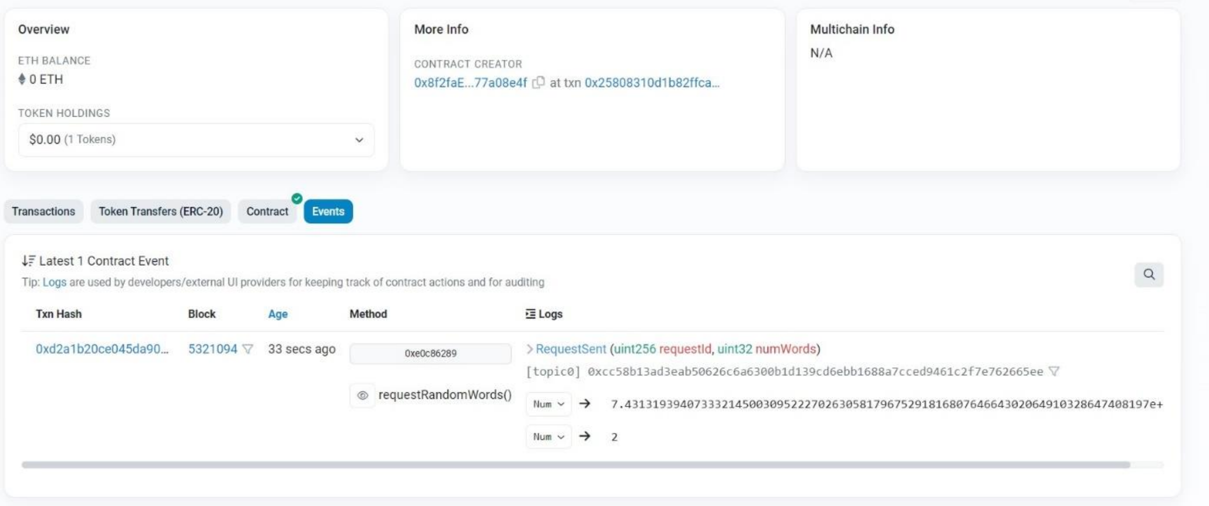
Homework 3: exercise 1: VRF Oracle

Part A - Exploring direct funding VRF



Overview

ETH BALANCE
0 ETH

TOKEN HOLDINGS
$0.00 (1 Tokens)

More Info

CONTRACT CREATOR
0x8f2faE...77a08e4f at txn 0x25808310d1b82ffca...

Multichain Info
N/A

Latest 1 Contract Event

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

Txn Hash	Block	Age	Method	Logs
0xd2a1b20ce045da90...	5321094	33 secs ago	0xe0c86289 requestRandomWords()	RequestSent (uint256 requestId, uint32 numWords) [topic0] 0xcc58b13ad3eab50626c6a6300b1d139cd6ebb1688a7cced9461c2f7e762665ee Num → 7.43131939407333214500309522270263058179675291816807646643020649103286474081 97e+ Num → 2

Part B - Adding a VRF oracle to coinflip

https://github.com/nathcc/Coinflip-VRF

Part C - Contrast data serving methods

The landscape of Verifiable Random Function (VRF) services offers two distinct approaches: direct funding and the subscription method. With direct funding, consumer contracts pay for each random number request, ensuring precise control over costs on a per-request basis. This method suits scenarios where randomness needs are occasional, allowing contracts to manage expenses efficiently. On the other hand, the subscription method streamlines the process by pre-paying for a set number of requests or a subscription period upfront. Contracts that demand frequent or continuous access to random values benefit from this approach, as it simplifies payments and guarantees uninterrupted service. Ultimately, the choice between direct funding and the subscription method hinges on the specific requirements and usage patterns of the application leveraging VRF services.

Part D - Reflect on the currect state of Blockchain

In the realm of blockchain, the cost per random number request can vary based on factors like network activity and gas prices, ranging from a few dollars to dozens ones. Before starting, businesses must ensure they have sufficient funds to cover initial contract funding, whether through a subscription model or pay-as-you-go approach. From a user standpoint, the experience can differ based on the chosen funding method. With direct funding, users need to have wallet funds to cover gas fees per request, whereas a subscription model offers a smoother experience upfront. As blockchain technology continues to evolve, striking a balance between scalability, decentralization, and cost efficiency remains a key challenge. Advancements in scalability solutions, gas fee reduction, and interoperability could propel blockchain towards a future of enhanced user experience and broader adoption.

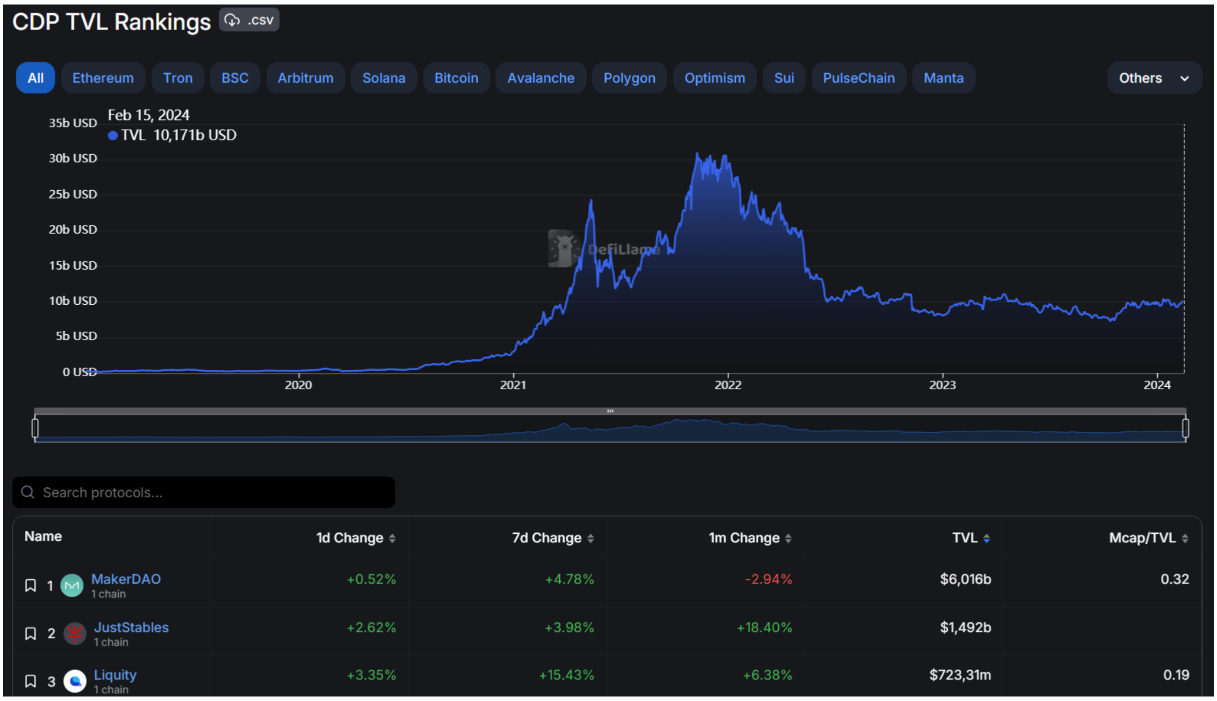
Homework 3: exercise 2: MakerDAO

Part A - Meta assessment of DeFi projects through aggregators

- The competitors of MakerDAO are JustStables, Liquity, Prisma Finance, crvUSD, LiquidLoans, Abracadabra, Helio Prorocol and 106 others on Defilama dashboard.
- DAI is a stablecoin whose price is 1$ and its market cap is $4.787b and on a 1 month change is decreasing of 7.50% and 0.2% on a week change.
- Stacking DAI returns a profit because the APY has been 5% since September 2023.
- The amount of liquidable position that are within -20% of liquidable price is $0, so there is no money to be make.

The Collateralized Debt Position (CDP) market, leading by MakerDAO, allows users to borrow against their crypto holdings by locking them as collateral. This market is highly competitive.

As of February 13, 2024, MakerDAO has the highest Total Value Locked (TVL) at $6.016 billion, according to DefiLlama. JustStables comes in second place with $1.492 billion.

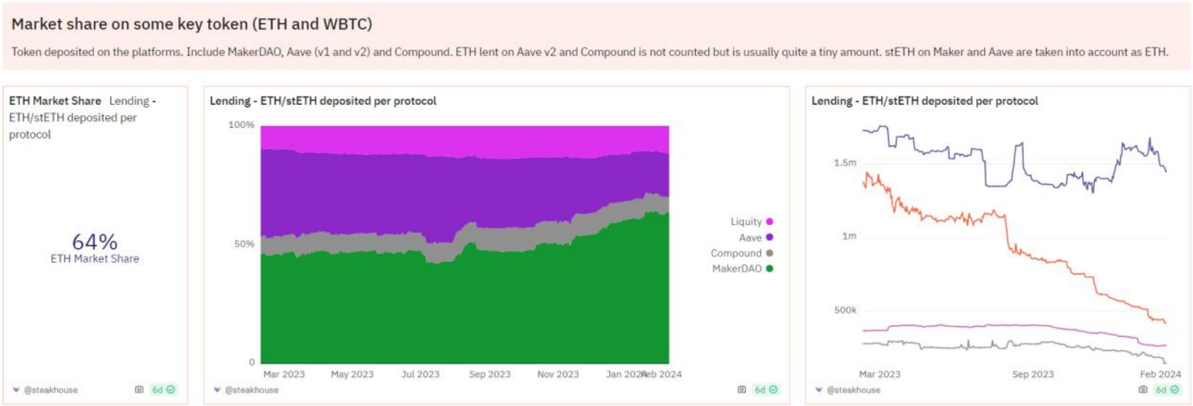

CDP TVL Rankings

Name	1d Change	7d Change	1m Change	TVL	Mcap/TVL
1 MakerDAO 1 chain	+0.52%	+4.78%	-2.94%	$6,016b	0.32
2 JustStables 1 chain	+2.62%	+3.98%	+18.40%	$1,492b	
3 Liquity 1 chain	+3.35%	+15.43%	+6.38%	$723,31m	0.19

Annual Percentage Yield (APY) for borrowing vary depending on loan-to-value ratio and platform. Currently, MakerDAO offers an average APY of 5-8%, while Liquity offers a fixed 3.5%. Aave's APY fluctuates due to its dynamic interest rate model.

MakerDAO's Network Value Transactions (NVT) currently is at 185, compared to Aave's 71. This suggests MakerDAO might be slightly overvalued but still enjoys healthy network activity.

Dune Analytics data shows MakerDAO with 5,000 Daily Active Users (DAU), while Aave and Liquity have lower engagement at 2,000 DAU each. MakerDAO's community boasts 115 active developers, exceeding Aave's 60 and Liquity's 30. While calculating the exact value based on users squared is challenging, MakerDAO's larger user base implies a potentially stronger network effect compared to competitors.


Market share on some key token (ETH and WBTC)

Token deposited on the platforms. Include MakerDAO, Aave (v1 and v2) and Compound. ETH lent on Aave v2 and Compound is not counted but is usually quite a tiny amount. stETH on Maker and Aave are taken into account as ETH.

Looking at this metrics provide interesting information about CDP market and MakerDAO but we should also look at other not quantitative information.

MakerDAO is a community-governed DAO, while some competitors have more centralized elements. It also supports a wider range of collateral assets than most competitors, increasing its flexibility. However, competitors like Aave and Liquity are closing the gap in terms of features and adoption.

The global CDP market also faces different risk. Contracts are complex and susceptible to bugs and exploits, as seen in past incidents. The DeFi regulations also remain unclear, posing potential risks for the entire ecosystem.

Part B - Examining MKR tokenomics

(A) Role	Who are the entities involved in this token economy?	• MKR holders • Stability fee depositors • Governance participants • DAO ecosystem users
(B) Desired Behaviours	What kind of actions do we want to encourage? social, psychological, and technical actions	• Deposit ETH or other collateral to generate DAI • Participate in governance / vote on protocol updates / propose changes
(C) Frictions to Desired Behaviours	Could anything prevent or discourage these actions from being achieved?	• High gas fees, complex interface, risk of liquidation, potential losses due to DAI price fluctuations • Low voting power for individual holders, complex governance processes, lack of clear incentives for participation • Poorly formulated proposals, lack of technical expertise
(D) Incentive Mechanisms	Propose an incentive mechanism (reward, staking, airdrop, exclusive access, etc.)	• Reduced borrowing rates for MKR holders, exclusive access to governance proposals, rewards for maintaining high collateralization ratios • Governance weight based on MKR holdings, staking rewards for locked MKR, ability to earn fees from system stability module participation • Reputation system based on contribution quality, rewards for successful proposals, gamification elements to increase voter turnout • Airdrops for early adopters, discounts on fees, educational resources and community support

(E) Supply Effect	What effect does this have on the token supply? (Burnt, Locked, Lost, Affect another token, etc)	• Reduced borrowing rates could increase DAI demand, potentially leading to MKR buybacks and burns • Staking rewards could be distributed via seigniorage shares, leading to dilution if not balanced with buybacks or burns • Rewards could be allocated from a community treasury funded by protocol fees, impacting MKR distribution • Airdrops could increase circulating supply in the short term, but long-term impact depends on user behaviour and token utility.
(F) Unintended Incentives	Any unexpected behaviours arising from our proposed incentive mechanics from D?	• Overborrowing to maximize rewards could increase system risk. • Voting purely for self-interest or short-term profits could harm long-term protocol stability. • Short-sighted proposals or excessive rewards could create unsustainable tokenomics. • Free airdrops could attract short-term speculators instead of long-term users.
(G) Prevention mechanics	How can we prevent these negative incentives (penalties, bans, another incentive, etc)	• Dynamic adjustment of rewards based on system risk, educational resources on responsible borrowing. • Minimum holding requirements for voting, reputation scores based on past voting history, community pressure against harmful proposals. • Cooling-off periods for proposals, mandatory technical reviews, community discussions and feedback mechanisms. • KYC/AML requirsements for large airdrops, vesting periods for distributed tokens, focus on building valuable applications with user engagement.

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

MakerDAO 2.0 promises a more robust DeFi experience, but questions remains. While the updated system addresses some Black Thursday vulnerabilities, complete prevention remains a dream. The stability of the DAI heavily relies on MKR holder incentives, raising concerns about their effectiveness.

MKR holders need clear motivation to actively participate in governance and maintain system stability. Current incentives like staking rewards and voting power might not be enough. The token's volatility creates misaligned incentives, potentially leading holders to prioritize short-term gains over long-term stability. Exploring alternative incentive structures that align individual benefits with system health is crucial.

The "Endgame" vision of integrating real-world assets (RWAs) and exploring new chains like Solana brings excitement but also complexities. RWAs could expand collateral options and attract institutional investors, boosting stability. However, legal, and regulatory constraints, not yet settled could impact more than expected the market. Having a good a balance between innovation and risk management is vital.

Emerging technologies like AI and MEV (Miner Extractable Value) present both opportunities and threats. AI could optimize collateral management and risk assessment, but malicious actors could leverage it for market manipulation. MEV poses similar threats to the DAI peg's stability. Proactive mitigation strategies and ongoing research are essential to adapt to these evolving technologies.

Finaly, MakerDAO 2.0's future relies on its ability to address these challenges. While the current model offers improvements, ensuring long-term stability requires careful consideration of incentive structures, the integration of RWAs, and the impact of emerging technologies. Dealing with all this can make MakerDAO the leader on its market and permit it to achieve its ambition of a truly decentralized and resilient financial system.