**Sumary**

The research looks for the following declarations from the institutional investors(individual and organizations). With these declarations, we looking to recognize the risk when they fund a project on defi.

* Define the risk parameters - Financial & Technical

**Institutional investors**

An institutional investor is a company or organization that invests money on behalf of other people. Mutual funds, pensions, and insurance companies are examples. Institutional investors often buy and sell substantial blocks of stocks, bonds, or other securities. The group is also viewed as more sophisticated than the average retail investor and, in some instances, are subject to less restrictive regulations.

**Risks for investing in DeFi**

**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 adviceand 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: t**he 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 high.

**Centralization:** many of the protocols within the DeFi space are dependent or make use of a centralized tool. Due to the very nascent nature of the DeFi sector, the developing teams have systems in place that confer certain power to a centralized party to reduce inefficiencies or reduce attack vectors.

Ironically, while these centralized systems provide the developing platform with some advantages, they are also a significant risk for the functioning of the ecosystem.

Take, for instance, Oracles, which are leveraged by a number of Automated Market Makers (AMMs) and decentralized exchanges (DEXs), typically receive data from a single source. This can pose a risk as it is trivial for a malicious party to take control of the singular source of data and manipulate the market to their profit.

While it is important to note that most developer teams are focused on phasing out the centralized aspects of their ecosystems over time, these tools still pose risks while they are in place. According to the Cryptoasset Benchmarking Study, “Oracles, either hardware or software, funnel real-world data to the smart contract. As several attacks targeted at decentralized protocols have shown, oracles are a possible source of systemic risk and their data feeding role is prone to manipulation.”

**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.

### **Procedural Risks in DeFi**

The final entry among the risks points out to procedural risks. Interestingly, procedural risks primarily focus on the different security risks associated with DeFi products and services by users. The most common security risks in DeFi include phishing attacks in which a malicious agent duplicates a website or service to lure unsuspecting users into sharing their sensitive information.

Phishing attacks are also possible through emails in which users are sent an email mirroring that of service providers. As soon as the user clicks on the email, they are redirected to a malicious website. On the other hand, the phishing email can run malicious code in browser for adding keyloggers in the victim’s system.

The hacker could then leverage sensitive information for transferring funds or conduct illegal transactions without the knowledge of the user. Such phishing attacks are widely known across the cryptocurrency community, with hackers posing as representatives of a concerned DeFi service.

The understanding of procedural risks in DeFi should also accommodate other notable procedural hacks. The risks include baiting, pretexting, SIM-swapping, spearfishing, quid pro quo, and tailgating. Pretexting involves a hacker posing as a representative of a DeFi service and convincing users to share sensitive information. Baiting risks arise with ‘bait and switch’ methods for infection of a web page.

Spear phishing can present threats to the whole enterprise as it targets individuals in the organization for attacking the system. Spear phishing involves gaining system access to any person to control the core system functionalities and data. Quid Pro Quo risks are somewhat same as baiting; however, with the difference of hackers providing large incentives for motivating victims to work according to their wishes.

SIM-swapping is a dominant procedural risk found with DeFi, especially due to the use of personal information of users for creation of new SIM from concerned mobile service providers. Hackers can use the counterfeit SIM for committing illegal activities in the name of the user. Tailgating is one of the dominant risks in DeFi when it comes to accessing real-world locations by tricking a person in a superior position.

**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.

The first and foremost recommendation to avoid risks in DeFi is the use of trusted products and services. Users should look for recommendations and reviews about a specific DeFi product or service before finalizing it. In event of any discrepancies in trust with a specific DeFi product or service, take a step back.

Multi-factor authentication is a formidable tool for ensuring security, especially with different credible verification methods. For example, email confirmation, two-factor authentication, or multi-signature authentication are some of the proven recommendations to avoid DeFi risks.

Users should always refrain from showcasing details of their digital assets to ward off the attention of hackers on them. keep your digital assets confidential just as you keep other high-end personal data and you will be successful in avoiding the risks.

The security of digital assets can play a huge role in resolving threats of various risks in DeFi. Hot and cold storage are ideal choices for security of digital assets. Hot storage serves as an ideal wallet solution for actively accessing DeFi services. On the other hand, cold storage enables offline storage of digital assets to prevent the attention of malicious agents.

Backups and updates are also recommended best practices for keeping the risks related to DeFi to a minimum. Enterprises introduce new updates and patches in DeFi solutions for improving its security. Therefore, regular updates of DeFi software can take off the risks of new vulnerabilities. Furthermore, backups of digital assets on a different drive or in a diary can ensure higher availability of digital assets.

**Research Method**

Available online resources where they have presented their view like on Twitter threads, Medium posts, podcasts, YouTube videos that presents the thoughts on risks in DeFi in their view and what is important to them when they are looking to invest in DeFi.

**Researcher**

Manuel Rios.

**Resources and Investors**

* [Coinmonks Medium](https://medium.com/coinmonks/2020-defi-bible-5-must-knows-bef%20ore-you-enter-the-defi-space-2f9fe87c0e95)
* [Parafi Capital SIte](https://www.parafi.capital/)
* [Pantera Capital Medium](https://panteracapital.medium.com/)
* [Moonrock Capital Medium](https://moonrockcapital.medium.com/)
* [Defi Prime site](https://defiprime.com/risks-in-def)
* [Dragon Fly Capital Site](https://www.dcp.capital/)
* [Electric Capital](https://www.electriccapital.com/)
* [Electric Capital Youtube Video](https://www.youtube.com/watch?v=vfEYeKGqhMg)

**Links to PDF and Google Form survey**

* [PDF Survey](https://github.com/ManyRios/Subtask-1.1---Design-User-Survey/blob/main/Survey.pdf)
* [Google forms link](https://docs.google.com/forms/d/1iLq5PCVrx1qXWUIhZ3ontddeRXQDZ6_abjqXp1sUJ9I/edit?usp=sharing)