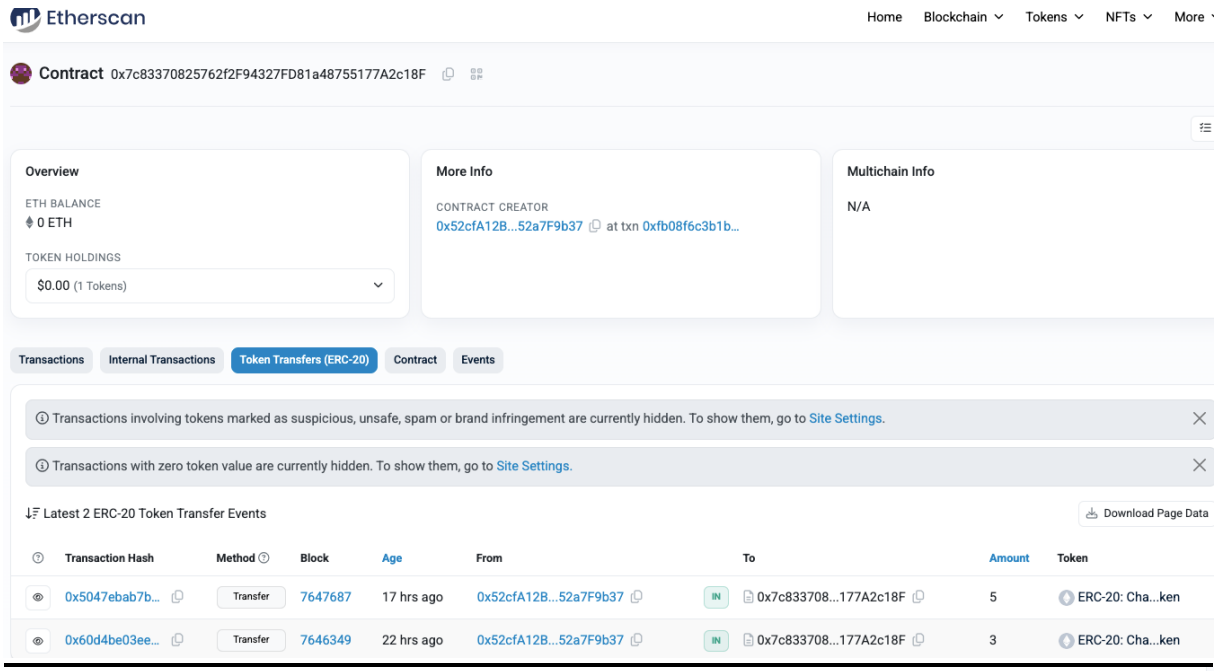
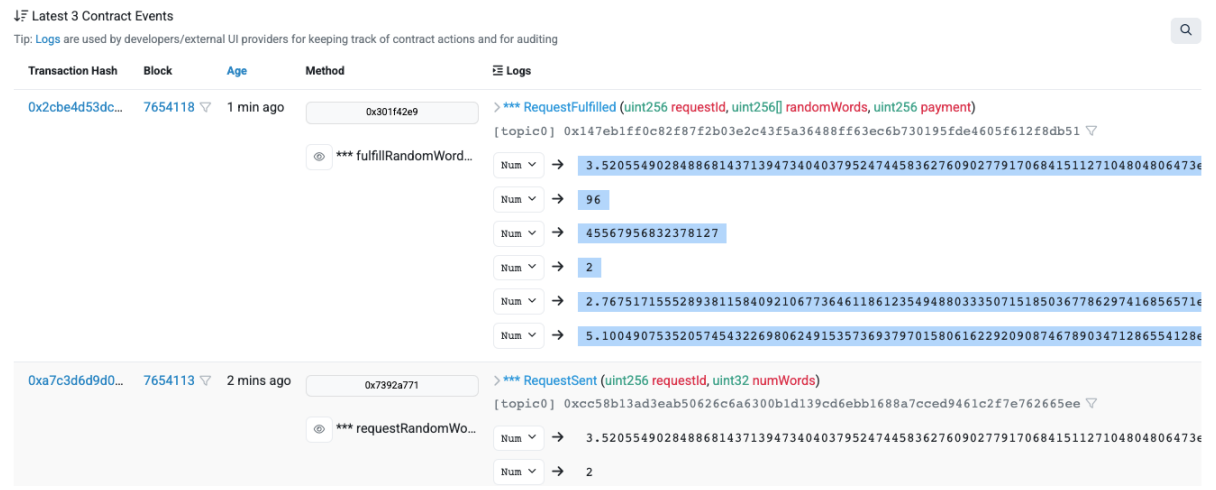
Exercice 1 :PART A

- Two screenshots showing the two events on Etherscan. One with Hex values and one with number values.





- What were the 2 random numbers the oracle generated for you?

The two random numbers generated were (as seen in the screenshot) :

- 96
- 45567956832378127

- RequestSent returns 2 fields and RequestFulfilled returns 6 fields. Explain what information each of these fields conveys. 1 point for RequestSent and 2 points for RequestFulfilled.

In chain link VRF and oracle-based request response mechanisms: “request send” and “request fulfilled” are essential events to keep tabs on the randomness requests evolution.
“Request send” returns two fields :

1. Request Id: It is a unique identifier for the randomness request assigned from the start of the process to track the request throughout it .
2. Numwords: The number of random values requested by the requester from the Chainlink VRF.

“Request fulfilled” returns six fields :

1. Request Id: It is a unique identifier for the randomness request assigned from the start of the process to track the request throughout it .
2. RandomWords: Array of random numbers generated by chainlink VRF. (2nd and 3rd line are generated random numbers)
3. NumWords confirmation : in our case we have 2 meaning it successfully generated two random numbers which matches the requestsent.
4. Paid: Cost of fulfillmentmeaning how much gaz fee or LINK was spent to achieve the randomness request. (2 last lines)

Part C - Contrast data serving methods (1 point)

The two data serving approaches are : the direct funding method in which each request is paid for using Link, appropriate for rare occurrences: for example single event decisions which only require one time randomness. The subscription method on the other hand, is based on a shared link funded account which can deal with multiple contracts.
In opposition to the direct funding method, the subscription one is better at fund management and reducing gaz costs thus more appropriate for events like lotteries and NFT minting which require more randomness needs.

Exercice 2 :

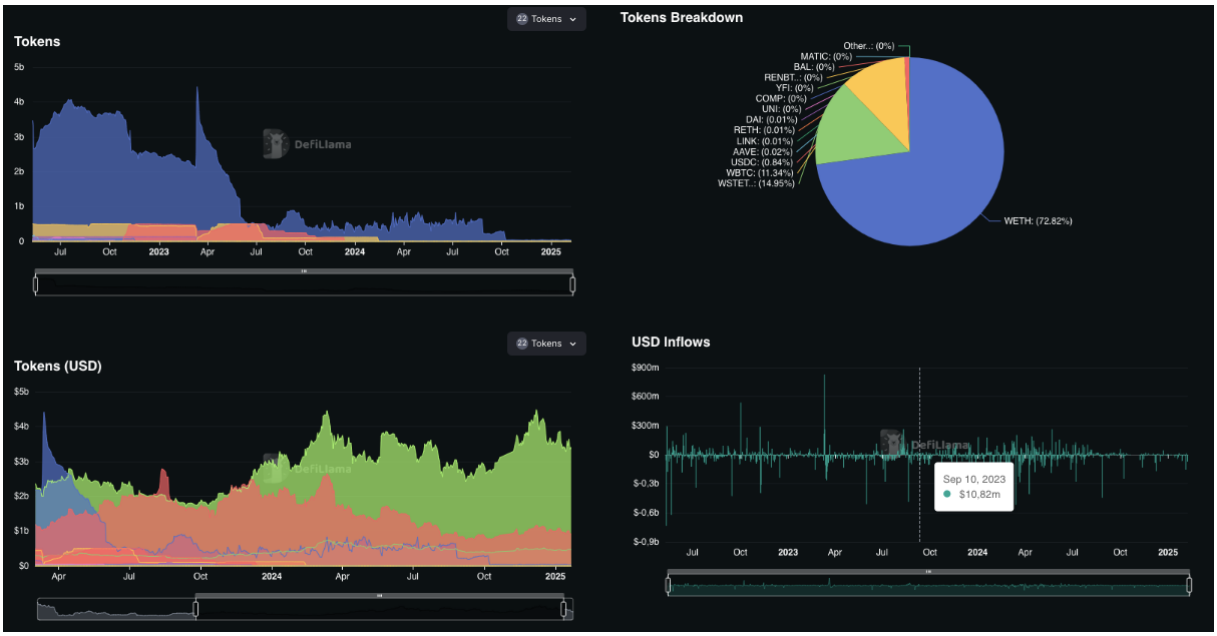
Part A - Meta assessment of DeFi projects through aggregators (3 points)

CDPs short for collateralized debt positions are necessary in the decentralized finance world as they allow generating stable coins through the locking of assets as collateral.

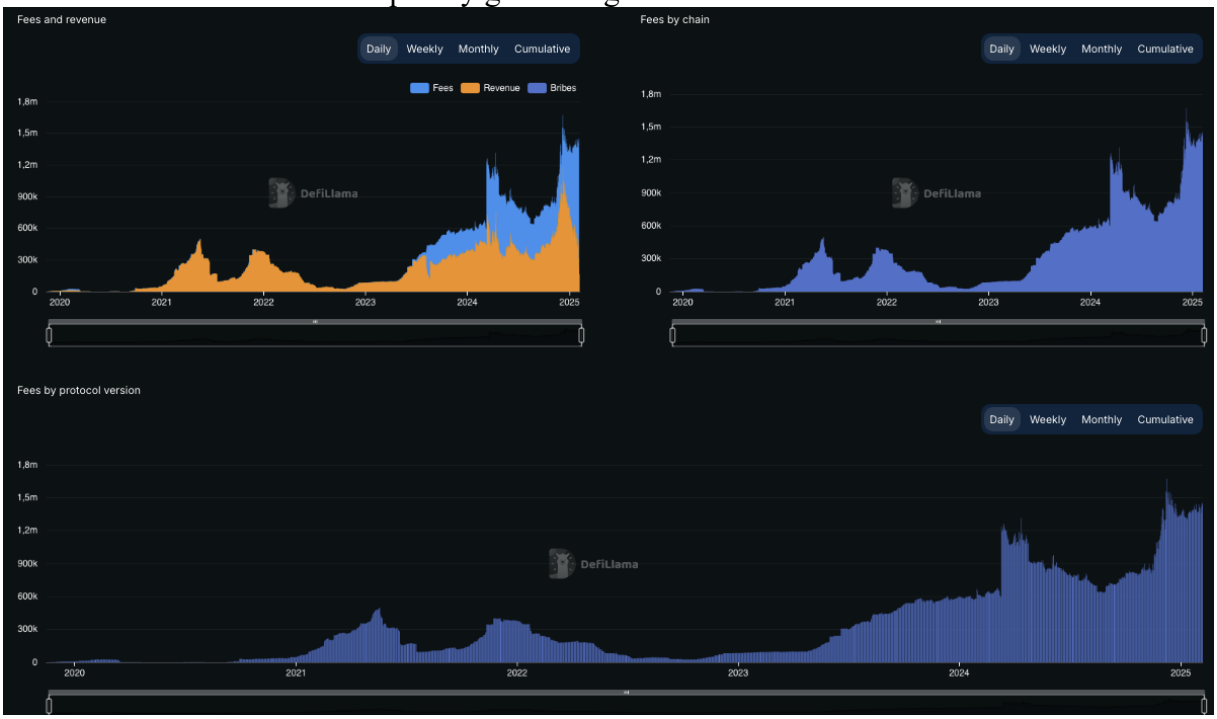
Some examples of the known defi protocols offering CDP services with each their own processes: MakerDao, liquidity, curve finance Davos and Ramp with MakerDao being one of the earliest adopters.

The Defi landscape is continuously growing with ethereum as the leader blockchain for these Defi activities.
Looking at DefiLlama, we find that ethereum's total value locked is about 56.6 billion $ which shows their ruling in the sector. But what is total value locked ?
It is a defi protocol assessing metric showcasing how much a platform is used and trusted through their total capital deposited into smart contracts.
Another key metric that could be used is annual percentage yield which measures as its name entails the annualized returns users profit from staking and lending assets in the protocol.

As of today, using Defi llama reports we can rank protocols based on their TVL such that MakerDao comes first with 3.978 billion $ TVL, followed by Avalon USDa with 540.69 million $ TVL and liquidity V1 in 3rd position with 333.58 million $ TVL.



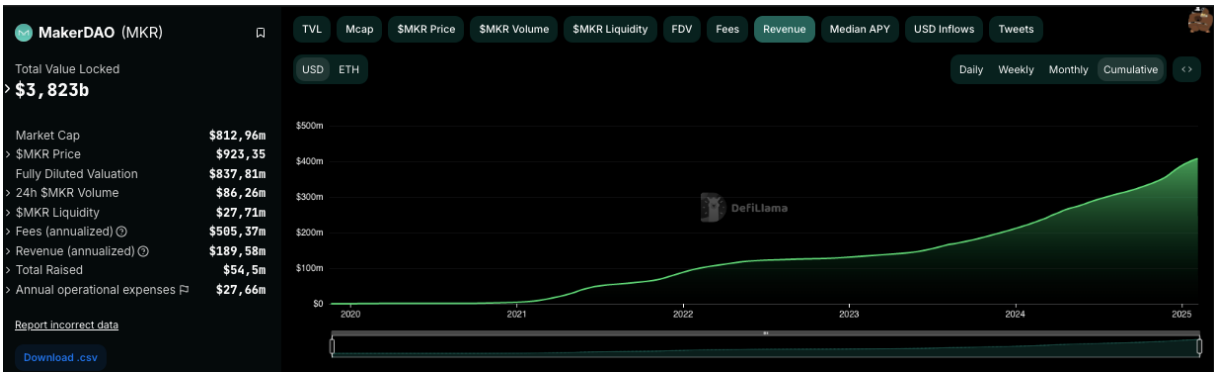
This ranking makes sense as MakerDao possesses a robust protocol based automated liquidation (gains from liquidation penalties) and on fees stability which acts as interested rates on borrowed DAI consequently generating revenue for MakerDao.



Let’s dig deeper on MakerDao success understanding its stable coin DAI and how it performs:

DAI MakerDao’s decentralized stable coin is their main successful innovation.
Dai combines strategies like over collateralization, market arbitrage, minting or burning processes to be soft pegged to the us $.

In this dune analytics graphic, we can see that the DAI adoption has steadily grown strengthening MakerDao 's well established reputation. Indeed, thanks to this type of profitable stable coin, the defi ecosystem as a whole including its stability, liquidity provision and arbitrage opportunities, is enhanced.
About MakerDao's liquidity threshold, it is set to 150% meaning that's user's collateral gets liquidated as soon as it falls below this ratio which is quite attractive to liquidators as they get a lot of gain opportunities from these discounted liquidated assets.



Through the analysis of dune analytics and Defi Llama data, we can say that the CDP market continues to be very competitive with Maker Dao dominating in tvl, revenue but also in its stable coin issuance:
Indeed, Makerdao exceeds its competitors (liquidity, crvUSD,…) in terms of tvl with 3.978 billion $ thanks to its stability fees revenues which contributed over 2.46 million $ in the last 30 days alone.
Dai its stablecoin is circulating more and more translating more and more adopters.
Finally, its market dynamic's liquidation creating gain opportunities ensuring DAI's stability plays a major role in its continuous growth.
All of this allowing MakerDao to dominate in the field align perfectly with the principles of risk management, token design and finance metrics studied in class during lecture 5.

Part B - Examining MKR tokenomics (3 points)

The event which occurred on march 12th 2020 “Black Thursday” marked the whole crypto market which experienced the worst downturn with ether’s value getting cut by half in only one day. This 50% loss of ETH in one day badly impacted MakerDao because it relies on ETH as its primary collateral which led to multiple collateralized debt positions’ liquidation, thus, giving rise to unbacked Dai threatening the protocol stability (about 4.5 million $ of unbacked DAI).
Let’s look at the beginning of 2020: the MKR token’s price was 500$ to 600$.
However, after this downturn event, its price decreased significantly to 200$.
This is because the black Thursday also had catastrophic effects on the market’s confidence within MakerDao’s risk management.
MKR succeeded in rebounding immensely after working on its vices and improving itself making it stand at more than 2500$ in early 2021 already and exceeding it afterwards reaching its peak at 6300$ in May to be exact.
Black Thursday episode exposed Maker Dao’s first design weaknesses and forced to enhance it.
Focusing now on the improvements implemented which helped recover from the crisis but also prevent future failures, we notice three main changes:
First, regarding its debt auctions, new MKR tokens are minted and sold to solve the unpacked DAI issue so there is no more insolvency.
This restored the protocol by increasing MKR supply and decreasing temporarily its value.
Second, it adjusted it system parameters by implementing higher collateralization rations to prevent volatility. In the same sense, it continuously adjusted their stability fees so that it is more sensitive to market changes.
Third, it expanded its collateral types. Indeed, because MakerDao relied heavily on ETH as its number one collateral, It was decided to add new assets such as usdc or wbtc or other stable coins to reduce this heavy reliance that proved was not the right choice when it collapsed on black Thursday.

Part C - Personal reflection on the current and future state of MakerDAO (2 points)

From MakerDao to Sky, the protocol decided to rebrand in august 2024 introducing new tokens (the usdc token and the sky governance token) providing the users more alternatives to exchange their DAI or MKR tokens for USDS and SKY tokens as now each MKR token is convertible into 28000 SKY tokens although the initial tokens.
The old tokens still are in circulation with the newer ones allowing the users to choose between the two.
This MakerDao to Sky rebranding along with the modified tokenomics and the newer token improved features was an important step in their EndGame plan to better the protocol’s security, scalabilty and overall performance.This strategy’s main goal is to increase the protocol adoption but also boost its flexibility in the evolving Defi world.
Furthermore, with the rapid growth of AI and quantum computing, protocols like SKY can take advantage of these technologies advantages if designed and organized correctly.
For instance, AI can help optimize protocol’s processes becoming more efficient thanks to well predicted market trends and bettering security through better predictive analysis or enhanced fraud detecting models.
However, these protocols should be aware of the potential dangers of quantum computing which could easily break the cryptographic algorithms ensuring the blockchain’s security.

Therefore, these protocols need to anticipate these risks and build quantum resistant cryptographic algorithms and find better suited solutions for this emergent issue to be mitigated thus maintaining security.

Sky - Balance Sheet - Yearly

Yearly BS since 2020, in DAI

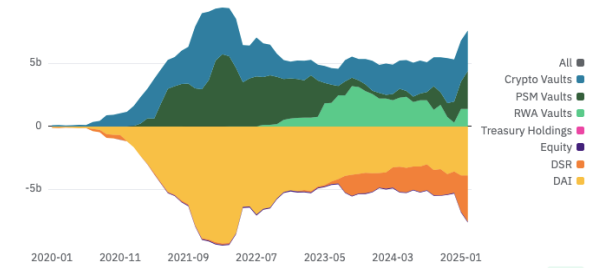
item	2025 YTD	2024	2023	2022	
Assets	7,597,410,340	5,323,462,605	5,221,623,914	5,139,467,166	9,099
Crypto Vaults	3,199,473,899	3,338,079,321	2,380,440,019	1,315,371,585	5,419
PSM Vaults	2,996,707,970	1,682,620,128	260,424,144	3,183,945,519	3,661
RWA Vaults	1,399,529,460	300,712,202	2,580,107,213	639,568,366	17
Treasury Holdings	1,699,011	2,050,954	652,538	581,695	1
Liabilities	7,530,206,450	5,253,897,113	5,168,577,458	5,064,027,420	9,033
Dai Saving Rate (DSR)	3,653,794,856	1,696,488,002	1,465,943,820	2,012,554	91
Dai in Circulation	3,876,411,594	3,557,409,111	3,702,633,639	5,062,014,866	8,942

11 rows Search...

@steakhouse ··· 14h

Sky - Balance Sheet - Monthly

Monthly BS since 2020, in DAI



@steakhouse ··· 14h