Homework 3: Analysing DeFi

Exercise 1 - VRF Oracle

Part A - exploring direct funding VRF

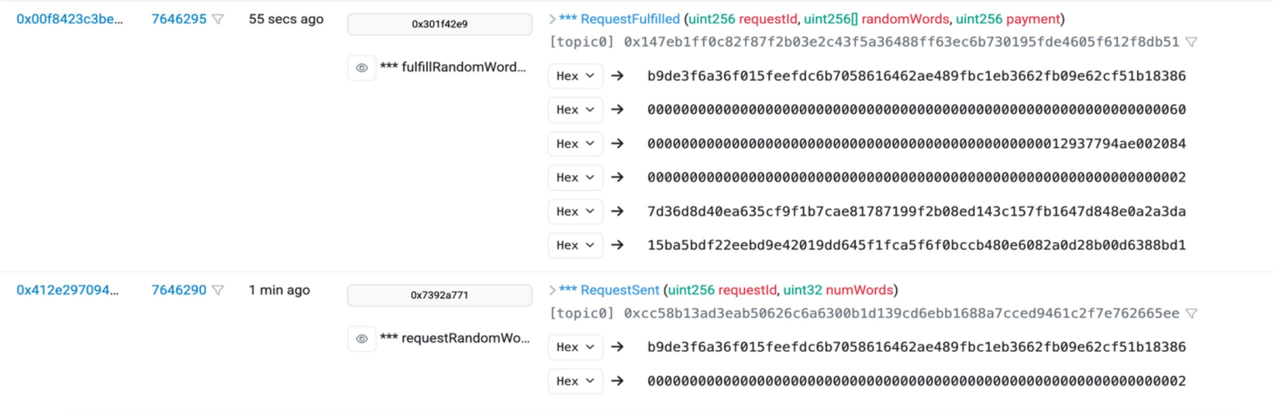
I deployed DirectFundingConsumer.sol and got the following message:

```
Deployer: 0xf23fd4b5675d5BAe6B2C95313e6C183489e940D6

Deployed to: 0xc83B07ff47A8f8eB8965deE0134ce3264Afc728d

Transaction hash:
0xa92076db0c2b4990a97df38affdefb8cfe216208475480d772bdbb5681ff7b30
```

I then sent some LINK tokens to the contract and requested a random number. I typed the following command:

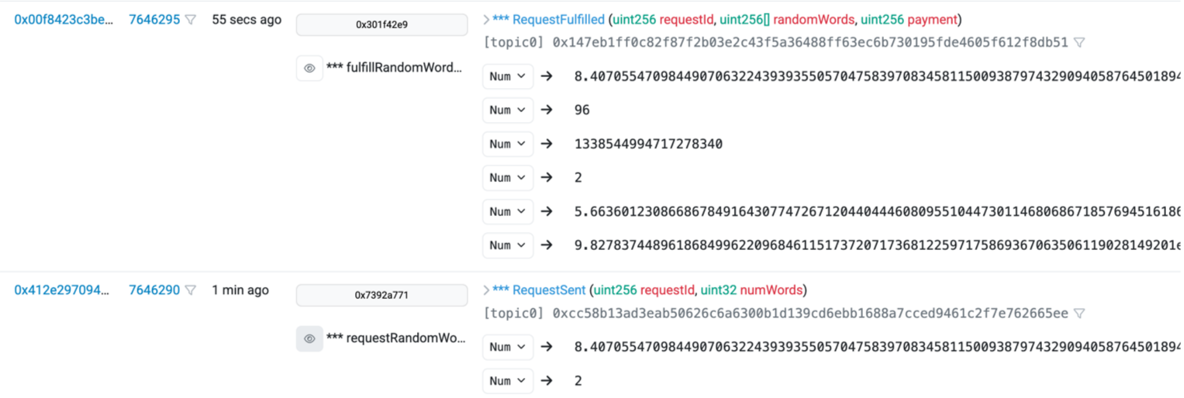
```
cast send --rpc-url https://ethereum-sepolia-rpc.publicnode.com --private-key my_private_key
"requestRandomWords(bool)" false
```

Here are the two screenshots, the first showing the events in hex representation, and the second one in numerical form.



```
0x00f8423c3be...   7646295   55 secs ago   0x301f42e9   *** fulfillRandomWord...
> *** RequestFulfilled (uint256 requestId, uint256[] randomWords, uint256 payment)
[topic0] 0x147eb1ff0c82f87f2b03e2c43f5a36488ff63ec6b730195fde4605f612f8db51
Hex → b9de3f6a36f015feefdc6b7058616462ae489fbc1eb3662fb09e62cf51b18386
Hex → 0000000000000000000000000000000000000000000000000000000000000060
Hex → 00000000000000000000000000000000000000000000000012937794ae002084
Hex → 0000000000000000000000000000000000000000000000000000000000000002
Hex → 7d36d8d40ea635cf9f1b7cae81787199f2b08ed143c157fb1647d848e0a2a3da
Hex → 15ba5bdf22eebd9e42019dd645f1fca5f6f0bccb480e6082a0d28b00d6388bd1

0x412e297094...   7646290   1 min ago   0x7392a771   *** requestRandomWo...
> *** RequestSent (uint256 requestId, uint32 numWords)
[topic0] 0xcc58b13ad3eab50626c6a6300b1d139cd6ebb1688a7cced9461c2f7e762665ee
Hex → b9de3f6a36f015feefdc6b7058616462ae489fbc1eb3662fb09e62cf51b18386
Hex → 0000000000000000000000000000000000000000000000000000000000000002
```

Figure 1: Events from requestRandomWords with hex values



```
0x00f8423c3be...   7646295   55 secs ago   0x301f42e9   *** fulfillRandomWord...
> *** RequestFulfilled (uint256 requestId, uint256[] randomWords, uint256 payment)
[topic0] 0x147eb1ff0c82f87f2b03e2c43f5a36488ff63ec6b730195fde4605f612f8db51
Num → 8.4070554709844907063224393935505704758397083458115009387974329094058764501894
Num → 96
Num → 1338544994717278340
Num → 2
Num → 5.6636012308668678491643077472671204404446080955104473011468068671857694516186
Num → 9.827837448961868499622096846115173720717368122597175869367063506119028149201e

0x412e297094...   7646290   1 min ago   0x7392a771   *** requestRandomWo...
> *** RequestSent (uint256 requestId, uint32 numWords)
[topic0] 0xcc58b13ad3eab50626c6a6300b1d139cd6ebb1688a7cced9461c2f7e762665ee
Num → 8.4070554709844907063224393935505704758397083458115009387974329094058764501894
Num → 2
```

Figure2: Events from requestRandomWords with numerical values

The two random numbers the oracle generated are (in hex):

- 7d36d8d40ea635cf9f1b7cae81787199f2b08ed143c157fb1647d848e0a2a3da
- 15ba5bdf22eebd9e42019dd645f1fca5f6f0bccb480e6082a0d28b00d6388bd1

RequestSent returns 2 fields: requestId (the first field), which is a unique identifier for the request (parameter of type uint256) and numWords, which is the number of random numbers I want (2 in this instance).

RequestFulfilled returns 6 fields, which were a bit harder to understand, because the function only has 3 main events: requestId, randomWords (which is an array of 2 here), and payment.
The first field is in fact the requestId (it is the same as RequestSent).
The second field is the memory location of unint256[]: it is an offset to where the data is stored.
The third field is the payment.
the fourth is the length of the array (2 here).
The last two fields are the random numbers.

Part B - Adding a VRF oracle to coinflip

I deployed my modified Coinflip.sol file and got the following message:

```
Deployer: 0xf23fd4b5675d5BAe6B2C95313e6C183489e940D6

Deployed to: 0x70ae24510fC4E14fF1D37c9c3530736dD8C98753

Transaction hash:
0x44daea99ee47bf9044b2aecb94feee9325fd7da8d1db2f8659b9cb332a01e9b0
```

Part C - Contrast data serving methods

In the direct funding method, users fund each randomness request individually by providing LINK tokens directly to the contract making the request. There is no need to create a subscription beforehand. The payment for the randomness is made each time a request is made, ensuring that the contract has enough funds at the moment of the request. This method is more suitable for one-off or infrequent randomness needs, as it provides flexibility in managing funding, especially for smaller contracts or projects with varying funding needs.

On the other hand, the subscription method involves creating a subscription and pre-funding it with LINK tokens. The subscription allows the contract to make multiple randomness requests using the balance in the subscription without having to fund each request individually. This method is more efficient for applications that require frequent or recurring randomness requests. It ensures a smooth operation where randomness can be requested multiple times without manual intervention for each request. This method is ideal for applications that need a continuous supply of randomness, such as games, lotteries, or applications with recurring randomness needs. It also offers centralized management of funding, which is particularly useful for managing large systems or multiple contracts within a single application.

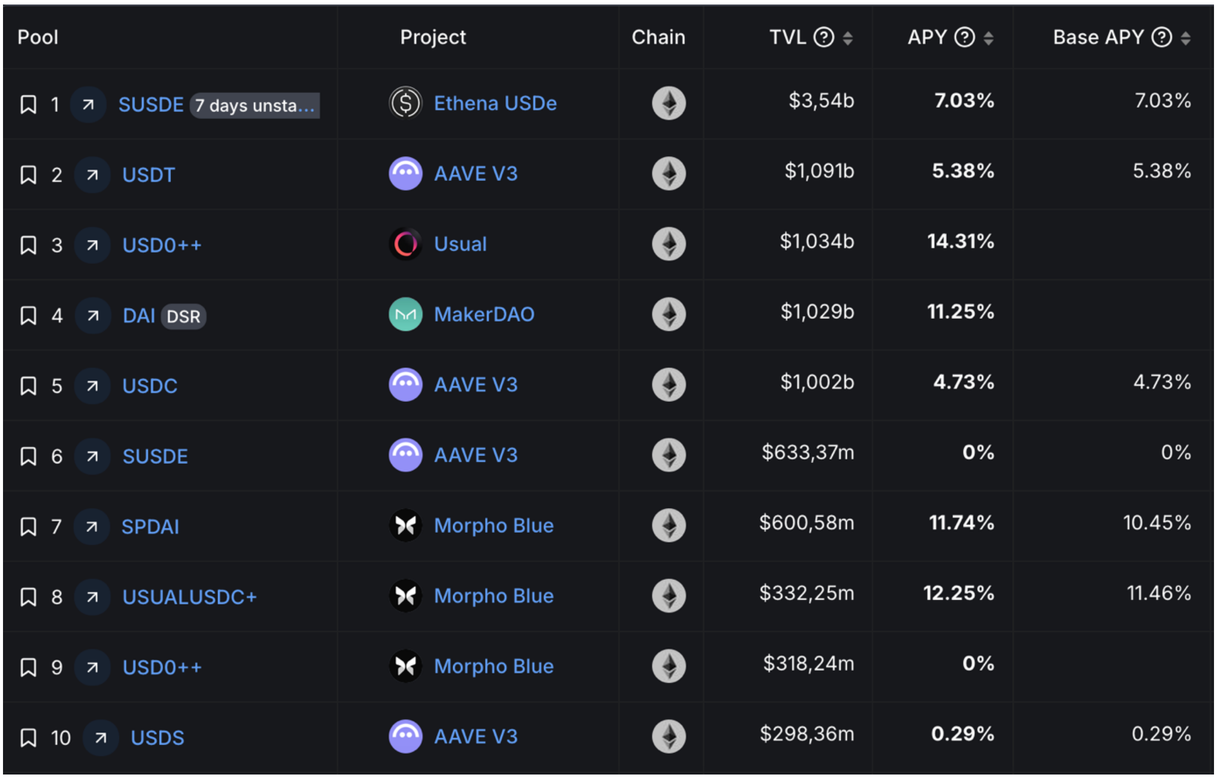
Exercise 2 - MakerDAO 2.0 Tokenomics

Part A - Meta assessment of DeFi projects through aggregators

Collateralized Debt Positions (CDPs) are a key part of decentralized finance (DeFi). They let users lock up assets as collateral and create stablecoins. MakerDAO was one of the first to use this system and remains a major player, but it now faces growing competition from projects like Liquity, Curve Finance, Davos, and Ramp. Let's look at the CDP market using data from DefiLlama and Dune Analytics, focusing on key metrics that we studied in class such as TVL, APY, and NVT ratio.

According to DefiLlama's dashboard (Figure 1), MakerDAO's DAI remains one of the most significant decentralized stablecoins, ranking fourth in market capitalization behind centralized alternatives like USDT and USDC. The DAI Savings Rate (DSR), which acts as the CDP mechanism within MakerDAO, has successfully maintained a substantial TVL of $1.029 billion. The associated APY currently stands at an attractive 11.25%, making it one of the most appealing stablecoin staking options in the market.

Despite MakerDAO's strong position, newer CDP protocols have been quickly gaining traction. Ethena USDe, for instance, has already surpassed MakerDAO in terms of TVL, reaching an impressive $3.54 billion in locked assets with a 7.03% APY. Other competitors, such as Liquity's LUSD and Usual's USD0++, have also been making notable progress, with Usual currently offering an even higher APY of 14.31%. This shift in liquidity distribution suggests that users are increasingly seeking alternatives that provide better yields or novel mechanisms that enhance capital efficiency.



Pool	Project	Chain	TVL	APY	Base APY
1 ↗ SUSDE 7 days unsta...	Ethena USDe	⟠	$3,54b	**7.03%**	7.03%
2 ↗ USDT	AAVE V3	⟠	$1,091b	**5.38%**	5.38%
3 ↗ USD0++	Usual	⟠	$1,034b	**14.31%**	
4 ↗ DAI DSR	MakerDAO	⟠	$1,029b	**11.25%**	
5 ↗ USDC	AAVE V3	⟠	$1,002b	**4.73%**	4.73%
6 ↗ SUSDE	AAVE V3	⟠	$633,37m	**0%**	0%
7 ↗ SPDAI	Morpho Blue	⟠	$600,58m	**11.74%**	10.45%
8 ↗ USUALUSDC+	Morpho Blue	⟠	$332,25m	**12.25%**	11.46%
9 ↗ USD0++	Morpho Blue	⟠	$318,24m	**0%**	
10 ↗ USDS	AAVE V3	⟠	$298,36m	**0.29%**	0.29%

Figure 3: TVL and APY distribution for the top 10 stablecoins

MakerDAO has historically been recognized as a stable and reliable CDP platform, benefiting from its decentralized governance model and deep liquidity. However, the rise of protocols like Morpho Blue and AAVE V3 has significantly changed the competitive landscape. The data from DefiLlama shows that AAVE V3 is rapidly growing in influence, with $1.091 billion in TVL for USDT CDPs and another $1.002 billion for USDC. While these figures highlight AAVE's increasing market presence, the lower APYs of 5.38% and 4.73%, respectively, suggest that MakerDAO still offers a more attractive yield in comparison.

Dune Analytics (Figure 4) further shows MakerDAO's strength by presenting its gross revenue from interest income**.** In 2024, MakerDAO's revenue has surged, peaking at $43 million in December, which reflects increased DAI adoption and higher borrowing rates. By contrast, competitors exhibit flatter revenue trajectories, with only a few surpassing MakerDAO's monthly performance.

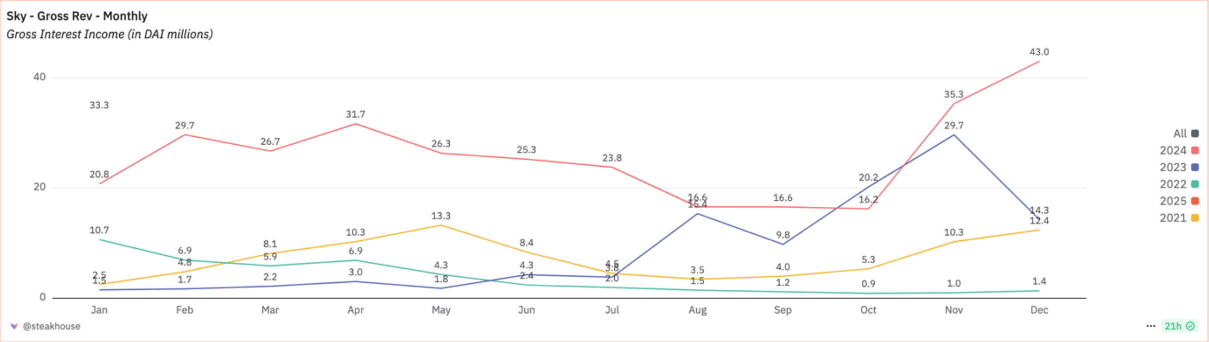


Figure 4: Gross Interest Income (in DAI millions) of MakerDAO from 2021 to 2024

MakerDAO remains a leading CDP protocol, offering high stability and competitive yields through its DAI Savings Rate. However, competitors like Ethena and Usual are attracting liquidity with higher APYs and more aggressive expansion strategies. MakerDAO continues to generate excellent revenue, but in order for that to be sustainable, new mechanisms of collateral-including dynamic adjustments of interest rates-will be necessary to deal with the ever-changing DeFi landscape.

Part B - Examining MKR tokenomics (3 points)

Black Thursday, which occurred on March 12, 2020, was a major stress test for the DeFi ecosystem, particularly for MakerDAO and its governance token, MKR. During this event, the price of ETH, which was heavily used as collateral in MakerDAO's Collateralized Debt Positions (CDPs), crashed by nearly 50% in a single day. This rapid drop in collateral value led to mass liquidations within Maker's system, many of which occurred at nearly zero cost due to network congestion and auction failures. As a result, DAI lost its peg, and MakerDAO faced a severe crisis.

Prior to Black Thursday, MKR traded at around $500**.** However, due to the sudden liquidation issues and uncertainty surrounding MakerDAO's ability to maintain system stability, MKR's price plummeted to approximately $200 in the days following the event. This drastic decline reflected investors' lack of confidence in MakerDAO's ability to recover.

In response, MakerDAO implemented several critical changes to restore stability and investor confidence. The most significant measures included introducing USDC as an emergency collateral type**,** modifying auction parameters to prevent zero-bid liquidations, and overhauling the risk management framework to enhance the protocol's resilience. These changes gradually restored trust in MakerDAO, and as DeFi adoption surged in the following months, MKR rebounded, eventually reaching new all-time highs above $6,000 in 2021.

Feature	**Before Black Thursday**	**After Black Thursday**
Collateral Types	ETH was the primary collateral	USDC, WBTC, and other assets added to reduce reliance on ETH
Liquidation Mechanism	Auctions could be executed at near-zero prices due to network congestion	New auction mechanisms implemented with better protections
Governance Changes	Slow and reactive governance	More active governance with quicker parameter adjustments
Risk Management	Minimal external risk assessments	More robust risk frameworks introduced
MKR Burn Mechanism	Burned through stability fees	More systematic adjustments to MKR burning strategies

These changes significantly improved MakerDAO's resilience, ensuring that the MKR token could better withstand future market shocks. The lessons from Black Thursday led to a stronger governance framework, improved liquidation mechanisms, and broader collateral diversification, all of which have contributed to MKR's long-term recovery and growth.

Part C - Personal reflection on the current and future state of MakerDAO

The transition of MakerDAO to Sky is a significant shift in governance and operational structure. The rebranding reflects a broader decentralization strategy, moving away from Maker Foundation oversight toward a fully autonomous, community-driven model. This evolution aligns with the core principles of DeFi: reducing centralized control and ensuring long-term sustainability. The transition introduces new tokenomics with the SKY token, replacing MKR and aiming for more efficient governance, incentivization, and scalability. The redesign aims to solve some of the inefficiencies in MKR's economic model, such as governance inefficiencies and lack of widespread participation. If successful, this could set a precedent for other DAOs looking to refine their structures of governance.

The implications of future technological developments in AI and quantum computing on MakerDAO and blockchain in general are interesting to consider. It can enhance the role of risk assessment, collateralization models, and liquidation mechanisms within MakerDAO for better resilience of the system to different outcomes. AI-driven trading and lending models might also help optimize liquidity efficiency and dampen systemic risks within the DeFi ecosystem. On the other hand, quantum computing presents a potential existential threat to blockchain security. If quantum-resistant cryptographic methods are not implemented in time, smart contracts and private key security could be compromised, which would affect the entire DeFi industry, including MakerDAO.

Overall, MakerDAO’s transformation into Sky is a step towards a more sustainable and decentralized governance model. However, the success of its new tokenomics will depend on adoption and whether it balances incentives for users and governance participants. Meanwhile, the broader DeFi industry, including MakerDAO, must stay ahead of emerging technological disruptions to ensure long-term viability.