Smart contract risk

The Volt system utilizes smart contracts such as the Peg Stability Module (PSM), which allows users to execute swaps between stablecoins and Volt. A bug in a smart contract can result in total or partial loss of funds. The Volt team has taken extreme measures to ensure that smart contract bugs do not make it into production. All code has been mainnet fork tested that simulates the state of mainnet when the contracts go live. Extensive code and architecture reviews are performed internally and externally before any contracts enter production. Furthermore, Volt Protocol conducts security reviews of all integrated protocols. Each pull request in the Volt Protocol github has an associated review log, and system-wide audits are available at https://github.com/volt-protocol/volt-protocol-core/tree/develop/audits

Despite these measures, no amount of security is infallible. As a user, you should be aware of the risks associated with the Volt smart contract system. Volt is an early stage experimental smart contract system and using it could result in a total loss of funds due to various risks materializing.

Principal risk

This form of risk occurs because there is a chance an asset held by VOLT loses value, such as a stablecoin breaking peg, or bad debt in a lending market. Any smart contract system or on chain yield venue has a risk of loss. The Volt team takes this risk very seriously and will never include undercollateralized or low quality stablecoins in the Protocol Controlled Value. Furthermore, Volt Protocol maintains reserves to help protect VOLT holders from loss. If a loss exceeds the reserve buffer, then the Volt system would become under collateralized and need to pay out users on their pro-rata share of the Protocol Controlled Value (PCV) instead of the current target price.

The Volt team conducts economic diligence before depositing PCV into external protocols or yield venues. All such research is publicly available on the community forum. For example, see this thread on Maple Finance Venue Onboarding:
https://community.voltprotocol.io/t/vip-xx-maple-venue-onboarding/27

Despite the presence of the surplus buffer and scrutiny into venues, it is impossible to guarantee that VOLT holders never take a lending loss. Be aware of the risk in the system and join the conversation on the community forum to shape the future of VOLT.

Key compromise risk

The Volt system is controlled by a multisignature smart contract wallet whose signers include core team members and advisors. This wallet is controlled by EOA's. If enough of these EOA's are compromised, the system would be drained of its funds, making Volt unbacked. Since the

core team is globally distributed, the signing keys are never physically in the same location. Likewise, the Governor Multisig could take malicious actions resulting in the loss of user funds.

Yield venue liquidity risk

Volt Protocol deposits PCV into various yield venues, some of which may not be instantly liquid on demand. If there is extremely high demand to redeem VOLT while part of the backing is in illiquid venues, it would put the peg at risk. For this reason, the amount of PCV in illiquid venues is limited based on the size of the surplus buffer, which can be used to offer a higher VOLT rate and defend liquidity at peg.