DeFi Overview and Analysis

Alexander Marrero, Gautham Gali, Vincent DiPerna, Helen Zhu

Introduction

The Current Financial System - Centralized Finance (CeFi)

Centralized Finance:

- Several types of services (loans, insurance, savings/checking accounts, stock exchange)
- Reliant on intermediaries such as banks and governments to help manage money
- Several inefficiencies
    - Intermediaries
    - Charges
- Solutions?

The New Financial System - Decentralized Finance (DeFi)

Advantages

- Transparency
- Interoperability
- Free to Use
- Many Protocols and Applications

Objectives

- Conduct a theoretical analysis and comparison of existing DeFI protocols and platforms.
- Analyze the performance of these protocols and explain them.
- Goals for the reader:
  - Develop a deeper understanding of DeFi
  - Explore various popular protocols

Related Work

Blockchain Platforms and DeFi Operations

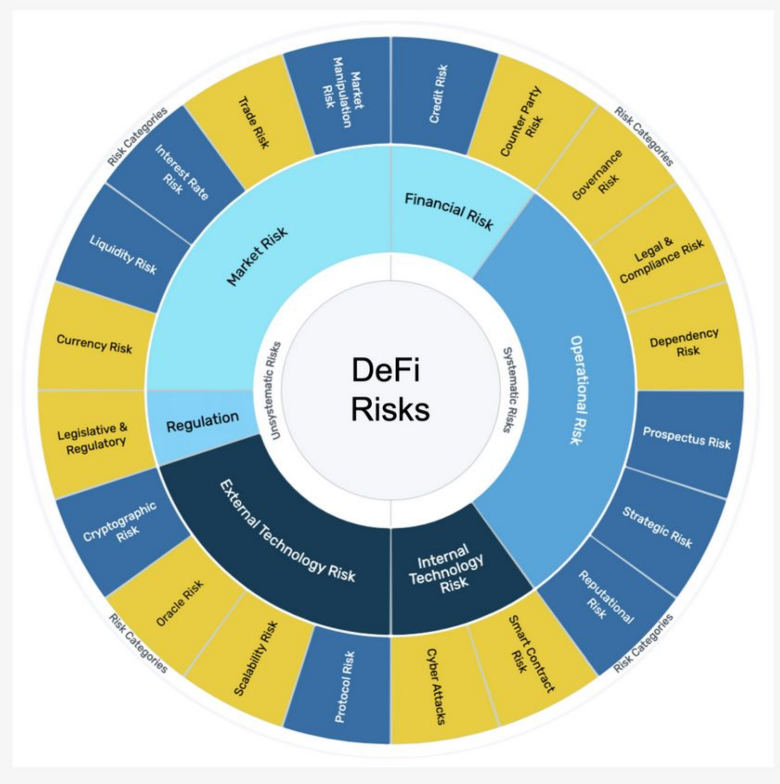
1. Transition to Proof-of-Stake (PoS) Consensus Mechanisms:

   Major blockchain platforms like Ethereum, Polkadot, Cardano, and Lukso are moving from energy-intensive proof-of-work (PoW) to more sustainable proof-of-stake (PoS) systems.

2. Impact of Ethereum 2.0 on Sustainability:

   Ethereum's upgrade to Ethereum 2.0 highlights a significant reduction in energy consumption—by approximately 99%.

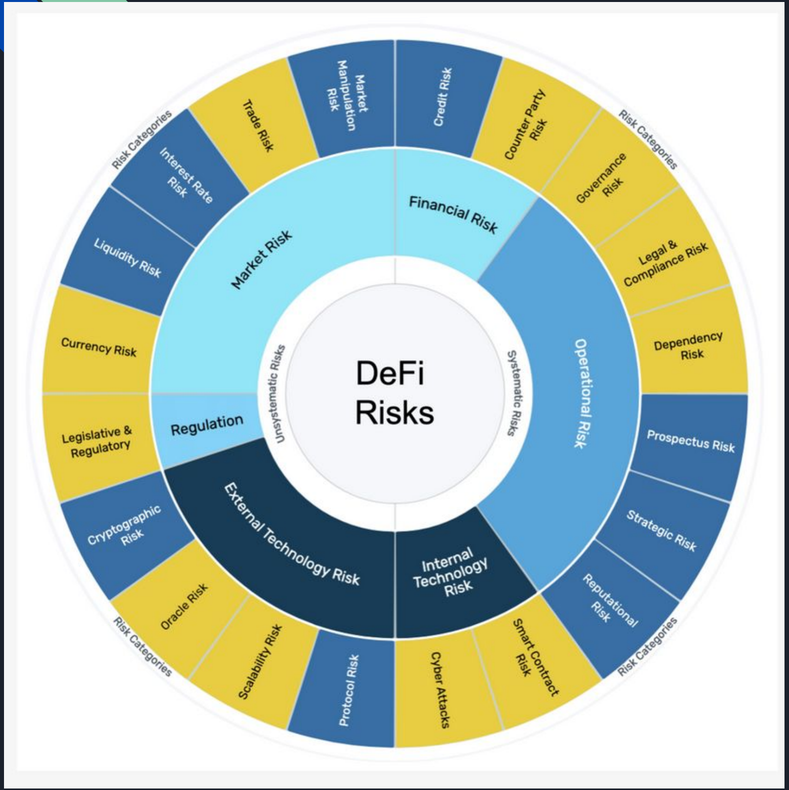
Security Aspects of DeFi



The left half of the figure represents unsystematic risks, whereas the right half illustrates systematic risks. The inner colored circle denotes the level 1 categories.

1. Systematic risks
2. Unsystematic Risks

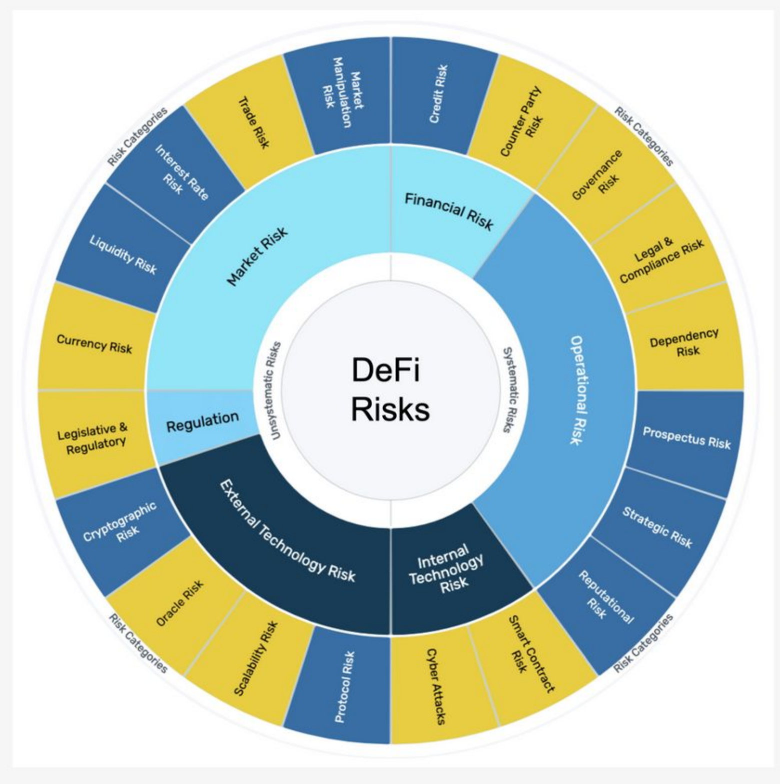
Security Aspects of DeFi



Systematic risks

- Financial Risk
- Operational Risk
- Regulation Risks

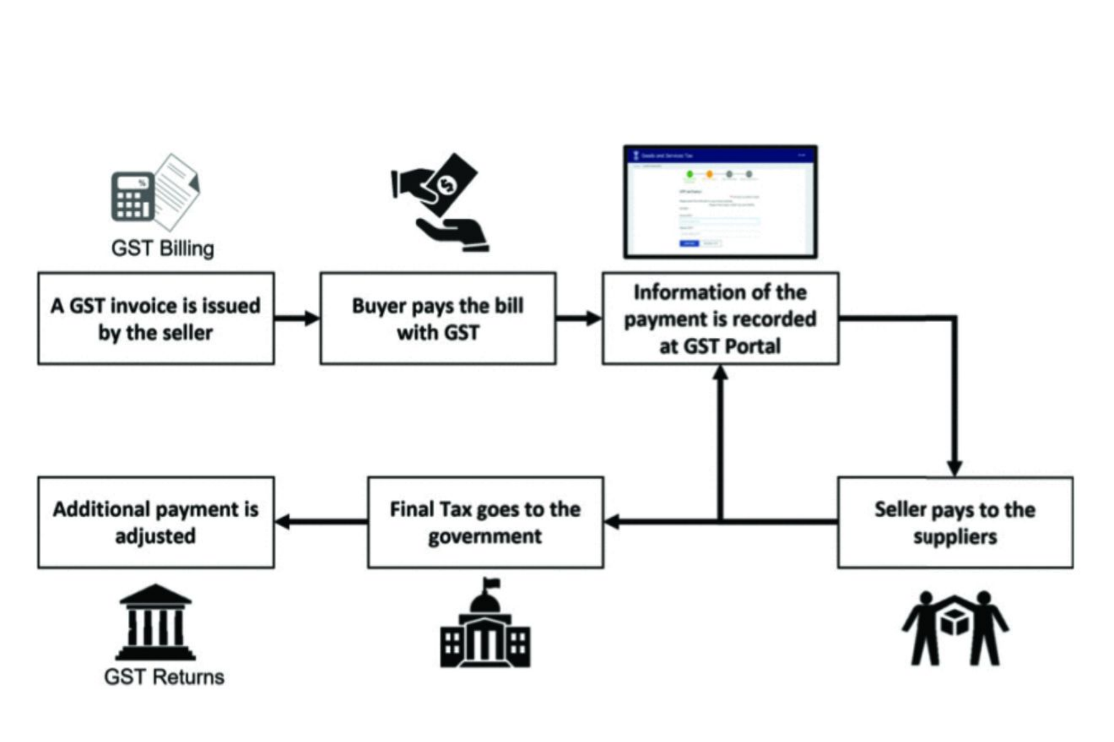
Security Aspects of DeFi



UnSystematic risks

- Technological Risks
- Cryptographic Risks
- Liquidity Risks

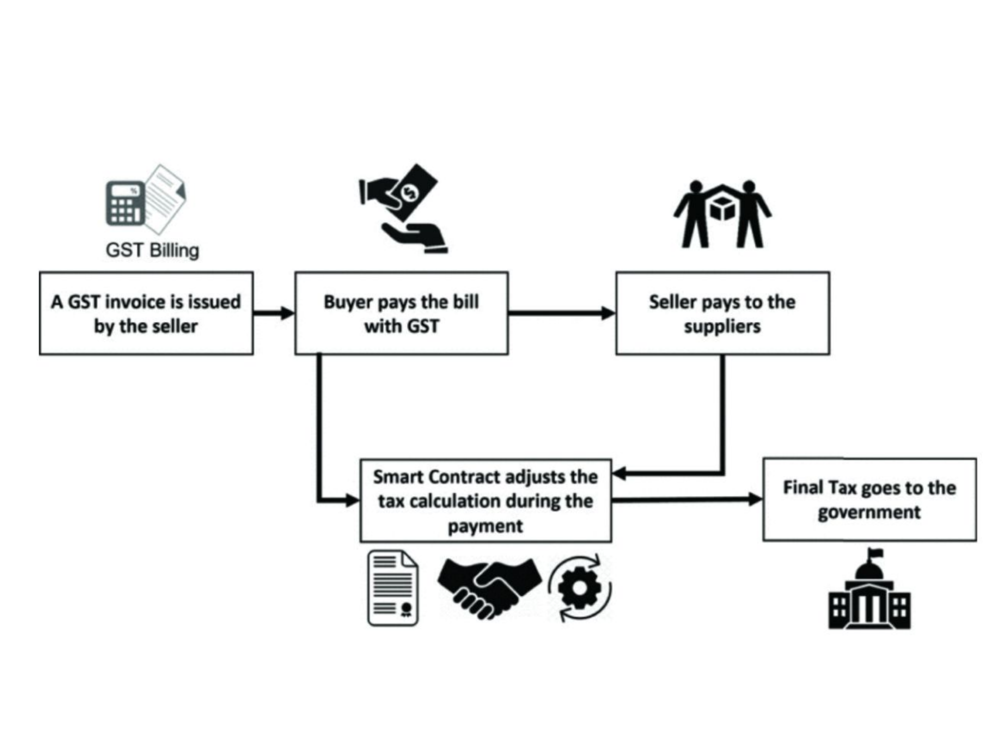
DeFi Applications and their Implications



GST Billing
A GST invoice is issued by the seller
Buyer pays the bill with GST
Information of the payment is recorded at GST Portal
Seller pays to the suppliers
Final Tax goes to the government
Additional payment is adjusted
GST Returns

Goods and Services Tax (GST) is an indirect tax imposed on the supply of goods and services in India.

DeFi Applications and their Implications

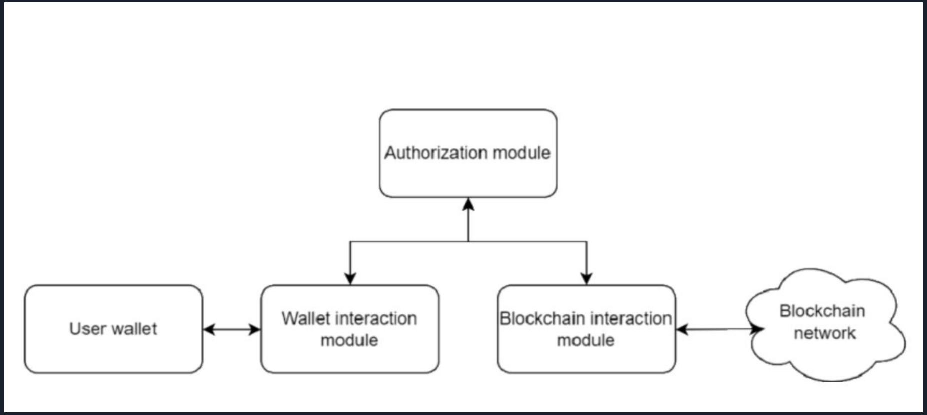

GST Billing
A GST invoice is issued by the seller
Buyer pays the bill with GST
Seller pays to the suppliers
Smart Contract adjusts the tax calculation during the payment
Final Tax goes to the government

Preliminaries

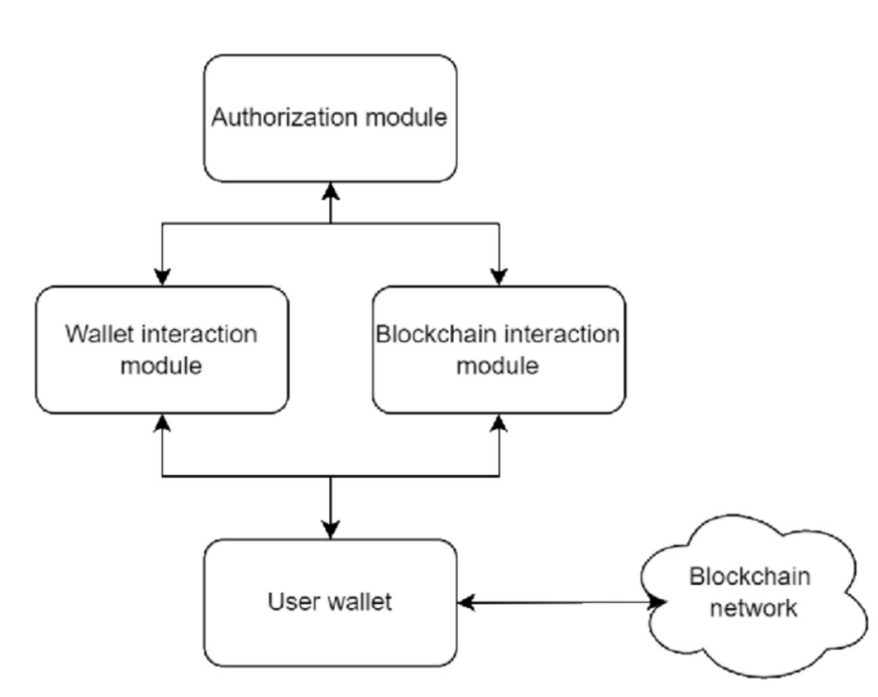
DeFi Overview

1. Definition and Role of DeFi
2. Decentralization and User Contro
3. Ethereum as a Platform for DApps
4. Currency Utilization in DeFi

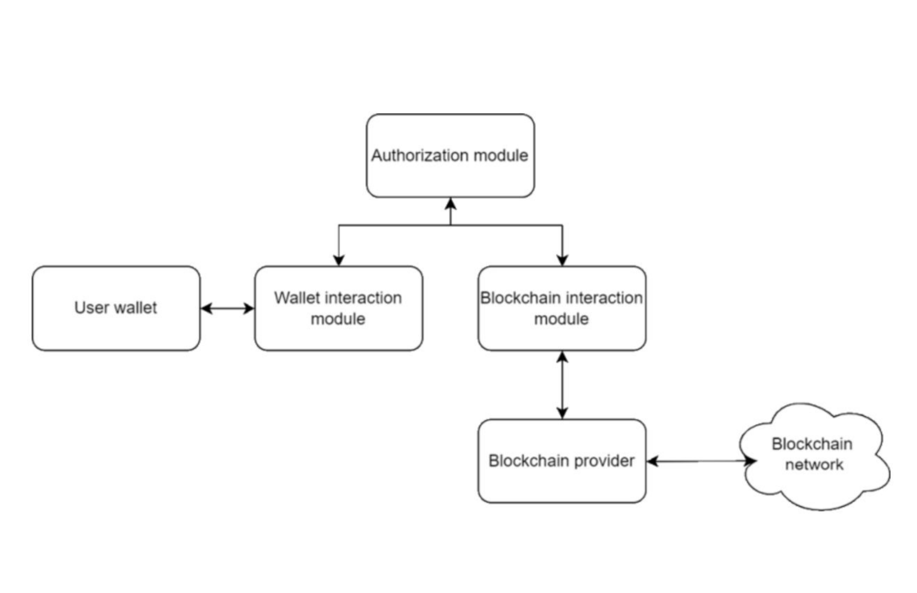
Data Storage Models:
Web Implementation of Authorization Module



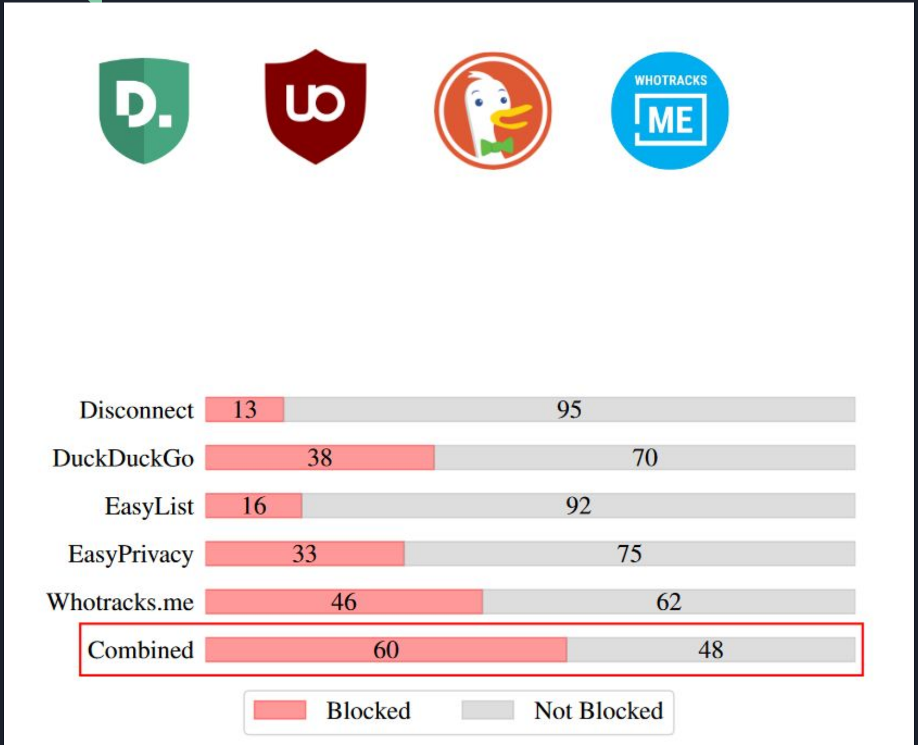
Data Storage Models: Ethereum Web Module



Data Storage Models: Cardano Web Module



Security in DeFi



- Analyzed efficacy of 5 popular Ad blockers:
- Whotracks.me provides best protection (43%)
- Disconnect provides weakest protection (12%)
- Installing multiple Ad blockers improves privacy
- Combination of all blocks 56% of third-parties

Model

System Model

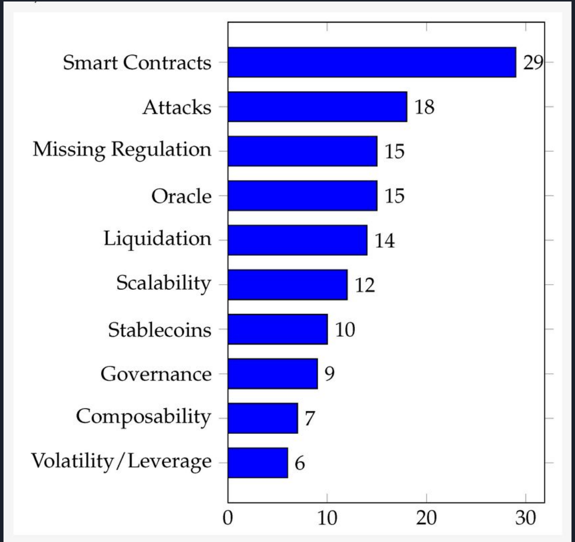
The DeFi Model consists of 4 main parts:

- Decentralized Exchange Aggregators
  - Examples: DEX.AG, Bancor, Dolomite
- Decentralized Exchange Platforms (DEX)
  - Examples: Uniswap, Kyber Network, Balancer, Curve Finance
- Decentralized Money Markets
  - Examples: Aave, Compound
- Decentralized Insurance
  - Examples: Nexus Mutual, Bridge Mutual

Threat Model

Concerning Threats in DEFI:

- Smart Contract Vulnerabilities
- Attacks
- Oracle Manipulation
- Government Regulation
- Liquidation
- Scalability



Top Ten Most Mentioned DeFi risks in Literature

Security Model

Addressing These Threats:

- Smart Contract Vulnerabilities and Attacks
    - Solution: Code audits, more testing before deploying code, bug bounties
- Oracle Manipulation
    - Solution: Use trusted Oracles, data verification mechanisms
- Government Regulation
    - Solution: Implement compliance measures, consult with legal professionals
- Liquidation
    - Solution: Stable Coins
- Scalability
    - Solution: Off-chain techniques such as state channels and side chains

System and Security Assumptions

DeFi Assumes Several Different Factors:

- Underlying structures are completely decentralized
- Transactions are immutable
- Transparency / Open Source Code
- Permissionless access

Research Methodology

High-Level Idea and Intuition

- Theoretical Analysis of Four Protocols
  - Uniswap
  - Kyber Network
  - Curve Finance
  - Protocols
- By understanding the protocols we can gain insights

Analysis of Protocol Designs

- Focus on 6 main features
  - Operational Efficiency
  - Security Infrastructure
  - Risk Exposure
  - Liquidity
  - User Adoption
  - Protocol Governance

Implementation and Experiments

Uniswap V3 Protocol

Implementation Details

- Implemented in Solidity
- Automated Market Maker
- Used primarily for the Ethereum blockchain on the Ethereum Virtual Machine (EVM)
- Focus on security

Evaluation Metrics

- Operational Efficiency
  - Automated Market Maker Model
  - Concentrated Liquidity
- Security Infrastructure
  - Open Source Smart Contracts
  - Audits by Third Parties
  - Bug Bounty Program
- Risk Exposure
  - Impermanent Loss
  - Security Flaws from the EVM
- Liquidity
  - Determined by total value of the liquidity pools

- Slippage
  - Potential Risk with low liquidity
- Price Oracle Accuracy
  - Used to track the geometric Time Weighted Average Price (TWAP)
  - Update over V2 which used TWAP
  - More accurate
- User Adoption
  - Most popular AMM on Ethereum
  - In March 2024
    - Roughly $90 billion in monthly volume
    - Liquidity of about $7.2 billion
- Protocol Governance
  - Governed by UNI (Uniswap token) ticket holders
  - Decentralized governance
  - Theoretical risk of a Sybil attack, but unlikely due to scale

Kyber Network Protocol

Implementation Details

- Allows for instant decentralized token exchange
- Primarily operates on the Ethereum blockchain
- Powered by contracts
- Uses a reserve of tokens held by Reserve Entities

Evaluation Metrics

- Operational Efficiency
  - On-Chain
  - No order book is needed
  - Token swaps can be performed in a single transaction
- Security Infrastructure
  - Built on the Ehtereum Blockchain
  - Security benefits, and downsides of Ethereum
  - Less control, if Ethereum makes a change to the blockchain
- Risk Exposure
  - Reduces risk of counter-party default
  - Potential vulnerabilities in the smart contracts
  - Third Party Audits were conducted
- Liquidity
  - Aggregates liquidity from various sources
  - Ensures network can provide competitive rates
  - Anyone can contribute liquidity, and individuals are incentivized to

- Slippage
  - Very low risk due to liquidity coming from various sources
- Price Oracle Accuracy
  - Provides a price feed on-chain
  - Resistant to price manipulation
- User Adoption
  - Widely adopted due to versatility
  - Can be used for more than Ethereum
- Protocol Governance
  - Decentralized and governed by users
  - Votes on proposals, and changes to network, and the parameters

Curve Finance

Implementation Details

- Protocol on Ethereum blockchain
- Uses Solidity for smart contracts
- AMM model of stablecoins
- Dynamic liquidity pool adjustments
- Rates correlate with market rates

Evaluation Metrics

- Operational Efficiency
  - Optimized AMM algorithm for stablecoins enhance operational efficiency
  - Focus on stablecoin market ensures low volatility and predictable returns
- Security Infrastructure
  - Regular audits, community governance, and insurance boost security
  - Stable trading limits volatility, enhancing safety
- Risk Exposure
  - Exposure to smart contract vulnerabilities, liquidity risks, and regulatory changes
  - Systemic risks from integration with other DeFi protocols
- Liquidity
  - Users deposit assets to earn fees and CRV tokens
  - Decentralized governance by CRV holders supports adaptability and security
- Slippage
  - Focuses on stablecoins and assets of similar value
- Price Oracle Accuracy
  - On-chain price feed
- User Adoption
  - Widely adopted due to versatility
- Protocol Governance
  - Decentralized Autonomous Organization (DAO) model

Balancer

Implementation Details

- Protocol on Ethereum blockchain
- Primarily implemented using Solidity, leveraging smart contracts
- Automates and optimizes stablecoin trading
- Utilizes an automated market maker (AMM) model specifically designed for stablecoins
- Features a reserve of various stablecoins
- Dynamically adjusts the liquidity pool to ensure rates on the platform closely match actual market rates

Evaluation Metrics

- Operational Efficiency
  - Allowing up to eight different token weightings
  - Intelligent order routing for best price execution across different pools
- Security Infrastructure
  - Regular audits by top firms and a modular architecture to minimize risks
  - License-free and custodial-free features
- Risk Exposure
  - Faces risks from smart contract vulnerabilities, market volatility, and regulatory changes
  - Dependence on external price predictions and fluctuating asset prices

- Liquidity
  - Allowing the creation of muti-asset liquidity pools with customizable ratios
  - Dynamic fee adjustment mechanism
- Slippage
  - Combination of customizable pool weights and dynamic fees ensure competitive slippage
- Price Oracle Accuracy
  - Integrates with Chainlink
  - Utilizes multiple independent pricing sources
- User Adoption
  - Approximately 25,000 liquidity providers
  - $3 billion in locked liquidity
- Protocol Governance
  - Decentralized Autonomous Organization (DAO) model

Conclusion

- DeFi Protocols: No single solution exists for all protocol-related issues
- Third-Party Vetting: Protocols are thoroughly vetted by third parties
- Common Risks: All protocols face risks
- Liquidity Strategies: Aggregating from various sources versus using multi-asset liquidity pools
- Slippage Reduction: Methods vary
- DeFi Landscape: Continuously evolving
- Future of DeFi: Continuous risk management is crucial

Questions?