The bZx Attacks

Thematic Insights: February 2020

DELPHI DIGITAL

Table of Contents

Lead Analyst:

Anil Lulla

anil@delphidigital.io

Executive Summary

Earlier this month, the DeFi trading protocol bZX was exploited twice - resulting in almost $1 million of ETH stolen by the attackers. As we'll walk through this report, both attacks involved the respective trader astutely navigating a variety of crypto applications.

Flash loans were leveraged as a financing mechanism for both attacks. While we'll dive into these more in depth shortly, these essentially allow traders to open uncollateralized loans that are repaid in the same transaction as it's taken out. Due to this, the speed of these attacks was so fast because the loan, trade, settlement, and profits are executed simultaneously in a single transaction. Additionally, no upfront capital was needed - with the first attack costing $8.21 in network fees (this attack yielded ~$320K) and the second one costing a little over $100 in network fees (while this attack yielded over $600K).

We'll also examine the aftermath of these attacks, which involved the first payout ever from a decentralized insurance protocol. Our team has been working on two Thematic Insights reports on Insurance and Oracles, which will be out next month, but we thought a quick report walking through these two attacks would serve as a fitting prelude. We hope you enjoy the report, and feel free to reach out if you have any questions.

Used Before Attack*:

Used During Attacks:

Used After Attack*:

**Only used for first attack*

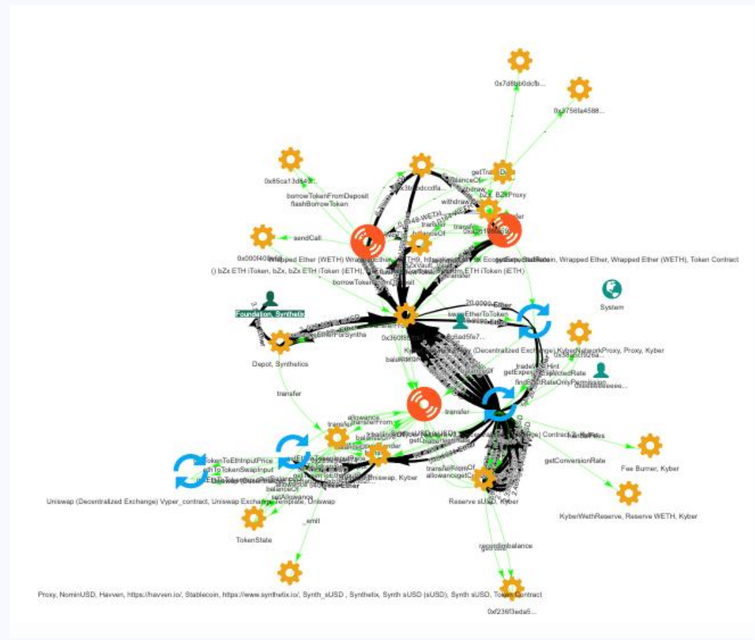
Flash Loans: Overview

In one of our first Thematic Insights reports, our team covered Decentralized Finance and stated that we were excited to watch as these applications recreated and improved upon the legacy financial system. We need to look no further for this anticipated ingenuity than flash loans. Essentially, flash loans allow traders to open uncollateralized loans that are repaid in the same transaction as it's taken out. If the loan is not repaid within a single transaction, the transaction does not go through and is not finalized in the blockchain. In other words, this means that you don't need money to make money, opening up new possibilities that were not possible in crypto beforehand.

At its core, flash loans provide the ability to leverage uncollateralized DeFi capital in order to profit from a well-executed DEX trade. Flash loans basically have zero risk, because the money borrowed needs to be repaid within the same transaction (otherwise the transaction is automatically rolled back via a smart contract). Due to being able to leverage these with no upfront capital, flash loans dramatically reduce the barrier to take advantage of an exploit. Before flash loans, an attacker would most likely have to go through KYC to bring the necessary amount of capital on-chain to take advantage of a bug. Flash loans eliminate this and, by combining this product with privacy protocols such as Tornado Cash, attackers can remain anonymous before and after the exploit.

Our team believes this is just the beginning of the impact flash loans will have on the space. Overall, the introduction of flash loans to this market will help bolster the security assumptions behind these applications. We're seeing this play out in real time, and are excited to keep an eye on it.

bZx Attack #1 Transaction



bZx Attack #2 Transaction

Attack #1: Applications Used

Before we walk through the attack, we wanted to provide a quick refresher on each of the applications involved within the attack. All of these are built on Ethereum, which is why the composability between the projects was leveraged with each flash loan.

bZx is an open finance protocol that allows applications to be built on top of it. These include things such as shorting, leveraging, borrowing, and lending. Currently, there are two products built on bZx: a margin trading platform (Fulcrum) and a crypto borrowing platform (Torque).

Compound Finance is a lending protocol which enables users to lend and borrow some cryptocurrencies.

dYdx is a non-custodial cryptocurrency exchange. It supports trading on margin with up to 4x leverage through custom, non-tokenized, positions, as well as borrowing and lending with no minimums or lock up periods.

Kyber Network is an exchange protocol that aggregates token liquidity from a variety of sources, both internal and external, and uses it to facilitate token swaps.

Tornado Cash is a privacy mixer built for Ethereum. A transaction mixer essentially scrambles together the funds from multiple users and transactions, before each transaction reaches its intended destination. After mixing, it becomes difficult to trace whose money went where.

Uniswap is a protocol that pools token liquidity on-chain in smart contracts and uses it to facilitate token swaps. Uniswap is completely on-chain, and individuals can make use of the protocol as long as they have MetaMask installed.

Attack #1 Walkthrough

		Debt	Assets
1	Attacker gets a flash loan of 10,000 ETH from δY/δX	(10,000 ETH)	10,000 ETH
2	Attacker deposits 5,500 ETH to Compound and borrows 112 wBTC	(112 wBTC)	(5,500 ETH) +112 wBTC
3	Attacker deposits 1,300 ETH to bZx to open a 5X short position for wBTC. *For this to happen, bZx converts 5,637 ETH to 51 wBTC with Kyber (which in turn leverages its Uniswap reserves). The swap drives up the exchange rate of 1 wBTC to ~110wETH (2.85x the normal exchange rate of ~38.5 wETH/wBTC)*	(5,637 ETH)	(1,300 ETH)
4	The attacker now swaps the 112 wBTC borrowed from Compound (in Step 2) to 6,871 ETH on Uniswap *This is because the wETH/wBTC exchange rate got skewed in Step 3.*		(112 wBTC) +6,871 ETH
5	Attacker pays back the flash loan of 10,000 ETH from δY/δX	+10,000 ETH	(10,000 ETH)
	Balance (At this Point)	**(112 wBTC) (5,637 ETH)**	**71 ETH**
6	Finally, the attacker's Compound position has 5,500 ETH as collateral for a debt of 112 wBTC. Leveraging an average exchange rate of ~38.5 wETH/wBTC, the attacker is able to repay this 112 wBTC debt with only ~4,300 ETH and pocket ~1,200 ETH. *Since the bZx position (the debt of ~5.6K ETH) is in default , the attacker doesn't bother closing it.*	+112 wBTC	+1,200 ETH
	Final Balance	***(5,637 ETH)***	**1,271 ETH**

Tx: [0xb5c8bd9430b6cc87a0e2fe110ece6bf527fa4f170a4bc8cd032f768fc5219838]

Attack #2: Applications Used

Before we walk through the attack, we wanted to provide a quick refresher on each of the applications involved within the attack. All of these are built on Ethereum, which is why the composability between the projects was leveraged with each flash loan.

bZx is an open finance protocol that allows applications to be built on top of it. These include things such as shorting, leveraging, borrowing, and lending. Currently, there are two products built on bZx: a margin trading platform (Fulcrum) and a crypto borrowing platform (Torque).

Kyber Network is an exchange protocol that aggregates token liquidity from a variety of sources, both internal and external, and uses it to facilitate token swaps.

Synthetix is a protocol that facilitates the issuance and trading of synthetic assets (“Synths”). While the platform can provide on-chain exposure to fiat currencies, commodities, stocks, and indices, it’s currently limited to select cryptocurrencies & fiat.

Uniswap is a protocol that pools token liquidity on-chain in smart contracts and uses it to facilitate token swaps. Uniswap is completely on-chain, and individuals can make use of the protocol as long as they have MetaMask installed.

Attack #2 Walkthrough

		Debt	Assets
1	Attacker gets a flash loan of 7,500 ETH from bZx	(7,500 ETH)	7,500 ETH
2	Attacker swaps 900 ETH for 156,003 sUSD in a few batches through Kyber Swap *For this to happen, Kyber pushes through a first order of 540 ETH for 92k sUSD via their Uniswap reserve and then does the rest via their Kyber-sUSD reserve to get an additional 63,584 sUSD. The swap skews the exchange rate for sUSD; going from 1 ETH = 270 sUSD (normal rate) to 1 ETH = 111 sUSD.*		(900 ETH) +156,003 sUSD
3	Attacker sells 3,518 ETH through the SYNTHETIX Depot contract to acquire 943,837 sUSD at market price (which is due to the Depot contract having more liquidity to be accessed). *Now the attacker has over 1M sUSD (around 20% of the total supply), and has significantly drove up the sUSD/ETH price. The next step will be executing the oracle attack.*		(3,518 ETH) +943,837 sUSD
	Balance (At this Point)	**(7,500 ETH)**	**3,082 ETH 1,099,841 sUSD**
4	Since bZx queries Kyber for the current ETH/sUSD rate (which the attacker has successfully manipulated), the attacker is able to borrow a lot more ETH than they normally could by using sUSD as collateral. They send 1,099,841 sUSD and are able to borrow 6,796 ETH. They now can pay back the 7,500 ETH flash loan from Step 1., while walking away from their underwater bZx position (+1,099,841 sUSD/-6,796 ETH)	(1,099,841 sUSD) +7,500 ETH	(1,099,841 sUSD) +6,796 ETH (7,500 ETH)
	Final Balance	***(1,099,841 sUSD)***	**2,378 ETH**

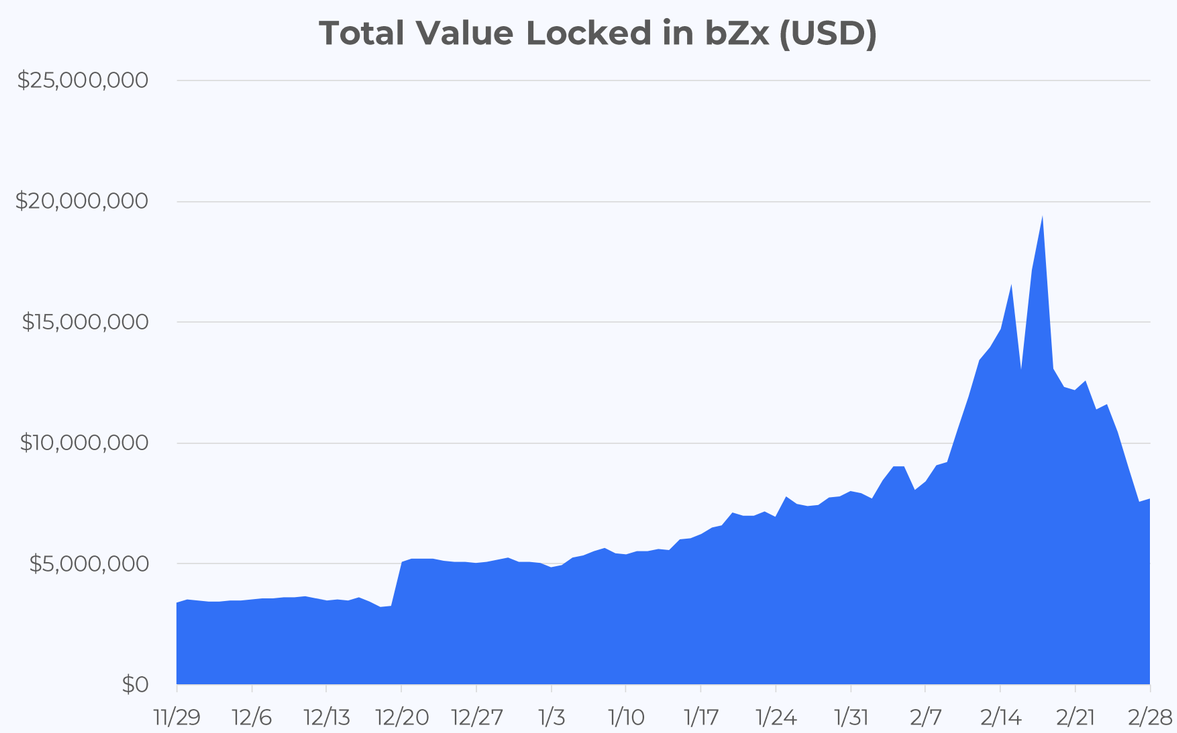
Tx: [0x762881b07feb63c436dee38edd4ff1f7a74c33091e534af56c9f7d49b5ecac15]

The Aftermath

Not surprisingly, the two attacks sent ripples throughout the crypto community as members attempted to make sense of what exactly had happened and how to prevent events like this going forward. The bZx team was able to quickly shut down Fulcrum using a master key, causing community members to question whether this qualified as “decentralized finance” at all. For the first attack, the team stated the collateral left by the attacker should be able to service the open loan and cover interest for an estimated ~200 years. At that point, the bZx team expects their insurance fund will be large enough to cover the loss or the company can use its own funds to cover the shortfall.

As you can see in the table on the upper right of the page, both attacks profits came at the direct expense of Fulcrum’s ETH lenders. If the collateral was liquidated at current prices, this still leaves a net loss of close to 4,700 ETH (or a little over $1 million). The attacks have left a lasting impact on the bZx protocol, as withdrawals have been significantly up over the past two weeks. Total Value Locked in bZx is down over 60% from its peak on February 18th of almost $20 million locked up.

	Attack #1	Attack #2
Amount of ETH Withdrawn by Attacker	4,337 ETH *($997,510)*	6,796 ETH *$1,563,080)*
Collateral Left by Attacker	51 WBTC *($448,800)*	1,099,841 sUSD *($1,033,850)*



Source: CoucourseOpen

The Aftermath

An interesting lense to better understand each attack is to understand whether Nexus Mutual would pay out claims related to these attacks. As a refresher, Nexus Mutual is an insurance company that works as a cooperative. At the moment, anyone can take out a policy against any valid smart contract on Ethereum (basically just betting against whether or not a smart contract will fail in some way). Essentially, token holders (NXM) govern the insurance pool - so in Nexus Mutual's case, holders vote to render a decision on each claim.

As we've now learned, in the first attack - the attacker simply used dYdX and Compound to get leverage. The position the attacker took on bZx causes a huge Uniswap skewing which the attacker then exploits. As soon as word of the attack got around, claims were made on the Fulcrum smart contract. Nexus Mutual holders subsequently denied these claims, since it seemed as if the attackers had manipulated the oracles Fulcrum referenced - which doesn't qualify as a smart contract failure itself.

Eventually, bZx's team published a "Post-Mortem" post outlining the attack as well as telling all their users that none of them have or will lose funds. Within this post, the team admitted to a fault in its code. Afterwards, the two users who had submitted the initial claims that had gotten denied resubmitted. This time, these were both approved by holders since the bZx team had clearly stated their smart contract had a bug.

For the second attack, the attacker simply took advantage of bZx's price oracle (Kyber, which subsequently got its price feeds from Uniswap reserves). Since this was chalked up as an oracle attack, Nexus Mutual did not pay out any claims in reference to this event. Shortly after, the bZx team met with Chainlink to expedite the addition of their oracle to their model.

Leader Commentary

Kyle J. Kistner
Founder of bZK Network

“This attack is one of the most sophisticated we’ve ever seen, possible only with an extremely in-depth knowledge of every DeFi protocol and its various tools. This attack demonstrates the power of composability and how many different protocols can interface meaningfully with bZx at the same time. Without tornado cash and flash loans, it would be difficult to have the anonymity or capital to pull an attack like this off. The space is evolving quickly, and security is becoming increasingly more dire as the barriers to entry to executing an exploit drop to zero. There is no analog to this in the traditional financial system. We are now in uncharted territories.”

Source: bZX Network Blog

“In both attacks, flash lending was just a financing mechanism for the attack – it was not materially apart of the vulnerability itself. A lot of people have been saying “we have to reconsider everything with flash lending in the game” and that “flash lending has changed the smart contract security assumptions”. I think it’s possible that some people were assuming that malicious users / hackers would not be well funded so therefore you should only worry about attacks that were possible without any up front funding – it’s clear that that was never a good assumption to make. With flash lending, it invalidates this assumption since you can now use smart contracts to fund your attacks.”

Source: Laura Shin’s Unchained Podcast

Lev Livnev
Formal Verification
Researcher at Dapp.org

Robert Leshner
Founder of Compound

“Security is the ultimate priority for a financial product. The bZx team has repeatedly demonstrated that it isn’t capable of protecting user funds, and should immediately cease operations until the platform can be thoroughly and completely audited.”

Source: The Block

Disclosures

The Research Team may own the tokens represented in this report, and as such this should be seen as a disclosure of any potential conflict of interest. Anyone can contact Delphi Digital for full token disclosures by team member at Team@DelphiDigital.io. This report belongs to Delphi Digital, and represents the opinions of the Research Team.

Delphi Digital is not a FINRA registered broker-dealer or investment adviser and does not provide investment banking services. This report is not investment advice, it is strictly informational. Do not trade or invest in any tokens, companies or entities based solely upon this information. Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. Investors should conduct independent due diligence, with assistance from professional financial, legal and tax experts, on topics discussed in this document and develop a stand-alone judgment of the relevant markets prior to making any investment decision.

Delphi Digital does not receive compensation from the companies, entities, or protocols they write about. The only fees Delphi Digital earns is through paying subscribers. Compensation is not received on any basis contingent upon communicating a positive opinion in this report. The authors were not hired by the covered entity to prepare this report. Delphi Digital did not receive compensation from the entities covered in this report for non-report services, such as presenting at author sponsored investor conferences, distributing press releases or other ancillary services. The entities covered in this report have not previously paid the author in cash or in stock for any research reports or other services. The covered entities in this report are not required to engage with Delphi Digital.

The Research Team has obtained all information herein from sources they believe to be accurate and reliable. However, such information is presented “as is,” without warranty of any kind – whether expressed or implied. All market prices, data and other information are not warranted as to completeness or accuracy, are based upon selected public market data, reflect prevailing conditions, and the Research Team’s views as of this date, all of which are accordingly subject to change without notice. Delphi Digital has no obligation to continue offering reports regarding this topic. Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances. The graphs, charts and other visual aids are provided for informational purposes only. None of these graphs, charts or visual aids can and of themselves be used to make investment decisions. No representation is made that these will assist any person in making investment decisions and no graph, chart or other visual aid can capture all factors and variables required in making such decisions.

The information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. No representations or warranties are made as to the accuracy of such forward-looking statements. Any projections, forecasts and estimates contained in this document are necessarily speculative in nature and are based upon certain assumptions. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond control. It can be expected that some or all of such forward-looking assumptions will not materialize or will vary significantly from actual results.

DELPHI DIGITAL

85 Broad Street
New York, NY 10004
www.delphidigital.io