César Denost

M2DE

Solidity and Smart contracts

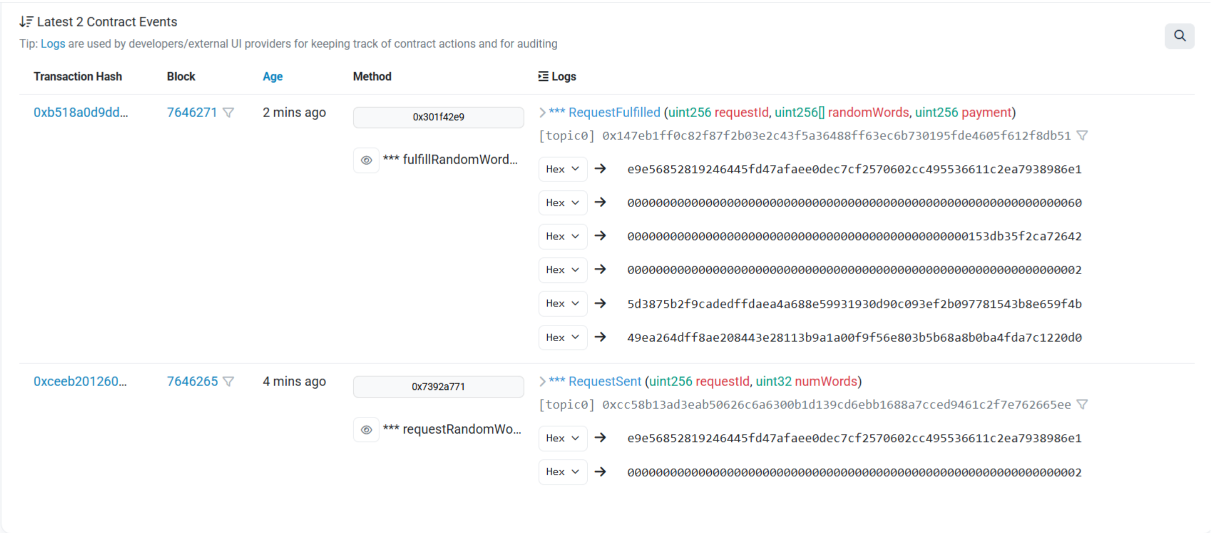
Homework 3

SUMMARY

Exercice 1 :

PART A :

Hex Values Events :

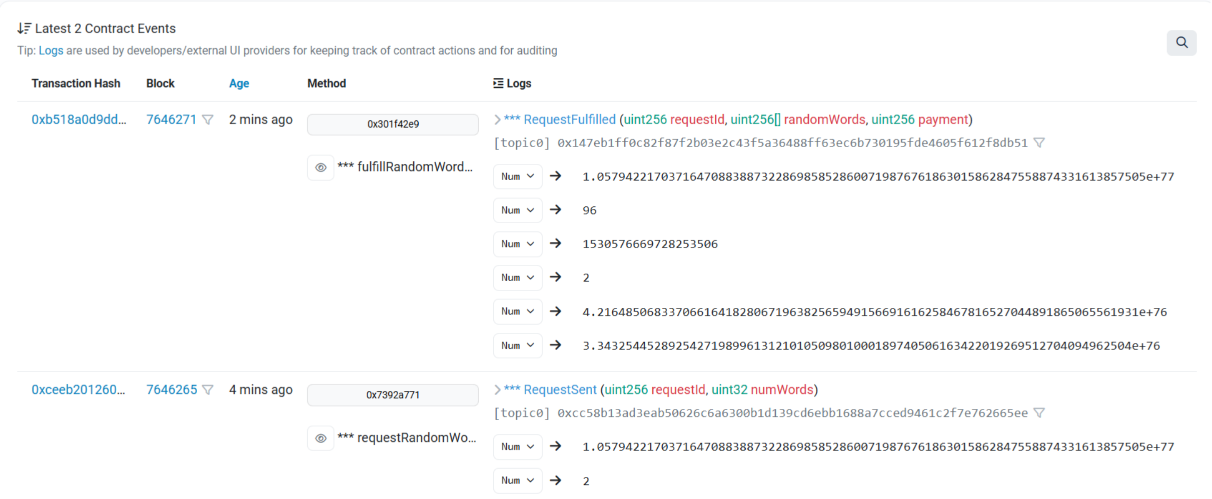


↓☰ Latest 2 Contract Events

Tip: Logs are used by developers/external UI providers for keeping track of contract actions and for auditing

Transaction Hash	Block	Age	Method	☰ Logs
0xb518a0d9dd...	7646271 ▽	2 mins ago	0x301f42e9 👁 *** fulfillRandomWord...	> *** RequestFulfilled (uint256 requestId, uint256[] randomWords, uint256 payment) [topic0] 0x147eb1ff0c82f87f2b03e2c43f5a36488ff63ec6b730195fde4605f612f8db51 ▽ Hex ⌄ → e9e56852819246445fd47afaee0dec7cf2570602cc495536611c2ea7938986e1 Hex ⌄ → 0000000000000000000000000000000000000000000000000000000000000060 Hex ⌄ → 000000000000000000000000000000000000000000000000153db35f2ca72642 Hex ⌄ → 0000000000000000000000000000000000000000000000000000000000000002 Hex ⌄ → 5d3875b2f9cadedffdaea4a688e59931930d90c093ef2b097781543b8e659f4b Hex ⌄ → 49ea264dff8ae208443e28113b9a1a00f9f56e803b5b68a8b0ba4fda7c1220d0
0xceeb201260...	7646265 ▽	4 mins ago	0x7392a771 👁 *** requestRandomWo...	> *** RequestSent (uint256 requestId, uint32 numWords) [topic0] 0xcc58b13ad3eab50626c6a6300b1d139cd6ebb1688a7cced9461c2f7e762665ee ▽ Hex ⌄ → e9e56852819246445fd47afaee0dec7cf2570602cc495536611c2ea7938986e1 Hex ⌄ → 0000000000000000000000000000000000000000000000000000000000000002

Num Values Events:



↓☰ Latest 2 Contract Events

Tip: Logs are used by developers/external UI providers for keeping track of contract actions and for auditing

Transaction Hash	Block	Age	Method	☰ Logs
0xb518a0d9dd...	7646271 ▽	2 mins ago	0x301f42e9 👁 *** fulfillRandomWord...	> *** RequestFulfilled (uint256 requestId, uint256[] randomWords, uint256 payment) [topic0] 0x147eb1ff0c82f87f2b03e2c43f5a36488ff63ec6b730195fde4605f612f8db51 ▽ Num ⌄ → 1.05794221703716470883887322869858528600719876761863015862847558874331613857505e+77 Num ⌄ → 96 Num ⌄ → 1530576669728253506 Num ⌄ → 2 Num ⌄ → 4.2164850683370661641828067196382565949156691616258467816527044891865065561931e+76 Num ⌄ → 3.343254452892542719899613121010509801000189740506163422019269512704094962504e+76
0xceeb201260...	7646265 ▽	4 mins ago	0x7392a771 👁 *** requestRandomWo...	> *** RequestSent (uint256 requestId, uint32 numWords) [topic0] 0xcc58b13ad3eab50626c6a6300b1d139cd6ebb1688a7cced9461c2f7e762665ee ▽ Num ⌄ → 1.05794221703716470883887322869858528600719876761863015862847558874331613857505e+77 Num ⌄ → 2

The 2 random numbers generated (in Hexadecimal then in Number format):

Hexadecimal format:

- `5d3875b2f9cadedffdaea4a688e59931930d90c093ef2b097781543b8e659f4b`
- `49ea264dff8ae208443e28113b9a1a00f9f56e803b5b68a8b0ba4fda7c1220d0`

Number format:

- `4.21648506833706616418280671963825659491566916162584678165270448918650655 61931e+76`
- `3.34325445289254271989961312101050980100018974050616342201926951270409496 2504e+76`

1) RequestSent (uint256 requestId, uint32 numWords):

The `RequestSent` event is emitted when a random number request is made.

The fields are:

requestId (uint256):

- `0xe9e56852819246445fd47afaee0dec7cf2570602cc495536611c2ea7938986e1`

This field represents the unique identifier for the request. It is a static parameter of type uint256 that directly encodes the request ID.

uint32 numWords:

- `0000000000000000000000000000000000000000000000000000000000000002`

This field indicates the number of elements in the randomWords array. In this example, the value 2 means that there are two random words in the array.

2) RequestFulfilled (uint256 requestId, uint256[] randomWords, uint256 payment):

The `RequestFulfilled` event is mainly used to notify that the random number request has been processed and completed by the oracle (e.g. Chainlink VRF).

The fields are:

requestId (uint256):

- `0xe9e56852819246445fd47afaee0dec7cf2570602cc495536611c2ea7938986e1`

This field represents the unique identifier for the request. It is a static parameter of type uint256 that directly encodes the request ID.

randomWords (uint256[]):

- `0x0000000000000000000000000000000000000000000000000000000000000060`

Since randomWords is a dynamic array, the ABI encoding does not store its contents directly in the static section. Instead, this field provides the offset (in bytes from the start of the encoding) to where the dynamic data for randomWords is located. Here, 0x60 (or 96 in decimal) indicates that the dynamic part starts 96 bytes from the beginning.

payment (uint256):

- `000000000000000000000000000000000000000000000000153db35f2ca72642`

This field holds the payment amount for the request. It is also a static parameter and directly encodes the payment value as a uint256.

Length of the randomWords array (uint256):

- `0000000000000000000000000000000000000000000000000000000000000002`

This field indicates the number of elements in the randomWords array. In this example, the value 2 means that there are two random words in the array.

First element of randomWords (uint256):

- `5d3875b2f9cadedffdaea4a688e59931930d90c093ef2b097781543b8e659f4b`

This field encodes the first random word generated by the request. It is a uint256 value represented in hexadecimal.

Second element of randomWords (uint256):

- `49ea264dff8ae208443e28113b9a1a00f9f56e803b5b68a8b0ba4fda7c1220d0`

This field encodes the second random word generated by the request. Like the first, it is a uint256 value.

PART C:

The direct funding model requires every request for randomness to be paid for directly through the consumer contract's own balance of LINK tokens. In other words, every call from a contract for a random number needs to have enough funds on it to cover such a request. It is better suited for low-frequency or smaller-scale applications where requests are infrequent. On the other hand, the subscription model pools the funds into one common pool from which several contracts or requests may draw. This approach will be perfect for high-volume scenarios or multi-contract situations because the aggregation of payments will make management of funds easier, reduce funding of each request individually, and can simplify billing across many requests.

Exercise 2

PART A:

MakerDAO was one of the most influential and earliest DeFi protocols, and to date remains one of the key players in the CDP market. Nowadays, however, it is highly competitive. Using DeFiLlama and Dune Analytics together, we can see that MakerDAO is looking at protocols such as Liquity, Curve Finance, and Ramp, each of which uses various collateral types, liquidation mechanisms, and stability fees.

In Graph1, taken from DeFiLlama, maps the TVL across the CDP category. MakerDAO consistently holds a significant share of the TVL-over 40% in some recent snapshots-which underlines its deep liquidity and market confidence. This metric, along with the protocol's stablecoin supply, DAI, provides key insights into the health and adoption of MakerDAO relative to its peers. A second informative metric from lecture 5, the liquidation volume, also has a place on DeFiLlama. MakerDAO's liquidation volume stands high, both a reflection of the scale of its CDP base and of the intrinsic volatility risks arising from ETH as collateral.

More granular insights come from Dune Analytics dashboards. In a dashboard custom-built for the purpose shown in Graph 2, it is possible to trace how CDP openings and liquidations have varied over time. This dashboard shows the user activity of MakerDAO, underlining that while new protocols have grown rapidly, the MakerDAO user base remains strong and stable. Another metric is the average collateralization ratio that gives insight into risk management: MakerDAO normally keeps its average collateralization ratio above the minimum requirement, hence CDP owners have been over-collateralizing their positions to adapt to market stress. In contrast to that, some competitors use different risk buffers and liquidation penalties; for example, Liquity targets users with larger or smaller risk appetites.

In general, these aggregators confirm that MakerDAO is the leader in both TVL and market share but also in terms of standard setting with regards to risk management in the CDP market segment. Stable performance of DAI, combined with large TVL and controlled liquidation volume, testifies to a mature ecosystem. Competitors may be fast on innovation for alternative collateral and low liquidation penalties, but legacy and governance-driven improvements in MakerDAO are very strong to help it further consolidate its position in the market. With comprehensive historical data and clear governance, and with protocol improvements in process, Maker positions itself as a pioneer and survivor of the CDP space.

Coupled with metrics such as TVL, liquidation volume, and average collateralization ratio, these charts underpin the growth of the CDP market and place MakerDAO in the center among its competitors.

PART B:

The MKR token has undergone a number of changes in terms of valuation and structural function since Black Thursday. Going into the event, MKR was primarily a governance token whose role in the system's risk management was, at best, ambiguous. A dramatic market downturn on Black Thursday revealed weaknesses in the protocol's risk parameters; substantial losses were taken, and the system destabilized. MakerDAO subsequently overhauled its mechanism-rebranding SAI to DAI and reimagining MKR's role as both a governance and recapitalization token.

Changes after Black Thursday were aimed at aligning MKR's value better with the health of the Maker ecosystem. Today, this token represents direct recourse for system recapitalization; thus, MKR holders equally share in the risk and reward related to the protocol stability measures. This has helped bring in a more disciplined approach toward risk management and better confidence among participants, slowly recovering MKR's market value on CoinMarketCap.

Here are the utility of MKR before and after the Black Thursday :

Utility Aspect	Before Black Thursday	After Black Thursday
Governance Role	Primarily voting rights with less direct impact	Enhanced governance with explicit risk control
Recapitalization Utility	Implicit safety mechanism	Explicitly used to recapitalize the system
Risk Alignment	Limited direct link to protocol stability	Directly tied to protocol health and risk management
Market Perception	Viewed as a speculative governance token	Considered a critical component for protocol recovery

These changes have helped to stabilize MKR’s market performance and align incentives between MKR holders and the overall stability of th eMArket system.

PART C:

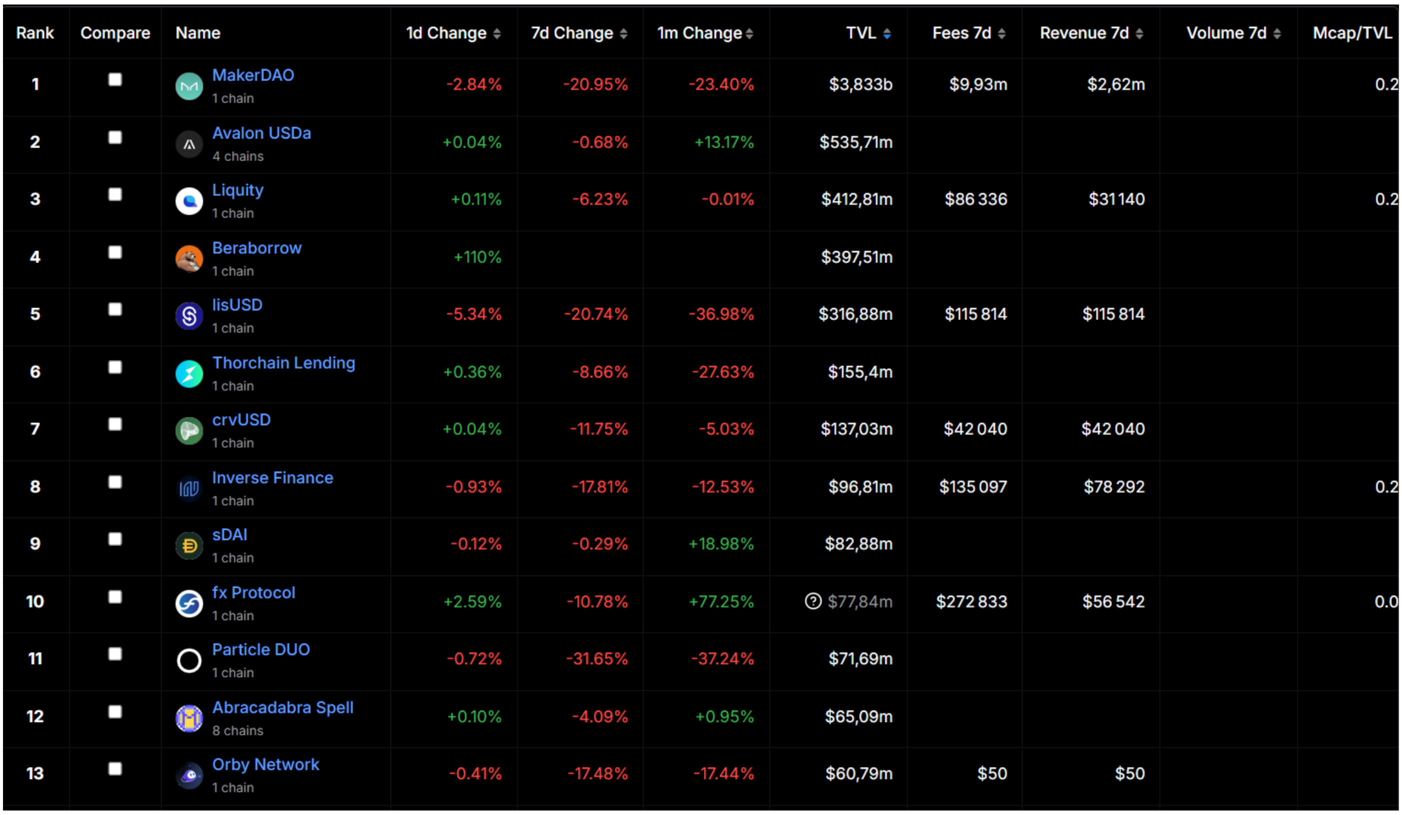
In my mind, the development road that MakerDAO has traveled reflects bigger signs of maturation within DeFi protocols. Maker's rebranding as "Sky" is not cosmetic in name but a paradigm change toward more transparency and better risk management. Its migration to MakerDAO 2.0 introduced explicit recapitalization mechanisms that have made the protocol resilient. New tokenomics for SKY will be better aligned in terms of incentives among all stakeholders, where those governing and supporting the system are also directly responsible for the stability of it.

After the turbulence created on Black Thursday-perhaps due to the poor risk parameters that almost collapsed the entire system-this change became inevitable. By reimagining MKR this way, MakerDAO built a much healthier safety net to protect not just the users but also significantly bolstered confidence among institutional and retail participants. The superior governance model will have better risk control and collateralization practices in place, setting it up to hold its leading edge in the more competitive CDP space.

If looking ahead, both AI and quantum computing are inevitable technologies that will affect blockchain protocols. While AI does enhance real-time risk modeling and decision-making, there are some quantum security challenges against which protocols would need to be prepared. Further evolution of MakerDAO, as with the transition to Sky+, speaks to resiliency and innovation. MakerDAO-better said, Sky-is going to continuously read the writing on the wall, remaining a leader in the DeFi segment through these changes in technology and shifting market dynamics.

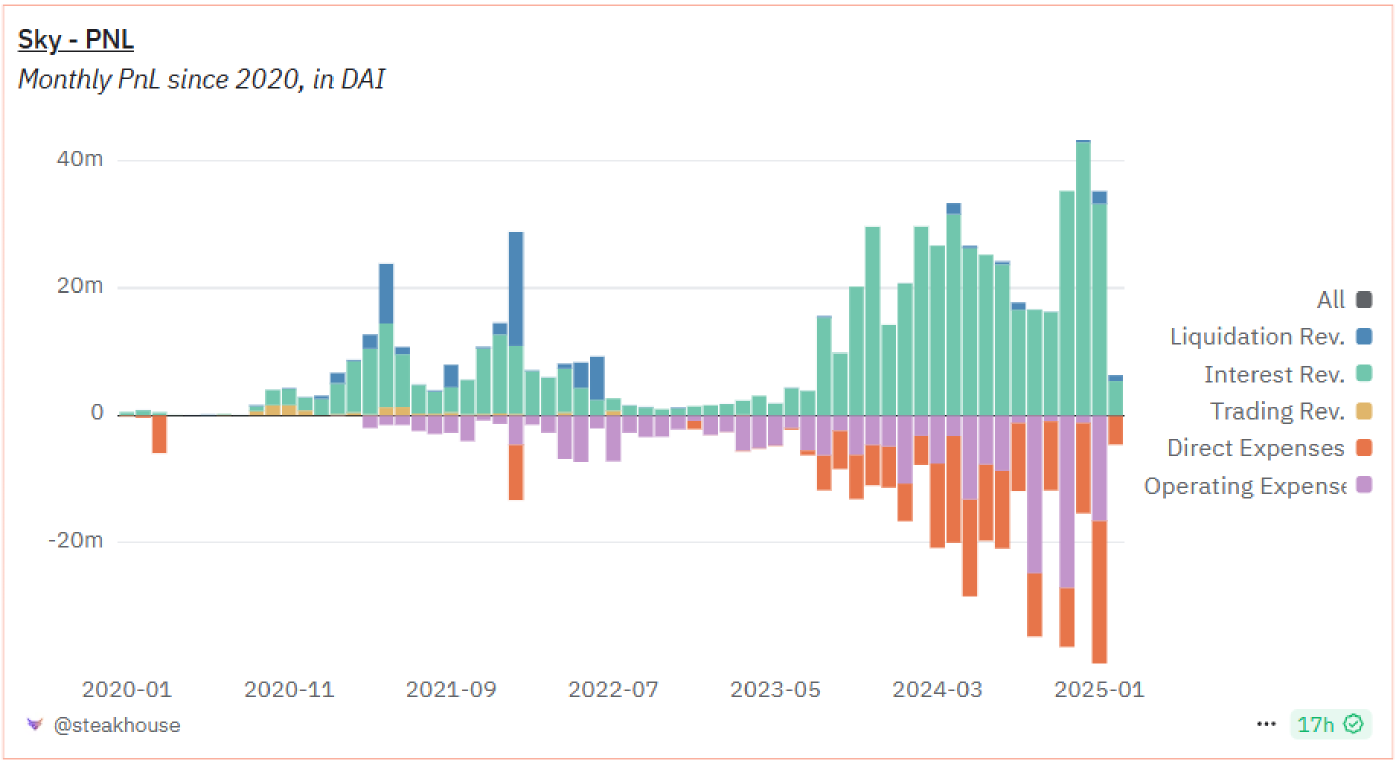
Appendix

Graph 1 : TVL Distribution among CDP Protocols



Rank	Compare	Name	1d Change	7d Change	1m Change	TVL	Fees 7d	Revenue 7d	Volume 7d	Mcap/TVL
1	☐	MakerDAO 1 chain	-2.84%	-20.95%	-23.40%	$3,833b	$9,93m	$2,62m		0.2
2	☐	Avalon USDa 4 chains	+0.04%	-0.68%	+13.17%	$535,71m				
3	☐	Liquity 1 chain	+0.11%	-6.23%	-0.01%	$412,81m	$86 336	$31 140		0.2
4	☐	Beraborrow 1 chain	+110%			$397,51m				
5	☐	lisUSD 1 chain	-5.34%	-20.74%	-36.98%	$316,88m	$115 814	$115 814		
6	☐	Thorchain Lending 1 chain	+0.36%	-8.66%	-27.63%	$155,4m				
7	☐	crvUSD 1 chain	+0.04%	-11.75%	-5.03%	$137,03m	$42 040	$42 040		
8	☐	Inverse Finance 1 chain	-0.93%	-17.81%	-12.53%	$96,81m	$135 097	$78 292		0.2
9	☐	sDAI 1 chain	-0.12%	-0.29%	+18.98%	$82,88m				
10	☐	fx Protocol 1 chain	+2.59%	-10.78%	+77.25%	? $77,84m	$272 833	$56 542		0.0
11	☐	Particle DUO 1 chain	-0.72%	-31.65%	-37.24%	$71,69m				
12	☐	Abracadabra Spell 8 chains	+0.10%	-4.09%	+0.95%	$65,09m				
13	☐	Orby Network 1 chain	-0.41%	-17.48%	-17.44%	$60,79m	$50	$50		

Graph 2: CDP Openings and Liquidation Trends


Sky - PNL
Monthly PnL since 2020, in DAI
40m
20m
-20m
All
Liquidation Rev.
Interest Rev.
Trading Rev.
Direct Expenses
Operating Expense
@steakhouse
17h