

Homework 3: Written Answers

Exercise 1: VRF Oracle

Part A: Exploring direct funding VRF

a) Here is a screenshot of the two events on Etherscan in Hex values:

[illegible]

Here is a screenshot of the two events on Etherscan in number values:

| Transaction Hash | Block | Age | Method | Logs |
|-------------------|---------|------------|------------|--|
| 0xf0f91beb081e... | 7640651 | 2 days ago | 0x301f42e9 | <div> <div>*** RequestFulfilled (uint256 requestId, uint256[] randomWords, uint256 payment)</div> <div>[topic0] 0x147eb1ff0c82f87f2b03e2c43f5a36488ff63ec6b730195fde4605f612f8db51</div> </div> <div> <div>*** fulfillRandomWords...</div> <div>Num → 8.3163425658249684330227475922907374004186075575678020319923633891127359985012e+76</div> <div>Num → 96</div> <div>Num → 44629231808931689</div> <div>Num → 2</div> <div>Num → 6.2599615646356822356848562427923451814629089809014876996707400279558520886419e+76</div> <div>Num → 1.9714175045937910702578937718545303120507407414636200980036689650398386439195e+76</div> </div> |
| 0x829bbe1d3bc... | 7640646 | 2 days ago | 0x7392a771 | <div> <div>*** RequestSent (uint256 requestId, uint32 numWords)</div> <div>[topic0] 0xccc58b13ad3eab50626c6a6300b1d139cd6ebb1688a7cced9461c2f7e762665ee</div> </div> <div> <div>*** requestRandomWor...</div> <div>Num → 8.3163425658249684330227475922907374004186075575678020319923633891127359985012e+76</div> <div>Num → 2</div> </div> |

b) The two random numbers generated by the oracle for me are the last two fields of the RequestFulfilled event:

- 6.2599615646356822356848562427923451814629089809014876996707400279558520886419e+76
- 1.9714175045937910702578937718545303120507407414636200980036689650398386439195e+76

c) We can now explain what each of these fields represent. First, we can take a look at RequestSent. It is the event emitted whenever you send a request to the

contract so that it generates random numbers (in our case, 2 random numbers).

Here are the fields of this event:

- requestId (type uint256): It is a unique identifier of the request made.
- numWords (type uint256): It represents the number of requested values

We can now take a look at the RequestFulfilled event. It occurs when the request that has been sent previously has been completed by the oracle. Here are the fields of this event:

- requestId (type uint256): It is again the unique identifier of the request made. Hence, it matches the one of the RequestSent event.
- randomWords (type uint256[], hence a dynamic array): Because it is a dynamic array, it has to state where the dynamic part starts (in our case, at the 96th bytes starting from the beginning). The last three fields will be linked to this one.
- payment (type uint256): This field simply represents the cost of the request.

As said previously, the last three fields of this event are linked to randomWords as it is a dynamic array, and Etherscan lists each element of this array separately:

- Length of the array (type uint256): It simply shows the number of elements in the array (in our case 2).
- 1st array element (type uint256): It is the first random number generated by the oracle.
- 2nd array element (type uint256): it is the second random number generated by the oracle.

Part B: Adding a VRF oracle to coinflip

Here is the contract address: 0xbEA0706A0f61cbbD89847FBF3e92C0D76B0Cc92A

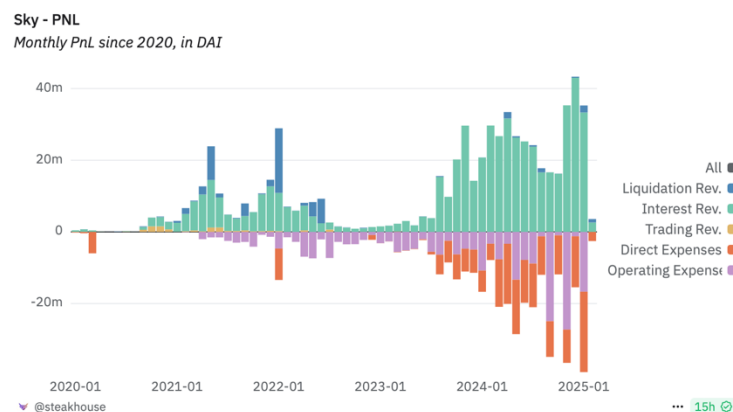
Part C: Contrast data serving methods

Two of the possible methods for a VRF are the direct funding method and the subscription method. For the direct funding method, each time a user requests random values, it will have to do so through a consuming contract that needs to be funded accordingly with LINK tokens. Concerning the subscription method, you can create a subscription account that you fund with LINK tokens. Thus, you can use this sole subscription account to call multiple consuming contracts. Hence, you only need to fund one contract in the subscription method. The latter is more effective when recurrent random requests are made, is better when there are multiple VRF-consuming contracts, is better at optimizing fees, and makes it possible to generate multiple random words in one single request. On the other hand, the direct funding method appears to be better for one-off requests. Also, you do not need to create subscriptions and pre-fund them.


Exercise 2: MakerDAO 2.0 Tokenomics

Part A: Meta assessment of DeFi projects through aggregators

DeFiLlama defines Collateralized Debt Positions (CDP) protocols as protocols that mint its own stablecoins using collateralized lending. There is about 6.8 billion dollars of combined Total Value Locked in this type of protocols, of which there are 173. We can rapidly observe that the most significant of these CDP protocols appears to be MakerDAO (now rebranded as Sky), with a Total Value Locked of nearly 4 billion dollars, and a market cap of 826 million dollars. Naturally, most of its revenue comes from the interest revenues they get from the debt. A very small part of it comes from liquidation revenues, as seen below.



Its closest competitors appear to be Lista DAO, Liquidity (providing 0% interest loans against Ether used as collateral) and Avalon CeDeFi lending protocol. Nevertheless, these protocols are way smaller. For instance, their respective TVL are between 330 to 530 million dollars. Avalon seems to be the second biggest, but not a lot of information are available on DeFiLlama. Thus, let's take a look at the third biggest CDP, Liquidity, that has a TVL of 411 million dollars (knowing that Avalon represents 530 million, thus only 100 million dollars of difference, which is small compared to the difference with Sky). We can now compare it to the metrics of Sky (again, MakerDAO has been rebranded as Sky). Below, you can find numerous metrics comparing the two:

| | |
|---|-----------|
|  MakerDAO (MKR) | |
| Total Value Locked | |
| > \$3,954b | |
| Market Cap | \$826,71m |
| > \$MKR Price | \$938,87 |
| Fully Diluted Valuation | \$851,98m |
| > 24h \$MKR Volume | \$89,32m |
| > \$MKR Liquidity | \$44,3m |
| > Fees (annualized) ⓘ | \$503,17m |
| > Revenue (annualized) ⓘ | \$201,26m |
| > Total Raised | \$54,5m |
| > Annual operational expenses | \$27,66m |

| | |
|--|------------------|
|  Liquity | |
| Total Value Locked | |
| > \$411,57m | |
| Market Cap | \$103,8m |
| > Token Price | \$1,07 |
| Fully Diluted Valuation | \$106,99m |
| > 24h Token Volume | \$43,9m |
| Staked | \$55,91m |
| | (53,87% of mcap) |
| > Fees (annualized) ⓘ | \$2,26m |
| > Revenue (annualized) ⓘ | \$1,01m |
| > Treasury | \$1,97m |
| > Total Raised | \$6m |

As said before, we can see that Sky really appears as a leader in the CDP market. Its fees and revenues are 200 times higher than the ones of Liquidity. Regarding the market cap, it is 8 times bigger than Liquidity. Nevertheless, in the global stablecoin market, Sky is downgraded as a minority player compared to Tether or Circle. These two have a combined TVL of about 195 billion dollars. These off-chain collateralized stablecoins are, as seen in the lectures, a big part of the stablecoin eco-system. Going back to the DAI, it is a stablecoin that is performing correctly. The changes in prices over the last month are similar to the ones provided by USDT (the stablecoin of Tether, which is the biggest player in this market), thus, we could say that it is performing as expected for a stablecoin, meaning, as stated in the name, that its value is stable. Of course, USDT and DAI do not share the same stability mechanisms, but as the goal is the same for both cryptocurrencies, it might be interesting to compare them. You can now upgrade your DAI to USDS as well. Also, you can earn rewards from USDS, with savings rate of about 12%. One could question the ability of Sky to maintain these high savings rates. As a matter of fact, we could think of Ethereum and its switch towards Proof-Of-Stake (POS). To some degree we could say that Sky is opting for a similar strategy. For context, when Ethereum wanted to operate the switch from Proof-Of-Work (POW) to POS, the staking rewards could go up to 17% through some providers. As they wanted to make a full switch, they used this financial incentive to maximize the number of new users and adopters. Again, as seen in class, this is generally how it is done in the DeFi space, as one can only use incentive to operate changes. Hence, Sky is, at least at first glance, using a similar strategy with high savings rate in order to encourage and incentivize the users to upgrade their DAI to USDS (and their MKR to SKY). We will be able to see in the future if this strategy was successful.

Part B: Examining MKR Tokenomics

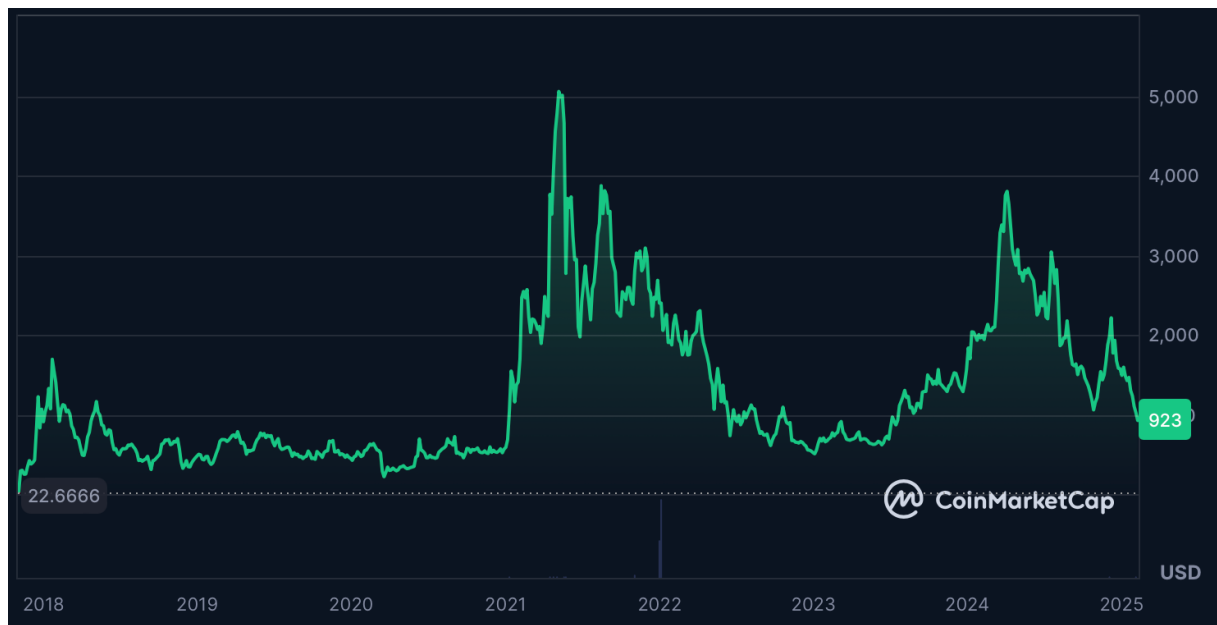
Before analysing the MKR token and its evolution, we should first take a look at the Black Thursday and what it represents. As a matter of fact, in human history, “Black Thursday” has been a recurring expression referring to important (and generally negative) events that happened on a Thursday. The most well-known is probably the Wall Street Crash of

the 24th of October 1929. On another (but no more joyful) note, we could also think of the devastating bushfires that happened in Victoria, Australia on the 6th of February 1851 that destroyed about 5 million hectares. In any case, we generally refer to Black Thursdays when these events are more or less catastrophic. With this in mind, we can now travel back to a more recent period, and more specifically on the 12th of March 2020. On that day, the US stock markets experienced their biggest single-day percentage drop since the 1987 crash. This global market crisis was mainly attributed to the COVID-19 crisis that caused general instability and uncertainty. The DeFi space was not spared from this general crash. Between the 12th and the 13th of March, crypto assets generally experienced drops between 40 to 60%. More specifically, ETH experienced a drop from 193\$ to 95\$ in about 24 hours. This massive descent did not come without consequences. As the network was overwhelmed by the number of transactions (as users reacted), spiking up the gas fees. Additionally, because of these high fees and the congestion of the network, price oracles of MakerDAO failed to update correctly the prices of ETH. Because of this lag, at some point, the prices of ETH given by the oracles suddenly fell drastically, triggering numerous liquidations of collaterals. In some cases, ETH was even sold for free. Hence, the MKR token (the native token of MakerDAO) also experienced a drop of 60% in value during this period. This MKR token is a governance token (enabling the users to vote on the changes applied to the protocol) that generally appreciates when there is an increase in the system surplus. On the other hand, it typically depreciates when MKR tokens are minted to cover losses from liquidations and debt auctions (Koshan and Viswanath-Natraj, 2021). We can now analyse its evolution. Please find below the evolution of the MKR price between January 2020 to May 2020:

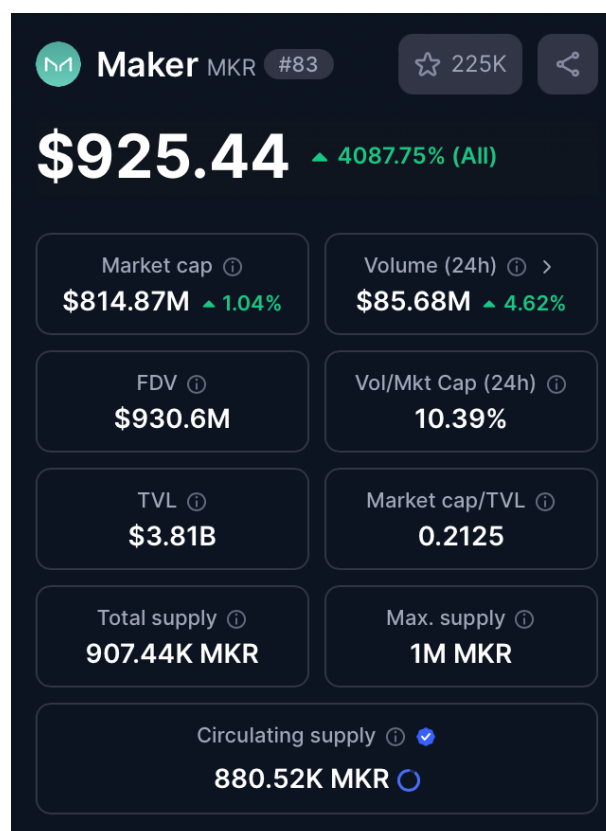


After the events that occurred on the Black Thursday, MakerDAO had to adapt. They revised their risk parameters, as well as their debt ceiling and stability fees. They also upgraded their auction mechanisms to avoid zero bid winnable auctions. In addition to that, they updated their oracle system, in order to limit the risk of delayed information, possibly resulting in drastic price changes.

The story of MakerDAO continues after that. Let's now take a look the price evolution onwards:



The sharp rise in 2021 could simply be explained by a general trend and hype towards the DeFi eco-system at that time. Right now, here are the characteristics of the MKR token:



With a market capitalization of over 800 million dollars, and a circulating supply of 880,520 MRK, taking into account a total supply of 907,440 MKR, the protocol is still

active. Finally, we could look at a table detailing the utility of the MKR token before and after the Black Thursday:

| | <i>Before Black Thursday</i> | <i>After Black Thursday</i> |
|-------------------------------|--|--|
| Governance | Giving the possibility to holders to participate in the governance, vote on the evolution of the protocol. | In the continuity, with the same perspective, accentuating the importance of risk management and system resilience. |
| Stability Mechanism | Used in surplus auctions to buy and burn tokens (the latter reducing the supply), in order to maintain the stability of the DAI. | Use of debt auctions in which MKR is minted, then sold to cover losses, thus giving an incentive to holders to manage their risks correctly. |
| Collateral Liquidation | Indirectly involved through governance and stability mechanism. | Improvements in the liquidation process in order to prevent zero-bid or minimal auctions, hence protecting the integrity of the system. |

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

As said before, Sky is the new name chosen for the rebranding of MakerDAO. Alongside a new governance token, the SKY, a new stablecoin is also implemented, the USDS. This whole move is part of MakerDAO's Endgame, of which the goal is to improve governance and ensure a truly decentralized structure. More specifically, they aim at improving resilience and scalability. Through Skylink, the goal is to reach other blockchains as well. In this plan, there is a will to integrate Artificial Intelligence (AI) in the governance process. In spirit, according to the founder, the goal is to distance themselves from the idea of having one single entity that claims to manage a decentralized system, as they do not consider it to be sustainable and possible in the long run. We observe the introduction of Stars, which are SubDAOs that can operate independently while still being connected to the Sky's protocol. These Stars will each be able to have their own tokens, rules, governances and communities. Even though the group announced that MKR and DAI would still be available, users are questioning the viability of these tokens. In fact, we go back to what was mentioned earlier with the comparison with the switch from POW to POS of Ethereum. It is surely a wish of the team to see their new project experience a mass adoption. As a matter of fact, the team also proposes Sealed Activation in order to lock-in users behind an exit fee in exchange for a reward. The latter corresponds to 25% of the stablecoin surplus of the protocols for sealed MKR and SKY holders. This again aims at incentivizing the adoption by new users. More on the practical side of things, USDS functioning is fairly similar to the DAI, except for some optimization of gas usage. Furthermore, holders of USDS will be able to claim Sky Saving Rate (SSR), like the Dai

Saving Rate (DSR), and Sky token rewards. For SKY, it is less comparable to MKR in the sense that more rewards come with the token. Also, as a governance token enables a community to take part in the evolution of a project, and the two projects are not of the same scale, the participation and incentives to participate to the projects differ. SKY appears to be linked to a larger vision, with a bigger potential target. It might be important to note that these rewards won't be available everywhere due to different legislations. In a nutshell, the objective seems to be to build a sort of raw and base layer over which independent protocols can establish truly decentralized tools and solutions. If done correctly, a well-built framework for decentralized governance could really help the advancement of the goals embodied by the DeFi space right now. As the latter is intricately dependent on the blockchain evolution, we could think of multiple areas of evolution. For instance, a parallel progress could be found in the AI field. It is possible for these two technologies to find a symbiosis-like balance as they could be compatible, each bringing solutions to each other's challenges. For example, one could think of the transparency brought by the blockchain technology into the data treatment of Large Language Models (LLM), and the algorithms provided by AI companies could be used to ensure the optimization and quality of smart contracts and software in general. Another potentiality of growth of blockchains could be implemented through the development of quantum computing. We should keep in mind that with this development, the security of blockchains provided by asymmetric cryptography could be, to some extent, threatened. Two main threats are posed, both due to the enormous computing power of quantum computing. Firstly, it could lead to a centralization of mining power, which could impact POW-powered blockchains. Moreover, it could enable malicious actors to decrypt private keys from public keys, which would be a huge security problem. Nevertheless, developers have already been working on quantum-resistant cryptography techniques. One could think of Quantum Key Distribution (QKD) as well as Quantum Secure Multi-Party Computation (QSMPC). In addition to that, this technology could in fact be used to further improve blockchain technology. For instance, it could be used to have more efficient and secure consensus mechanisms. Hence, we could tend towards consensus faster, and in a more secure way, more resistant and resilient to attacks. Furthermore, it could help scale blockchains even more, while optimizing their energy consumption and transaction time.