DeFi Talents

Organized by

Frankfurt School Blockchain Center

Web3 Talents

Powered by

KFW

WM INNO LAB

Deka

WM DATENSERVICE

dwpbank

Supported by

DEC INSTITUTE

DEA DIGITAL EURO ASSOCIATION

MAMA Multichain Asset Managers Association

ECOTA EUROPEAN CARBON OFFSET TOKENIZATION ASSOCIATION

Assignment 5

January 6, 2024

By

Manjiri Birajdar

Software Developer

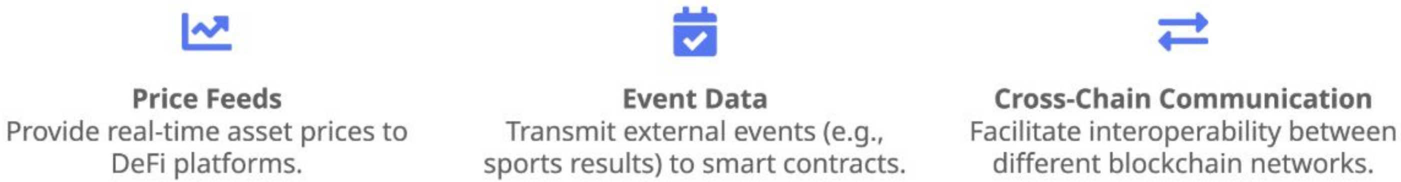
Assignment 5

1. **Oracles**
   a. What functions do oracles fulfill in DeFi?
   b. How do they connect off-chain information with on-chain information?
   c. How do you get random numbers on-chain?
   d. What are the risks of using oracles? State at least one type of oracle attack.
2. **Interoperability / Multi-Chain / Cross-Chain Bridges**
   a. What are the biggest cross-chain bridges in terms of tx volume? Which blockchain ecosystem is the most interconnected (e.g., number of integrated chains, transaction volume, etc.)? What risks do bridges bring?
   b. Choose either: i) Stargate Finance, ii) Cosmos, iii) Cross-Chain Interoperability Protocol (CCIP), iiii) Wormhole: How do they solve the interoperability issue?
3. **Getting to know stakeholder domains (Legalists and Technologists)**
   a. What are the top 3 questions an interviewer should ask a blockchain developer?
   b. If you were the supreme regulatory authority in your home country, how would you regulate the DeFi space? Do you want more or less regulation? Think of taxation, the definition of a security token, the emission of stablecoins, and other aspects you deem important.

Oracles

What functions do oracles fulfill in DeFi?

Oracles serve as critical bridges in the DeFi ecosystem, enabling smart contracts to interact with external data sources. For instance, they provide real-time price feeds, ensuring accurate asset valuations. They also transmit event data, allowing smart contracts to execute based on real-world occurrences. Furthermore, oracles facilitate cross-chain communication, enhancing interoperability across blockchain networks.



Price Feeds
Provide real-time asset prices to DeFi platforms.

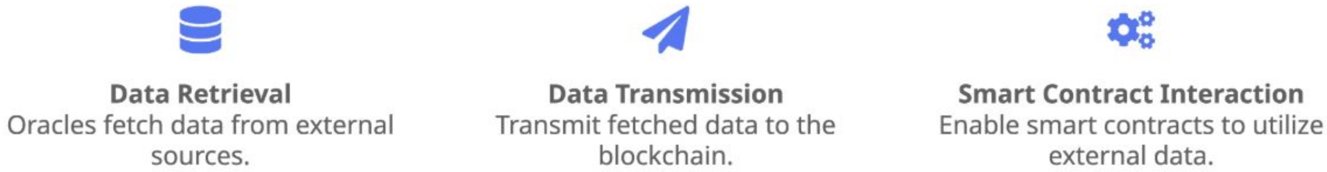
Event Data
Transmit external events (e.g., sports results) to smart contracts.

Cross-Chain Communication
Facilitate interoperability between different blockchain networks.

Oracles

How do they connect off-chain information with on-chain information?

Oracles operate by retrieving data from external sources, such as APIs or sensors. They then transmit this data to the blockchain, where it can be accessed by smart contracts. This process allows smart contracts to interact with real-world information, expanding their functionality beyond the blockchain



Data Retrieval
Oracles fetch data from external sources.

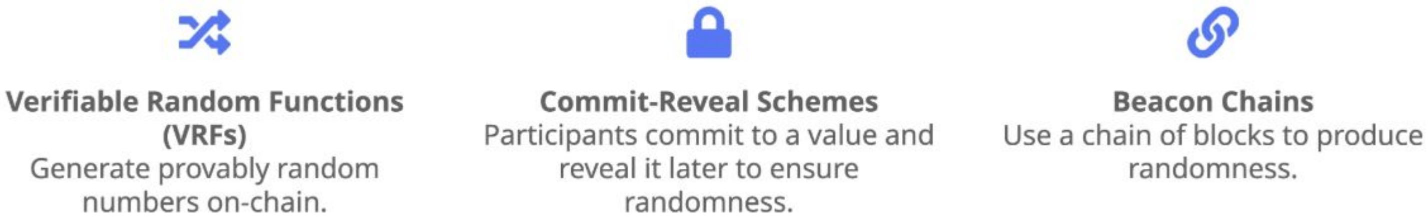
Data Transmission
Transmit fetched data to the blockchain.

Smart Contract Interaction
Enable smart contracts to utilize external data.

Oracles

How do you get random numbers on-chain?

Generating random numbers on-chain is crucial for applications like decentralized gaming. Methods such as Verifiable Random Functions (VRFs) provide provably random numbers. Commit-reveal schemes involve participants committing to a value and revealing it later to ensure randomness. Beacon chains utilize a sequence of blocks to produce randomness, enhancing security and unpredictability



Verifiable Random Functions (VRFs)
Generate provably random numbers on-chain.

Commit-Reveal Schemes
Participants commit to a value and reveal it later to ensure randomness.

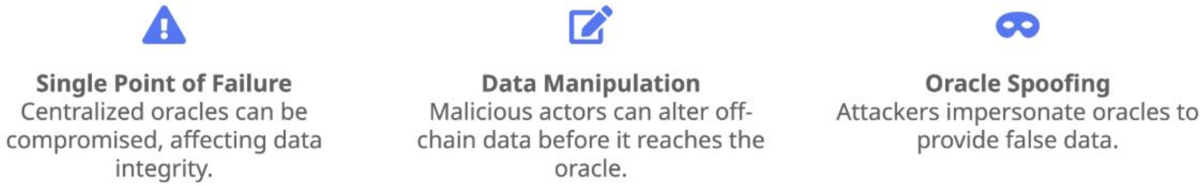
Beacon Chains
Use a chain of blocks to produce randomness.

Oracles

What are the risks of using oracles? State at least one type of oracle attack.

Oracles play a crucial role in connecting off-chain data with on-chain smart contracts, but they also introduce several security risks. Below are some of the key risks and attack vectors associated with oracles in decentralized finance (DeFi).

Types of attack:



Single Point of Failure
Centralized oracles can be compromised, affecting data integrity.

Data Manipulation
Malicious actors can alter off-chain data before it reaches the oracle.

Oracle Spoofing
Attackers impersonate oracles to provide false data.

Mitigating Oracle Risks

- **Use Decentralized Oracles**: Rely on multiple data sources and decentralized networks (e.g., Chainlink, Band Protocol) rather than a single centralized oracle.
- **Data Aggregation**: Fetch data from multiple independent sources and aggregate them to reduce the risk of manipulation.
- **Time-Weighted Averages**: Use time-weighted average prices (TWAP) to smooth out sudden price manipulations.
- **Verification Mechanisms**: Implement cryptographic proofs (e.g., Chainlink's Verifiable Random Functions) to ensure data authenticity.
- **Flash Loan Prevention**: Limit oracle price updates to prevent exploitation through rapid price changes.

Interoperability / Multi-Chain / Cross-Chain Bridges

What are the biggest cross-chain bridges in terms of tx volume?

Wormhole:

- One of the largest cross-chain bridges, connecting Ethereum, Solana, Binance Smart Chain, Avalanche, Terra, and other networks.
- It facilitates token transfers and data sharing across chains.

Polygon Bridge:

- Facilitates the transfer of assets between Ethereum and Polygon, enabling Ethereum's scalability.
- Known for high transaction volume, especially within the DeFi ecosystem.

Avalanche Bridge:

- A bridge between Ethereum and Avalanche, allowing seamless transfers of assets like AVAX and ERC-20 tokens.
- Popular for its low-cost transactions and fast finality.

Binance Bridge:

- Connects Binance Smart Chain with various other blockchains, including Ethereum and Bitcoin.
- Supports many assets and facilitates the large volume of transactions due to Binance's ecosystem.

Interoperability / Multi-Chain / Cross-Chain Bridges

Which blockchain ecosystem is the most interconnected (e.g., number of integrated chains, transaction volume, etc.)?

Cosmos:

- Known as the most interconnected ecosystem, thanks to its **Inter-Blockchain Communication (IBC)** protocol, which allows blockchains to communicate and transfer assets securely.
- The **Cosmos Hub** and its **Zones** (individual blockchains) work together, with a large number of integrated chains.
- Ecosystem is growing with a significant transaction volume as more blockchains join.

Polkadot:

- A close contender, Polkadot connects blockchains via its **Relay Chain** and **Parachains**, allowing interoperability.
- It's designed to allow multiple chains to share information and assets, creating a well-connected ecosystem.

Interoperability / Multi-Chain / Cross-Chain Bridges

What risks do bridges bring?

Risks of Bridges:

1. **Smart Contract Vulnerabilities:**
   - If a bridge's smart contract is compromised, it can lead to the theft or loss of assets.
   - Bugs in the bridge’s code can also be exploited by malicious actors.
2. **Centralization Risk:**
   - Some bridges rely on a centralized entity to manage transfers, increasing the risk of a single point of failure.
3. **Bridge Attacks:**
   - **Hacks and exploits** targeting bridges (e.g., the Wormhole hack) have resulted in the theft of millions of dollars. Bridges can be a prime target for attackers because of the valuable assets they handle.
4. **Transaction Delays:**
   - Some bridges might have slower transaction times or delays in cross-chain asset finality, which could affect users.

Interoperability / Multi-Chain / Cross-Chain Bridges

Choose either: i) Stargate Finance, ii) Cosmos, iii) Cross-Chain Interoperability Protocol (CCIP), iiii) Wormhole: How do they solve the interoperability issue?

- **Cosmos:**
  - Cosmos is designed with **interoperability** at its core through the **Inter-Blockchain Communication (IBC)** protocol.
  - IBC allows different blockchains to **transfer data and tokens** securely without needing a centralized intermediary.
  - Each blockchain in the Cosmos ecosystem is independent but can **communicate** with others via IBC. This decentralized framework allows for **trustless cross-chain interaction**, making Cosmos highly scalable.
  - With its **Cosmos Hub** at the center, this interconnected ecosystem can facilitate a broad range of decentralized applications (dApps) and protocols to operate across various blockchains.
  - **IBC** enables atomic transactions, which means that transfers are either fully completed or fully reverted to maintain consistency across chains.

In short, Cosmos allows for decentralized, secure communication between different blockchains, solving the interoperability issue by facilitating direct communication without reliance on a central authority or third party.

Getting to know stakeholder domains (Legalists and Technologists)

What are the top 3 questions an interviewer should ask a blockchain developer?

1. **How do you ensure the security and scalability of a smart contract?**
   - This question tests the developer's understanding of fundamental principles like gas optimization, avoiding common vulnerabilities (e.g., reentrancy attacks, overflow/underflow), and how to optimize code for performance, particularly in high-transaction environments.
2. **Can you explain the consensus algorithms in blockchain networks, and which one would you prefer for a specific use case?**
   - This question assesses their knowledge of different consensus mechanisms (e.g., Proof of Work, Proof of Stake, Delegated Proof of Stake, etc.) and their ability to choose the right one based on the requirements of the project (speed, energy efficiency, security, etc.).
3. **What is your experience with cross-chain interoperability, and how would you design a solution to bridge two different blockchains?**
   - Cross-chain interoperability is becoming increasingly important, especially in DeFi. This question explores the candidate's familiarity with tools and protocols for enabling communication and asset transfer between different blockchain ecosystems (e.g., using bridges, IBC, or layer-2 solutions).

Getting to know stakeholder domains (Legalists and Technologists)

If you were the supreme regulatory authority in your home country, how would you regulate the DeFi space?

1. Taxation:

- **Tax Reporting for DeFi Gains:**
  - **Tax reporting** would be required for any profits made through DeFi activities (e.g., staking, yield farming, lending/borrowing). Blockchain-based platforms could integrate tax reporting tools to track and report transactions to users.
  - **Capital Gains Tax:** Any increase in value through asset appreciation (such as holding tokens or NFTs) should be taxed based on capital gains.
- **Clear Guidelines for Staking/Yield Farming:**
  - Income generated through staking or yield farming should be taxed similarly to interest earned from traditional savings accounts, with clear tax guidelines for these income streams.

2. Definition of Security Tokens:

- **Clear Criteria for Security Tokens:**
  - I would advocate for **clear definitions** of what constitutes a security token in the context of DeFi. In most jurisdictions, tokens are considered securities if they represent shares, investment contracts, or profit-sharing mechanisms.
  - **Safe Harbor for Tokens:** There could be provisions for tokens that act purely as utility tokens (not tied to investment contracts), ensuring that developers aren't unduly burdened with compliance regulations if they are launching a non-securitized project.

Getting to know stakeholder domains (Legalists and Technologists)

If you were the supreme regulatory authority in your home country, how would you regulate the DeFi space?

3. Emission of Stablecoins:

- **Backed Stablecoins Regulation:**
  - Stablecoins that are backed by fiat or other assets should be required to maintain **adequate reserves** and undergo regular audits to ensure that the assets backing them are sufficiently collateralized.
- **Algorithmic Stablecoins:**
  - For algorithmic stablecoins, **transparency** about the mechanisms and risks would be essential. Regulations would ensure they cannot be manipulated or exploited for short-term gains.
- **Issuer Accountability:**
  - Stablecoin issuers would be required to maintain transparency, clearly outlining their reserve strategies, issuance policies, and risk management.

4. Smart Contract Audits and Security:

- **Mandatory Audits and Open-Source Code:**
  - All **smart contracts** that handle significant amounts of value should undergo **mandatory security audits** by certified third-party firms before deployment.
  - Contracts should be open-source for community inspection, encouraging transparency and peer review.
- **Security Standards:**
  - Establish clear security standards for DeFi platforms, and penalties for failing to meet these standards should be imposed.

Getting to know stakeholder domains (Legalists and Technologists)

If you were the supreme regulatory authority in your home country, how would you regulate the DeFi space?

5. Consumer Protection and Risk Disclosure:

- **Clear Disclosures for Users:**
  - Platforms must provide users with clear and easily understandable **risk disclosures**, especially in high-risk activities like liquidity mining and leveraged trading.
- **Consumer Protections for Vulnerable Users:**
  - Protection against fraud, hacks, and scams should be built into DeFi platforms, with clear dispute resolution mechanisms available for users in case of platform failures or breaches.

6. Privacy and Data Protection:

- **Data Protection Regulations:**
  - DeFi platforms should comply with data protection laws (e.g., GDPR or similar) to ensure users' personal data and transaction information are securely handled and stored.
- **Privacy Coins and Anonymity:**
  - Regulation would require that privacy-focused projects (like privacy coins) ensure **compliance with anti-money laundering (AML) regulations**, though they could operate in more limited or compliant environments.

Getting to know stakeholder domains (Legalists and Technologists)

If you were the supreme regulatory authority in your home country, how would you regulate the DeFi space?

7. Centralized Entities in DeFi:

- **Regulation of Centralized Entities:**
  - While DeFi is inherently decentralized, **centralized exchanges** or entities that control large portions of DeFi ecosystems (e.g., lending platforms or governance bodies) should be subject to regulatory oversight to prevent abuse of market power and ensure transparency.

8. Compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) Regulations:

- **AML/KYC for Certain Activities:**
  - While DeFi aims to reduce barriers to entry, certain high-risk activities like lending or large transactions should have **KYC/AML checks** to prevent money laundering and other illicit activities.
- **Privacy Considerations:**
  - Ensure that privacy is maintained without compromising the ability to trace illicit activities, using mechanisms like zero-knowledge proofs for compliance without revealing sensitive data.

Getting to know stakeholder domains (Legalists and Technologists)

Do you want more or less regulation? Think of taxation, the definition of a security token, the emission of stablecoins, and other aspects you deem important.

Balanced Approach: I would advocate for a **balanced approach** to regulation. We want to foster innovation in the DeFi space while addressing critical risks such as fraud, hacks, and market manipulation. Over Regulating could stifle innovation, but under regulating could lead to market instability and exploitation of consumers.

Regulatory Clarity: A **clear framework** will be crucial for encouraging both institutional and individual participation in the DeFi ecosystem without discouraging experimentation.

References

- https://www.upwork.com/resources/blockchain-developer-skills-what-to-look-for-in-a-blockchain-developer
- https://www.blockchain-council.org/blockchain-interview-questions-and-answers/
- https://www.entrepreneur.com/article/396225
- https://www.cointelegraph.com/news/the-importance-of-defi-regulation
- https://www.coindesk.com/defi/2022/07/11/the-global-regulatory-landscape-for-defi-2022/
- https://www.finextra.com/blogposting/21974/defi-regulation-how-governments-should-approach-the-emerging-sector
- https://www.coindesk.com/markets/2022/07/22/taxing-cryptocurrency-and-defi-in-the-us-what-you-need-to-know/
- https://www.developingblockchain.com/defi-taxation-overview/
- https://www.investopedia.com/terms/s/security-token.asp
- https://www.blockchain-council.org/blockchain/security-token-offerings-and-their-legal-implications/
- https://www.theblock.co/post/31384/the-legal-definition-of-a-security-token
- https://www.americanbar.org/groups/business_law/publications/blt/2022/04/stablecoins/
- https://www.coindesk.com/policy/2022/12/19/the-future-of-stablecoins-and-global-regulation/
- https://www.forbes.com/sites/forbestechcouncil/2022/12/06/what-regulators-need-to-know-about-stablecoins/
- https://www.coindesk.com/learn/2021/05/14/how-cross-chain-bridges-work/
- https://decrypt.co/115497/cross-chain-bridges-are-paving-the-way-for-defi-but-they-come-with-risk
- https://cosmos.network/learn/what-is-cosmos
- https://www.cosmos.network/resources/whitepaper
- https://www.coindesk.com/markets/2021/03/03/ibc-the-key-to-cross-chain-communication-in-the-cosmos-ecosystem/
- https://www.smartcontractsecurity.com/
- https://www.coindesk.com/learn/2022/02/04/common-smart-contract-vulnerabilities/
- https://www.certik.com/blog/blockchain-smart-contract-security
- https://www.coindesk.com/defi/2021/12/06/risks-of-centralized-exchanges-in-defi/