Exercise 1

Part C – Contrast data serving methods

The subscription and direct funding methods for Verifiable Random Function (VRF) offer different approaches tailored to various use cases within blockchain applications, such as those employed by Chainlink VRF for generating randomness.

The Direct Funding Method is for infrequent requests; it doesn't necessitate a subscription setup, but contracts using it directly fund their requests with tokens each time they call for randomness. Hence, this is useful for applications where end-users bear the cost of those requests (the cost is determined at the time of the request).

On the other hand, subscription method requires a subscription account, and you need to pre-fund it with tokens. It is better for frequent requests (more gas-efficient) since it allows batching multiple requests under a single subscription. I see it useful for dApps requiring lots of randomness, like lotteries or some games.

Part D – Reflect on the current state of Blockchain

When integrating the Chainlink Verifiable Random Function (VRF) into a crypto coinflip game, the gas used per random number request is variable, dependent on network congestion and the complexity of the contract interaction but is a critical cost component. Initial contract funding involves transferring enough cryptocurrency to cover the VRF fee plus the gas fees for transaction execution, which can be significant depending on the current gas prices on the network.

The speed at which Metamask estimates costs and performs transactions can vary a lot. During times of high network congestion, transactions can be slower and more expensive, potentially degrading user experience by causing delays and increasing the cost of playing the game proposed by the dApp.

For the business running this game, the primary costs include the gas fees for each transaction (including random number requests), the Chainlink VRF fees, and any additional operational or development costs associated with maintaining the game. The user experience is heavily influenced by transaction speed and cost, which can fluctuate with network conditions.

From a technical perspective, current challenges in blockchain involve scalability, transaction costs, and speed. To improve the future of blockchain technology, solutions such as layer 2 scaling solutions, more efficient consensus mechanisms, and optimization of smart contract execution can address these issues. Enhancing scalability can reduce gas fees and increase transaction throughput, improving both the cost-effectiveness for businesses and the overall UX. The development of more user-friendly tools and interfaces can also lower the barrier to entry, making blockchain applications more accessible to a wider audience. One way to solve some of these challenges can come from modular blockchains.

Exercise 2

Part A – Meta assessment of DeFi projects through aggregators

According to data from DeFiLlama, the Total Value Locked (TVL) in the Collateralized Debt Position (CDP) market is around $10.7 billion, maintaining a stable trend since the end of 2023. The TVL is a crucial metric in decentralized finance (DeFi), representing the total capital held within the smart contracts of a given protocol, indicative of its size and health. This market saw significant growth in mid-2021 and 2022, followed by a sharp decline. MakerDAO, a prominent player in the space, accounts for over 60% of the market's TVL, holding $6.421 billion. Despite its dominance, MakerDAO's growth rate in TVL is not the highest, showing a 10% increase in one month, compared to 22% for JustStables at $1.589 billion and 30% for Liquity at $774 million.

MakerDAO's main competitors include JustStables (USDJ stablecoin), Liquity (a borrowing protocol offering 0% interest loans against Ether with fees paid by borrowers), Prisma Finance, crvUSD, Helio Protocol, LiquidLoans, Abracadabra, Indigo, Lybra Finance/V2, and Kava Mint. Each brings unique offerings to the DeFi landscape, ranging from liquid staking tokens and decentralized stablecoins to cross-chain DeFi services.

In terms of market capitalization, DAI (MakerDAO's stablecoin) ranks third among all stablecoins, trailing significantly behind USDT (Tether) and USD Coin (USDC) with market caps of $97.811 billion and $26.946 billion, respectively. DAI's market cap stands at $4.859 billion, and it operates on fewer blockchain networks compared to its top competitors. Despite a slight deviation from its peg (-0.18%), DAI's circulation remains stable at around 5 billion units, crucial for its stability, with Ethereum backing 91.17% of its value. Around 500,000 wallets hold DAI, highlighting its widespread use.

MakerDAO also leads in potential liquidations, a scenario where collateral might be sold off due to market downturns. Currently, no collateral is near the 20% liquidation threshold. Among the top 100 positions across all protocols, the five largest are with MakerDAO, each exceeding $60 million in value. Notably, the ETH-C vault stands out for generating the highest monthly revenues from vault interest.

A notable portion of DAI is held in Treasury and Externally Owned Accounts (EOAs), indicating a preference for holding DAI outside of lending protocols and decentralized exchanges (DEXs), where it primarily circulates on Curve and Uniswap v3. Compared to counterparts like Liquity, AAVE, and Compound, MakerDAO has seen the most significant influx of ETH/stETH recently.

A dashboard created by Salva on Dune Analytics provides an insightful comparison of MakerDAO's balance sheet from 2022 to 2023. It shows an 87.42% reduction in stablecoin assets, offset by a 281.51% increase in real-world assets and an 80.97% rise in crypto-loans, leading to a modest 1.60% overall asset growth. Despite a 2.01% decrease in vault interest and a substantial 423.38% increase in the peg stability module, total income dropped by 52.78%. However, with a 10.27% decrease in total expenses, the net income fell by 49.89%.

Part B – Examining MKR tokenomics

The MKR token is the governance token of the MakerDAO system, designed primarily to facilitate voting on critical decisions related to the DAI stablecoin's operation and parameters. Its principal objective is to ensure DAI's stability against the US dollar on the Ethereum blockchain. Unlike many cryptocurrencies, MKR cannot be mined and is subject to price volatility. It plays several vital roles within the MakerDAO protocol, including fee payment for borrowing DAI, governance participation, and the stabilization of DAI.

MKR token holders are empowered to vote on various aspects of the project, including network operation, collateralization parameters, and stability fees. These fees represent a variable commission paid by DAI borrowers when they deposit collateral. Each MKR token grants its holder one vote, ensuring that changes to the protocol are community-driven. To safeguard the protocol's security, any approved changes take up to 24 hours to implement, allowing MKR holders to prevent unfavorable governance proposals.

MKR is crucial for maintaining DAI's peg to the US dollar, especially given the volatility of Ethereum, the primary collateral for DAI. The Collateral Debt Position (CDP) smart contracts govern DAI borrowing, requiring a collateral ratio of 150%. When Ethereum's price drops significantly, it could lead to under-collateralization, threatening DAI's stability (see Black Thursday). In such cases, MKR acts to prevent devaluation by facilitating auctions to convert MKR to DAI if the collateral value is insufficient. Conversely, if stability fees generate a surplus of DAI, the excess DAI is converted to MKR to maintain the peg.

MKR is used to pay fees associated with borrowing DAI. These tokens are then burnt, reducing the total supply and ensuring the protocol's proper functioning.

The holders of MKR can vote on the development and operational adjustments of the protocol, but unlike some governance tokens, MKR does not provide direct rewards to holders, only voting rights.

Regarding the allocation of the token, a total of 15.5% is distributed across three seed rounds, 15% is allocated to the development team and 69.5% is reserved for founders and the project itself.

In extreme situations, such as severe market volatility or a significant breach, MKR holders have the authority to initiate an emergency shutdown. This process settles all DAI debts and liquidates the system's collateral to cover DAI issuance, safeguarding the ecosystem's stability.

Part C – Personal reflection on the current and future state of MarkerDAO

On Black Thursday, the precipitous fall in ETH prices rendered many CDPs undercollateralized, triggering the protocol's automatic liquidation mechanisms designed to maintain the system's solvency. However, the confluence of a global pandemic declaration, an oil price war, and a general flight to liquidity across financial markets compounded the crisis. The resulting sell-off in the crypto markets led to a cascade of liquidations, exacerbating the situation on platforms like BitMEX and causing a liquidity crunch across the crypto space.

The intended liquidation process, involving debt and collateral auctions to manage undercollateralized positions, was overwhelmed. The chaotic market conditions allowed for exploitative bids on liquidated collateral, resulting in significant losses for MakerDAO (zero-bids managed to get ETH in the vaults, as there was no competition against them).

Following this crisis, MakerDAO undertook several governance and protocol adjustments to prevent a recurrence of such forced liquidations leading to substantial losses. These changes included revising auction mechanisms and governance protocols to enhance system resilience against extreme market volatility. Moreover, the inclusion of the stablecoin USD Coin (USDC) into its collateral pool was a strategic move to diversify the risk associated with reliance on volatile assets like ETH.

Since Black Thursday, MakerDAO has implemented several measures aimed at strengthening its governance framework, improving auction systems, and broadening its collateral base. These adjustments are designed to enhance the protocol's ability to withstand severe market downturns and prevent a recurrence of the systemic failures experienced. However, while these improvements

significantly increase resilience, the inherent volatility and unpredictability of cryptocurrency markets mean that risk cannot be entirely eliminated. Stakeholders ecosystem must remain vigilant and proactive in governance participation to navigate future challenges effectively.

Overall, the MKR token's governance and economic models provide a solid framework for incentivizing MKR holders to maintain the stability and security of the MakerDAO protocol. However, ensuring that these incentives lead to the desired outcomes requires continuous engagement from the community, effective communication of the implications of governance decisions, and ongoing education to increase the participation and quality of decision-making among MKR holders. Additionally, the protocol must continue to evolve and adapt to address emerging challenges and risks within the broader DeFi landscape. The lack of valuable rewards for MKR holders may be something to address, as other DeFi protocol propose rewards. The creation of SubDAOs is good, as it increases the decentralization aspect of the protocol; I believe one of the main reasons user don't participate in the voting system of protocols is due to the fact that they know their vote will not count much in the balance. One possible solution to tackle the low rate of voting participation would be to, thus, reduce the voting power of "whales". This would mean changing the intrinsic system delegating the power ("one-token, one-vote" mechanism). Using computation voting theory, we can cite "quadratic voting" which is such that the number of tokens to spend grows quadratically to the number of votes (tested by Gitcoin with good results). With that, people could have more incentives to participate in the development of the protocol.

Regarding the Endgame the goal is for the ecosystem to reach a self-sustainable equilibrium called the endgame state. The main aspect of the Endgame is the formation of a series of new DAOs called "MetaDAOs" which are for more specialized aspects of the protocol. This is to avoid having the DAO being too complex. They want to reorganize the existing decentralized workforce ecosystem into new self-sustainable DAOs (those MetaDAOs/SubDAOs), with each its own unique governance token, processes, workforce, and interfaces. The funder wrote that this new MetaDAOs would offer strong incentives for MKR holders to vote.

The last phase of the Endgame is the launch of a native blockchain, which will make the ecosystem more secure and efficient; they plan to deploy MakerDAO on a fork of Solana (not only Ethereum, but EVM-compatible); creator of Ethereum answered to that by selling $580000 worth of MKR (Solana being a competitor to Ethereum).

For those who hold DAI, the Endgame aims at giving stronger and more decentralized collateral backing of it. One part of the plan is to increase the supply of DAI to more than $100 billion worth of DAI withing 3 years.

The Endgame Plan's objectives align with the broader goals of ensuring that MakerDAO remains a leading and innovative force in the DeFi space. By focusing on decentralization, scalability, ecosystem integration, financial sustainability, and security, the plan addresses the critical challenges and opportunities facing the protocol. These goals are not only ambitious but also necessary for adapting to the rapidly evolving blockchain and financial landscapes.

Moreover, the plan's emphasis on governance and community involvement ensures that MakerDAO can continue to evolve based on collective decision-making and shared values. This approach is in line with the principles of DeFi and blockchain technology, emphasizing transparency, inclusivity, and decentralization.

Regarding new technologies, AI offers solutions to the blockchain scaling challenges by introducing advanced decentralized learning systems and novel data-sharing techniques.

One of the most sought-after benefits of AI in blockchain is enhanced transaction efficiency. P2P transactions in a Blockchain system currently cost $9067 billion annually due to redundant tasks performed by each node. AI can identify the node likely to deliver the solution first, allowing the others to cease their efforts. This reduces costs and boosts system efficiency.

Although Blockchain is known for its strong security features, applications built with this technology are not immune to flaws. The AI brings NLP, Image Recognition, real-time data transformation capabilities to blockchain peer-to-peer linking. This combination enables data miners to convert large-scale systems into micro-economic environments.

AI could enhance smart contract development, making it more efficient and secure. Through machine learning algorithms, AI can help identify vulnerabilities and optimize code, potentially reducing the risks of exploits and bugs in protocols like in MakerDAO's Black Thursday event. AI can be used to analyse market trends and predict potential future movements. For a DeFi lending protocol like MakerDAO, AI-driven predictive analytics could improve risk management strategies, collateral valuation, and stability fee adjustments to better maintain DAI's peg and ensure the system's solvency. AI could automate certain aspects of governance, analysing vast amounts of data to recommend optimal decisions for protocol adjustments. This might help in more dynamically adjusting parameters like stability fees or collateral factors based on real-time market conditions, enhancing MakerDAO's responsiveness to market changes.

In the future, all data is expected to be stored on a blockchain. This means that organizations will be able to purchase data directly from holders. AI will track data usage, manage access, and oversee related tasks. Acting as data gates, AI will ensure that the flow of blockchain data is streamlined.

Moreover, projects involving AI already start existing, leveraging the power of blockchain and the characteristics of data stored in it. AI can use this data, which is "good" and accessible. Moreover, using the blockchain technology, it is possible to see a future where AI model runs on VM against some rewards.

When producing blocks, miners (or validators) choose the transactions and the ordering in the it. This is done purely arbitrarily, and the profit that is being made from that is called the "Miners Extractable Value". Simply speaking, this is the value that they extract from the users. Many methods exist to extract MEV in a way that it is maximised, such as front-running (bots detect profitable transactions in the mempool), or sandwich attack (which consists in manipulating the market by artificially changing the price, once again by detecting important transactions). In the context of MakerDAO and blockchain at large, MEV could affect transaction ordering, leading to front-running or other types of transaction reordering that could impact the fairness and efficiency of the system.

Firstly, it's important to notice that a small level of MEV can still be considered as necessary to incentivize an efficient and secure mining, since it assures many people are willing to mine. However, when it is abused, it can lead to a centralisation of the value; miners that engage in MEV will, on average, get higher profits, which will help them get more computing power, and so excluding smaller entities. In traditional finance, similar problems to MEV are illegal since it resembles market manipulation; miners can take advantage of knowledge others don't have (pending transactions), which is a kind of imperfect information that needs a solution, as it drives the network in a way that is not beneficial to other's interest.

One potential solution would be to implement an algorithm that, randomly, or based on an honest ethical rule, would choose itself transactions ordering. In traditional finance, the orders are done based on their received time; doing so would require a sort of centralisation for a spread time base,

so it can’t really be implemented. But rather than relying on time, relying on randomization can be of interest. Also, unlike the timing, I think it is possible to implement something like real life when dealing with imperfect information, but also something that comes from game theory; to reach an equilibrium for everyone (Nash Equilibrium), the protocol could punish those that behave the wrong way (miners doing MEV), redistributing the extracted value to users, like a tax.

Awareness and mitigation of MEV-related issues will become increasingly important for protocols like MakerDAO. Designing mechanisms to minimize the negative impacts of MEV, such as through fair transaction ordering or improved auction systems for liquidations, will be crucial to maintain system integrity and user trust.