THOMSON REUTERS
PRACTICAL LAW™

Introduction to Flash Loans: Legal and Business Considerations

by Sumeet Chugani, Coinbase, and Robin Nunn, Morgan, Lewis & Bockius LLP, with Practical Law Finance

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/W-035-3468**
Request a free trial and demonstration at: **us.practicallaw.tr.com/practical-law**

This Note provides a basic introduction to flash loans, a decentralized finance (DeFi) tool that permits issuance of an instantaneous uncollateralized loan of cryptocurrency for a limited period. The Note also examines the 2022 Beanstalk Farms flash-loan attack, as well as important considerations for parties providing access to flash loans.

A flash loan is a DeFi ecosystem tool that permits issuance of an instantaneous (and thereby, ideally, zero-risk) uncollateralized loan of cryptocurrency for a limited period. Flash loans typically bypass traditional credit metrics such as credit scores used to assess suitability, because the smart contract guarantees that the lender will be repaid. Because payback is both imminent and recorded, flash loans can be in the amount of the crypto equivalent of millions of USD.

Flash loans provide short-term liquidity and are commonly used to take advantage of price arbitrage opportunities. This type of loan is possible because, on a blockchain, several transactions can be lined up and grouped, allowing for a smart contract to peek into the future and loan tokens that are paid back as part of the same transaction in split seconds. For example, a trader could propose the following smart contract transaction:

Smart Contract	*-> Loan 1,000,000 ABC Token to Trader*
Trader	*-> Pay Smart Contract $10 flat fee*
Trader	*-> Sell 1,000,000 ABC Token on Exchange A at $10*
Exchange A	*-> $10,000,000 to Trader*
Trader	*-> Buy 1,000,000 ABC Token on Exchange B at $9*
Trader	*-> Repay 1,000,000 ABC Token to Smart Contract*

The trader receives a $1 million token-based flash loan in the first step of the smart contract and pays it back in the final step. Since these component transactions are all grouped in the same block, they happen in a "flash," and the smart contract confirms payback through the blockchain. There is limited slippage risk since these component transactions are all part of the same proposed transaction on the blockchain, and the proposed transaction is crafted in such a way that if any single step fails, the transaction will not go through.

Beanstalk Farms

Beanstalk Farms (Beanstalk) is a stablecoin protocol that uses a decentralized credit system to issue stablecoins called $BEAN tokens. By eliminating collateral requirements, Beanstalk aims to act as the catalyst for a trustless solution to unlock DeFi potential. Beanstalk is also a decentralized autonomous organization (DAO) with no centralized authority. Individuals can buy governance tokens that allow them to make decisions for the organization. Any person holding or controlling at least 0.1% of the governance tokens can make governance proposals in the Beanstalk DAO, and any proposal that receives two-thirds of Beanstalk's governance token votes is approved and implemented into the Beanstalk protocol. This unique decentralized governance system is what made Beanstalk popular among its users, but it also left Beanstalk vulnerable to a flash loan attack.

Beanstalk Flash-Loan Attack

On April 17, 2022, Beanstalk fell victim to a flash-loan attack. The attacker drained approximately $182 million in cryptocurrency through an end-around of Beanstalk's governance model, coupled with a new arbitrage strategy referred to as the "flash-loan end-around strategy." The attack occurred when a user obtained a flash loan for approximately $1 billion. The attacker wrote a smart contract to obtain the loan in such a way that the funds would be used to acquire two-thirds of the Beanstalk governance tokens.

Upon acquiring two-thirds of the governance tokens, the attacker was able to single-handedly pass new governing protocols for the Beanstalk DAO, which permitted a large

amount of the assets in Beanstalk's proprietary account to be sent to an outside and independent crypto wallet. The same smart contract then returned the borrowed funds from the flash loan leaving the attacker with the siphoned Beanstalk funds.

Due to the nature of flash loans, the entire process of obtaining the loan (passing the protocol that allowed the attacker to siphon the Beanstalk assets and repaying the loan) all occurred within about ten minutes. The attacker then moved the funds received in the attack to the cryptocurrency mixing service Tornado cash. Following the flash loan attack, $BEAN plummeted from a valuation of $1 to approximately 20 cents. A fundraiser for Beanstalk is underway.

Flash-Loan Attacks: Lessons and Takeaways

This type of attack on a blockchain is not new, and Beanstalk is unlikely to be the last protocol victim; certainly this will not be the last misuse of a smart contract protocol in the blockchain space. This attack is a reminder of the importance of technical, governance, and legal due diligence for both DeFi protocols and users in this space. It also raises user-protection issues for decentralized exchanges, open-source liquidity protocols, and their users moving forward.

The Beanstalk attack should also serve as a reminder of the importance of diligence in DeFi investment and creation. Where possible, project code (both on-chain and off-chain) should be audited and include functionality to address newly discovered vulnerabilities. Governance in the new age of DAOs must also be tightly reviewed and stress-tested against exploits like flash-loan attacks. For example, DAOs may require funds used to gain governance powers in the organization to have a minimum vesting period in an effort to build community – and prevent flash loan attacks.

Another issue raised by the Beanstalk attack is who bears responsibility for funds stolen from the DAO. Unlike with a traditional finance model, no FDIC insurance or regulatory mandate requires payback to the DAO members. For Beanstalk, the entire community must share the loss.

Project operators (and investors) must consider their exposure from not only a technical perspective but also a legal one. In general, an organization soliciting deposits of assets, digital or otherwise, may owe a duty of care, which may be breached when it fails to patch governance or protocol deficiencies against known vulnerabilities or permits exploits on its protocol. The SEC's report on the Ethereum DAO hack in 2017 found that "the DAO" was an unincorporated organization, leaving the door open to an argument that its members were partners who could potentially face unlimited liability, see Legal Update, SEC Issues DAO Report Concluding Virtual Assets May Be Securities.

Although regulators primarily responsible for consumer protection, including the Consumer Financial Protection Bureau (CFPB), the Federal Trade Commission (FTC), and state regulators, have just begun to enter the DeFi space, exploits like the Beanstalk attack may intensify their involvement. As the space grows, the "buyer-beware" slogans of DeFi may need additional bolstering to sufficiently warn users about potential loss of funds or misinformation related to governance or protocol safety.

All participants in the DeFi ecosystem should begin to consider the range of applicable laws and regulations guiding their environment, as well as protections for users. User protection requires particular attention, since many DeFi players are retail users who do not require accreditation as sophisticated investors to participate in the DeFi market. Continued attention and improvement to protocols, audits, and vulnerability patching is essential to ensure user safety and mitigate the need for expanded regulation, which could handcuff future growth in DeFi.

Thanks to Jacob Minne and Bakari Ziegler of Morgan Lewis & Bockius, LLP for their contributions.