com/channel/UCatItl6C7wJp9txFMbXbSTg>

Economics Design - <https://www.youtube.com/c/EconomicsDesign>

The Defiant - <https://www.youtube.com/channel/UCL0J4MLEdLP0-UyLu0hCktg>

Yield TV by Zapper - <https://www.youtube.com/channel/UCYq3ZxBx7P2ckJuWVDC597q>

Руководство по Bankless

<https://bankless.substack.com/p/bankless-level-up-guide>

Понравившиеся проекты

Панели управления

Zapper - <https://zapper.fi/dashboard>

Frontier - <https://frontierwallet.com/>

InstaDapp - <https://instadapp.io/>

Zerion - <https://zerion.io/>

Debank - <https://debank.com/>

Децентрализованные обмены

Uniswap - <https://uniswap.org/>

SushiSwap - <https://sushi.com/>

Balancer - <https://balancer.exchange/>

Bancor - <https://www.bancor.network/>

Curve Finance - <https://www.curve.fi/>

Kyber Network - <https://kyberswap.com/swap>

Dodo - <https://dodoex.io/>

Агрегаторы обмена

1inch - <https://1inch.exchange/>

Paraswap - <https://paraswap.io/>

Matcha - <https://matcha.xyz/>

Кредитование и заимствование

Maker - <https://oasis.app/>

Compound - <https://compound.finance/>

Aave - <https://aave.com/>

Cream - <https://cream.finance/>

Оракулы и агрегаторы данных

Covalent - <https://www.covalenthq.com/>

The Graph - <https://thegraph.com/>

Рынки прогнозирования

Augur - <https://www.augur.net/>

Налоги

TokenTax - <https://tokentax.co/>

Кошельки

Metamask - <https://metamask.io/>

Argent - <https://argent.link/coingecko>

Dharma - <https://www.dharma.io/>

GnosisSafe - <https://safe.gnosis.io/>

Monolith - <https://monolith.xyz/>

Оптимизаторы дохода

APY Finance - <https://apy.finance/>

Yearn - <https://yearn.finance/>

Alpha Finance - <https://alphafinance.io/>