

dgen.capital

RISK MANIFIESTO

Overview

The following is a short description of identified risks by dgen.capital. It is important that users understand the potential risks before providing assets to different protocols as we will not take any liability or responsibility for issues arising due to these risks, as for example, complete loss of assets.

dgen.capital does a thorough review and examination of every protocol it is involved with, however even with the best reviews, audits and intentions the opportunity for them to occur is high given the initial phase blockchain is and how premature concepts & technology as DeFi are.

DYOR
(do you own research)

Topics addressed

1. Smart Contract risk
2. Downstream Smart Contract risk
3. Smart Contract Owners risk
4. Stablecoins unpegging from FIAT
5. Variable APY
6. Centralized vs Decentralized stablecoins
7. Scalability / Gas prices
8. Your Wallet Security
9. Governance Risk
10. BTC dominance
11. Regulators

1. Smart Contract risk

All these protocols are governed by smart contracts written in Solidity. As with any software program these may be prone to bugs, errors or even malicious code that deviate from its intended functionalities.

The consequences may vary from malicious people being able to drain funds to the funds getting locked forever in the smart contract itself.

The best way to protect yourself against this risk is to review the audits performed on the code, as well as the time these contracts have been deployed and the amount of funds managed over time.

2. Downstream Smart Contract risk

Many of these protocols actually leverage and make use / integrate other smart contracts created by other people & organizations. Therefore these risks multiply and should be properly understood and reviewed.

3. Smart Contract Owners risk

Every smart contract has an Owner or sometimes referred as the Controller., This Owner is a wallet belonging to someone or more people as smart contracts may have multiple Owner wallets. It's normal that Owner wallets are able to make configuration changes to the contract, and these can vary from small parameters to the ability to change the functionality of the smart contract.

A good way to address this risk is to understand and review what these Owner wallets are allowed to do & change in the protocol. Making sure that the Owner Wallet is a multisig owned by multiple people together with time delays for any changes in smart contract configurations are also a good indication of trustworthy principals.

4. Stablecoins unpegging from FIAT

Most stablecoins used are "soft pegged" to some FIAT value, in most cases USD. This means that their value varies at any time around \$1, normally those variations are quite small ~\$0.01 or less below or over \$1.

When an asset is in big demand the value may rise over \$1, but when there is an over supply of the asset, it may move under \$1. This is the reason when you calculate the USD value of your stablecoin investment over time that it may vary.

A good mitigation of this risk is to distribute your funds over multiple stablecoins. Also when entering or exiting a position look at the price of the stablecoin.

5. Variable APY

APY or Annual Percentage Yield is the current yield an asset is receiving. Given the nature of blockchain technologies this yield is paid off every second, and the APY itself is changing constantly depending on demand & supply. The APY may vary in a given minute or hour from 5% to 100% or even more. This constant fluctuation in APY makes it very difficult to accurately calculate and estimate what your ROI will be in 1 year or even 1 month.

6. Centralized vs Decentralized stablecoins

It is important to understand the difference between centralized and decentralized stablecoins. Centralized ones such as USDC & USDT mean that they are backed by FIAT held by a centralized organization/company. In the case of USDC each token is backed 1:1 by \$1 USD. In the case of USDT it is quite unclear, but the community believes that only a certain % of tokens are backed by actual USD.

Decentralized stablecoins like DAI or sUSD on the other side are not backed by FIAT. These are collateralized assets. For example DAI is collateralized by ETH at a 150%, meaning that for each DAI there is \$1.5 (in ETH) in collateral, which is managed by a smart contract (MakerDAO). sUSD works in a similar fashion but collateralized by SNX at a %600 rate.

The problem with centralized stablecoins is the fact they are managed by centralized companies subject to regulators. While this can be seen as a benefit and security, it also means that they can blacklist wallets or remove/block funds if they have a reason to do so or mandated by regulator/law. Decentralized stablecoins remove that risk, but introduce another risk, the unfortunate situation in which the asset becomes uncollateralized, for example in the case of DAI, if the price of ETH falls too much and the owners of those collateral contracts do not manage their collateral ratio, DAI may become uncollateralized and therefore losing their peg.

7. Scalability / Gas prices

It is no secret that current public blockchain technologies are not yet scalable to handle the amount of transactions needed to handle massive adoption. Lots of solutions are in the works and being tested like Layer 2 solutions, sidechains and moving from PoW to PoS or PoA.

The implications of a saturated network, among many others, are the increase in transaction fees aka Gas. Gas changes depending on the demand for the network in a dutch auction style, users send transactions with a certain amount of Gas, which is what miners gain for executing transactions. Therefore, whenever the network is saturated, miners will choose the highest Gas bidder and execute their transaction. This ends up in a Gas bidding war, where users increase the Gas price in order for their transactions to be executed faster.

From a normal user perspective this can imply that your transactions will take some time to execute unless you increase the Gas price, resulting in a potential disadvantage for example if you're trying to do arbitraging. Also, if you're trying to invest small amounts in a DeFi protocol, this may not make sense if you need to pay \$30-\$60 in Gas just to get in. Therefore we have minimum amounts for each investment pool.

Calculating the current value of your assets

An accurate calculation of the current value of your assets is a very difficult thing to track given the multiple protocols those assets may be distributed to, especially if you're looking to understand the USD value of that asset.

We've explained a couple of these issues above, like the fluctuation of stablecoins price, variable and ever changing APY, gas fees needed to be paid for withdrawing assets from multiple protocols, as well as being able to calculate the rewards or interest earned. Depending on the protocol these are clear and easy to track, but in other cases you won't know until you have fully withdrawn your assets from the protocol.

8. Your Wallet Security

One of the most, if not THE MOST important aspect is your wallet. Your wallet is the only way to manage, use and retrieve your funds. You lose access to your wallet, you lose all your assets in that wallet. There is no way to recover them.

Wallets are protected by private keys or a mnemonic. You should always keep these secret and safe, as well as backups of these in a safe of sorts. You can also make use of Multisig wallets, which mean that multiple wallets are required to sign a transaction before it executes.

For example, in dgen.capital we have a 3/6 multisig, meaning that we have 6 wallets (owned by us and secured in different parts of the world by us), these 6 are allowed to sign transactions, however only 3 are required. No single person has more than 2 allowed wallets, therefore at least 2 people are required to sign with their wallets in order to execute a transaction. This is also secured against the risk of someone losing access to their keys, very similar to how bank safes work.

9. Governance Risk

Many of these protocols were created by 1 or more people, however they later delegate the governance (changes to the protocol & smart contracts) to the people via a DAO. These people belonging to the DAO are normally users of the protocol, and they vote for changes to the protocol before they are allowed to be implemented.

It is important to review the structure of the DAO, especially how distributed the voting rights are and what are the thresholds. A red flag would be to see that 1 wallet owns more than half of the supply of governance tokens, allowing it to approve changes as they have the majority.

10. BTC dominance

Unfortunately BTC still dominates the crypto market. At the time of writing BTC represents ~60% of the Crypto Market Capitalization. Therefore when investing in crypto & DeFi you should try to always think in crypto and not in USD terms (except in the case of stablecoins)

You may be making great winnings and the interest received in DeFi protocols may be great, but these are always in respect to their own asset. Therefore you may have increased your BTC amount, but in terms of USD it may have fallen in price.

Recommendation: Take profits frequently!

11. Regulators

While most Regulators around the world have not been taking drastic measures towards crypto assets so far, there is always the risk the Regulator in your country may prohibit, ban or even declare a crime to hold cryptocurrencies.

You should always remain informed of the latest regulations and tax implications, if any.