Financial Risks

The financial risks in DeFi provide insights on better use of DeFi platforms and services. For example, developers should focus on the right thing and reducing the financial risks for customers through the facility of correct advice and implementation of modifications in their DeFi application.

Financial risk points out to the risk of losing money, and every user is responsible for understanding financial risk through an impression of their appetite for reward and risk. On the other hand, an enterprise would focus on financial risk by balancing money management based on business operations.

Liquidity: The fragmentation of a liquidity pool between many different protocols can lead to a low liquidity market within individual groups. That can lead to a big "slippage", where the quoted and strike prices are different, in a single transaction. Or if a user prefers to transact through different protocols, the transaction fee will be much higher.

Q 1. What financial risks are your biggest concern?

Opt1. Market Liquidity(when people want to exit their investments in a timely and effective manner.)

Opt2. Centralization risk

Opt3. Crypto volatility

Opt4. Other

Q2. Which ones do you consider most important financially when investing in defi?

Opt1. Risk management

Opt2. Trade execution

Opt3. Custody

Opt4. Other

Technical Risks

Technical risks in DeFi primarily arise from the issues with protocols, hardware, and software. The threat of technical risks is paramount as they can compromise the functionality of the complete platform.

Smart contract risks: include dependency on timestamp, front-running, inadequate gas griefing, integer underflow and overflow, and forcible transmission of ether to a contract. In front-running risk, hackers can leverage transactions mempool to take an unincluded block and make their desired modifications.

Hardware risks: are also important technical risks in DeFi, especially with hardware serving as the foundation of infrastructure to run decentralized services. The common hardware risks related to DeFi systems include sensitivity, power issues, and incompatibility.

Software risks: are also one of the crucial technical risks when it comes to DeFi. The general risks for DeFi software include Distributed Denial of Service or DDoS attacks, injection, uncontrolled format strings, and overflow. DDoS is a credible mention among techniques for disruption of the normal functioning of an app or service.

Q3. What technical risks do you consider to have when investing in DeFi?

Opt1. Smart contracts vulnerabilities

Opt2. Hardware (Wallet integration, Protocols)

Opt3. Software

Opt4. Other

Best Practices to Deal with DeFi Risks

The detailed impression of the risks associated with DeFi point towards the need for security of digital assets. The recommendations and best practices to avoid the risks with DeFi can serve dominant benefits for security and protection.

Q 4. The best practice to avoid risks in defi is:

Opt1. Choose Trustworthy Products and Services

Opt2. Leverage the Power of Multi-Factor Authentication

Opt3. Never Show Your Digital Assets

Opt4. Security for Digital Assets(hot and cold storage)

Opt5. Updates and Backups

Opt.6. Other

https://medium.com/coinmonks/2020-defi-bible-5-must-knows-before-you-enter-the-defi-space-2f9fe87c0e95

https://www.parafi.capital/

https://panteracapital.medium.com/

https://moonrockcapital.medium.com/moonrock-capital-invests-in-kylin-network-kyl-ed27a5830cbf

https://academy.ivanontech.com/blog/defi-deep-dive-on-chain-analysis-and-defi