Savings Vault Risk Disclosures

Revix SA OpCo Proprietary Limited

South African company number 11713189

Last update: **May 2022**

Risks Relating to the Use of Savings Vaults

By using Revix's Savings Vaults, you acknowledge, understand and assume the risks outlined in our General Risk Disclosures, Cryptocurrency Risk Disclosures as well as all risks outlined below.

Before using any of our (Revix's) services, you should ensure that you fully understand and can afford to undertake the risks involved in investing in cryptocurrencies. Please do your own research and consult a financial advisor before making any investment decisions.

1. Company-Specific Risk

Investing and earning through any platform operated by a company — such as ourselves, other fintechs and even banks — carries some degree of risk. The risks associated with any company depends on the solvency of the firm and the company's ability to pay off all creditors with its assets and manage liquidity effectively.

2. Counterparty Risk

Any loan agreement, in or out of the DeFi ecosystem, involves counterparty risk, which is the risk of loaning money to someone who does not repay. Most of the large DeFi lending protocols, including Aave, Compound, and Maker, require that borrowers over-collateralise their loans, meaning that borrowers must provide collateral worth over 100% of the borrowed amount.

Before we utilise in a DeFi lending protocol, we make sure to understand how well the loans are collateralised, and what quality of collateral is provided by borrowers.

3. Yield Risk

Decentralised Finance (DeFi) protocols are still maturing and the yields offered through lending protocols vary based on market conditions. The risk is the uncertainty of future yields.

4. Software Risk

DeFi protocols are software applications that run on the internet, generally with very little human oversight, and often with millions or billions of dollars flowing through them. Like all software, DeFi protocols have two main software risks – coding errors, "bugs," that may cause the software to malfunction, and security vulnerabilities that allow thieves, "hackers," to break in and steal funds from the protocol.

There is no guaranteed method to avoid Software Risk in a DeFi investment, but there are ways to reduce it. You may notice that brand new DeFi protocols offer extremely high rates of return on investments, sometimes 1,000% or 2,000%. While those numbers are enticing, remember that the higher the investment return, the higher the risk.

In general, DeFi protocols with higher deposits and longer track records may have less Software Risk than newer or smaller DeFi protocols. This is because a new piece of software is like a new car model – it takes time for the engineers to work out the kinks.

Longer running DeFi protocols have had more time to discover and repair problems with their software. And larger protocols are more likely to attract negative attention from hackers than smaller protocols. You can assume that larger protocols face frequent, if not constant, attacks on their security. If they have operated for months without suffering a security failure, it may suggest that their software security is reasonably sound.

To mitigate this risk, we at Revix only engage with smart contracts that have been thoroughly reviewed, audited and have substantial track records.

5. Price Risk

As long as you hold crypto — including stablecoins — you risk price risk, meaning that you are liable to the risk of losing your money if prices decline. Price changes happen every second in the crypto market. If the price of the cryptocurrencies you own loses value you would lose some or all of your money,

6. Risk of Hacking and Security Weakness

Cryptocurrencies may be subject to expropriation and/or theft if not securely custodied. Hackers or other malicious groups may attempt to obtain access to cryptocurrencies held in custody in a variety of ways, including, but not limited to,

malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing.

Where Revix's crypto wallets are accessed by third parties, we use leading wallet infrastructure providers, use cold storage reserves, and diversify our cryptocurrency reserves to protect the security of your funds. We have never been hacked because of our best-in-class security practices.

7. Risk of a Stablecoin’s Peg Breaking

Stablecoins are intended to maintain a consistent relative value to another asset, such as the US dollar. If the stablecoin cannot maintain its value relative to the assigned asset, investors may lose trust in it, potentially causing its value to decline.

In case there is a break in the peg, an investment may be temporarily or permanently impaired.

8. Notice Period Risk

Crypto Saving Vaults have 24-hour unlock periods which can have an impact on your liquidity.

9. Regulatory Risks

Currently, DeFi protocols operate with almost no government oversight or regulation from any government entity. Simply put, this situation could change, and it is impossible to predict how any new government regulations of DeFi protocols might affect your DeFi investments.

10. Unanticipated Risks

Cryptocurrencies are a new and untested technology. There are other risks associated with the use of cryptocurrency that cannot be anticipated.