

1 Jason Harrow
2 (Cal. Bar No. 308560)
3 Charles Gerstein
4 (*pro hac vice application forthcoming*)
5 GERSTEIN HARROW LLP
6 3243B S. La Cienega Blvd.
7 Los Angeles, CA 90016
8 jason@gerstein-harrow.com
9 (323) 744-5293

7 **UNITED STATES DISTRICT COURT**
8 **SOUTHERN DISTRICT OF CALIFORNIA**

9 CHRISTIAN SARCUNI, PEDRO
10 CUNHA, ALEXANDER LLOYD,
11 SKLIAR VIKTOR, MARC SIMON,
12 PILICI RUSTAM, DANIEL LU,
13 CLÉMENT OMÉTEK, EDISON
14 HO, KIRO ALEKSANDROV,
15 JONAS WERNECKE, PAOLO
16 LEITE, MIRAS ISSAKHOV, and
17 DANIELE PENNA, on behalf of
18 themselves and other similarly
19 situated,

17 Plaintiffs,

18 vs.

19 bZx DAO, KYLE KISTNER, TOM
20 BEAN, HASHED
21 INTERNATIONAL LLC, AGE
22 CRYPTO LLC, OOKI DAO,
23 LEVERAGEBOX LLC, and bZeroX
24 LLC,

24 Defendants.

Case No. [FORTHCOMING]

COMPLAINT '22CV0618 BEN DEB

CLASS ACTION
JURY TRIAL DEMANDED

Date: May 2, 2022

Preliminary Statement

1
2 1. This case arises from the use of novel cryptocurrencies, but it
3 is legally straightforward. First, the Plaintiffs in this case deposited
4 cryptocurrency with a protocol called bZx whose creators told users that
5 they need not “ever worry about . . . getting hacked or [anyone] stealing
6 [their] funds.” Second, despite this promise of security, the bZx protocol
7 in fact lacked reasonable safeguards and was hacked and the Plaintiffs’
8 funds stolen. Worse, the hack and subsequent theft were not the result
9 of some complex scheme or unknown vulnerability in the code, but rather
10 due to bZx’s simple negligence: by bZx’s own account, one of the bZx
11 developers fell for a so-called email “phishing” scam that permitted access
12 to key passphrases that then permitted the hackers to drain Plaintiffs’
13 accounts because the protocol had not yet implemented security
14 measures that its operators knew were reasonably necessary to protect
15 the protocol. The end result was a total theft of about \$55 million in US
16 Dollar equivalents: approximately \$1.6 million in total from these
17 fourteen named plaintiffs, and a substantial portion of the remainder
18 from a proposed class of similarly situated users.

19 2. The Defendants are jointly responsible for making good to the
20 Plaintiffs. Indeed, the protocol itself apparently acknowledges its
21 responsibility for the loss, though instead of making good, it has put in
22 place a woefully inadequate “compensation plan” where Plaintiffs could
23 receive IOUs with no real hope of repayment. Since the protocol has failed
24 to pay back what was taken as a result of the protocol’s negligence, all of
25 these Defendants are jointly and severally responsible for making good
26 to the Plaintiffs. That is because the bZx protocol purports to be a so-
27 called DAO, or de-centralized autonomous organization, that lacks any
28

1 legal formalities or recognition. There is another phrase in American law
2 for that kind of arrangement: general partnership. That means *each* of
3 the partners is jointly and severally liable to the Plaintiffs and must
4 make good on the full amount of its debts.

5 **Parties**

6 3. Plaintiff Christian Sarcuni is a bZx user who lost
7 approximately \$110,000 in the hack. He is a citizen of Italy.¹

8 4. Plaintiff Pedro Cunha is a bZx user who lost approximately
9 \$30,000 in the hack. He is a citizen of Portugal.

10 5. Plaintiff Alexander Lloyd is a bZx user who lost
11 approximately \$30,000 in the hack. He is a citizen of Canada and the
12 United Kingdom.

13 6. Plaintiff Skliar Viktor is a bZx user who lost approximately
14 \$450,000 in the hack. He is a citizen of Ukraine.

15 7. Plaintiff Marc Simon is a bZx user who lost approximately
16 \$80,000 in the hack. He is a citizen of France.

17 8. Plaintiff Pilici Rustam is a bZx user who lost approximately
18 \$800 in the hack. He is a citizen of the Republic of Moldova.

19 9. Plaintiff Daniel Lu is a bZx user who lost approximately
20 \$305,000 in the hack. He is a citizen of China.

21 10. Plaintiff Clément Ométak is a bZx user who lost
22 approximately \$92,000 in the hack. He is a citizen of France.

23
24
25 ¹ To prevent additional fraud and to minimize the risk of connecting individuals with specific
26 wallet addresses that may hold additional currencies, this Complaint will not reveal the precise loss
27 amount, cryptocurrency token type, and wallet address for each individual plaintiff. Those details are
28 unnecessary here, but they can be disclosed using sufficient safeguards at the appropriate time in this
litigation.

1 11. Plaintiff Edison Ho is a bZx user who lost approximately
2 \$25,000 in the hack. He is a citizen of the People's Republic of China and
3 resident in Hong Kong.

4 12. Plaintiff Kiro Aleksandrov is a bZx user who lost
5 approximately \$150,000 in the hack. He is a citizen of Bulgaria.

6 13. Plaintiff Jonas Wernecke is a bZx user who lost approximately
7 \$55,000 in the hack. He is a citizen of Germany.

8 14. Plaintiff Paolo Leite is a bZx user who lost approximately
9 \$14,000 in the hack. He is a citizen of Brazil.

10 15. Plaintiff Miras Issakhov is a bZx user who lost approximately
11 \$116,000 in the hack. He is a citizen of Kazakhstan.

12 16. Plaintiff Daniele Penna is a bZx user who lost approximately
13 \$180,000 in the hack. He is a citizen of Italy.

14 17. Defendant Kyle Kistner is an individual residing in or near
15 San Diego, California. He is the co-founder of the bZx protocol and a
16 member of the bZx DAO and general partnership.

17 18. Defendant Tom Bean is an individual residing in Alpharetta,
18 Georgia. He is the co-founder of the bZx protocol and a member of the bZx
19 DAO and general partnership.

20 19. Defendant Hashed International LLC is a Wyoming limited-
21 liability company with its principal place of business in San Francisco,
22 California. Hashed is an investor in the bZx protocol and a member of the
23 DAO and general partnership.

24 20. Defendant AGE Crypto GP, LLC is a Nevada limited-liability
25 company with its principal place of business in Los Angeles, California.
26 AGE Crypto is an investor in the bZx protocol and a member of the DAO
27 and general partnership.
28

1 21. Defendant bZx DAO is a purported Decentralized
2 Autonomous Organization that is a general partnership. The partnership
3 is headquartered in or near San Diego, California, where its co-founder
4 and primary decisionmaker lives and works. Alternatively, it is a

5 22. Defendant Ooki DAO is a purported Decentralized
6 Autonomous Organization that is a general partnership. The partnership
7 is headquartered in or near San Diego, California, where its co-founder
8 and primary decisionmaker lives and work.

9 23. Defendant Leveragebox LLC is a Delaware Limited Liability
10 Company that has a principal place of business in San Diego, California.
11 Leveragebox LLC operated the Fulcrum trading platform and may
12 continue to operate that platform.

13 24. Defendant bZeroX LLC is a Delaware Limited Liability
14 Company that has a principal place of business in San Diego, California.
15 bZeroX created the bZx protocol and, until August 2021, controlled the
16 protocol.

17 **Jurisdiction and Venue**

18 25. This Court has subject matter jurisdiction over this action
19 pursuant to 28 U.S.C. § 1332(a) because all Plaintiffs are foreign
20 domiciliaries and all Defendants are U.S. domiciliaries, and pursuant to
21 1332(d)(2)(A) because this is a class action in which the matter or
22 controversy exceeds the sum of \$5,000,000, exclusive of interest and
23 costs, and in which the minimal diversity requirements of that provision
24 have been met.

25 26. Venue is proper in this District under 28 U.S.C. § 1391(b)(2)
26 or (b)(3).

1 27. This Court has general jurisdiction over Defendants Kistner,
2 Hashed International LLC, AGE Crypto GP LLC, bZeroX LLC,
3 Leveragebox LLC, bZx DAO, and Ooki DAO.

4 28. This Court has specific personal jurisdiction over all
5 Defendants because they purposefully entered into a general partnership
6 controlled from California and because they are partners in a general
7 partnership with at least one member that has conducted partnership
8 business in California and they have directed at least some of their
9 partnership activities at California.

10 29. The Court also has personal jurisdiction over bZx DAO and
11 Ooki DAO because unincorporated entities take on the citizenship of
12 each of their members. *See Carden v. Arkoma Associates*, 494 U.S.
13 185 (1990). Because at least one member of each DAO is a citizen of
14 California, the DAOs are citizens of California and are subject to this
15 Court's personal jurisdiction

16 **Background on Cryptocurrency And The Products At Issue**

17 30. A cryptocurrency is a form of digital asset based on a network
18 that is distributed across a large number of computers. Cryptocurrencies,
19 at least right now, are not issued by central governments or authorities.
20 Bitcoin is the most well-known cryptocurrency, but there are thousands
21 of others. The value of some cryptocurrencies fluctuates with respect to
22 the U.S. Dollar and all other fiat currencies. Other cryptocurrencies, like
23 U.S. Dollar Coin, are so-called stablecoins because their value is pegged
24 to a fiat currency—for U.S. Dollar Coin, the U.S. Dollar.

25 31. Different cryptocurrencies are typically designated by three-
26 or four-letter symbols, like stock tickers. Bitcoin's is BTC. U.S. Dollar
27
28

1 Coin is USDC. Coins at issue in this case include ETH, BZRX, OOKI, and
2 several others.

3 32. The system by which a network of computers securely and
4 publicly records the transactions of a given cryptocurrency is called a
5 blockchain. There are several different blockchains that record
6 transactions of a variety of different cryptocurrencies. The blockchains at
7 issue in this case are called Ethereum, Polygon, and the Binance Smart
8 Chain. Each of these blockchains has a “native” cryptocurrency, in which
9 the computers operating the network are rewarded, and supports other
10 cryptocurrency transactions as well. Ethereum’s native cryptocurrency,
11 for example, is Ether (ticker: ETH).

12 33. A cryptocurrency token is a unit of a specific virtual currency.
13 These tokens are fungible and tradeable.

14 34. Cryptocurrency tokens are held via a virtual wallet. The
15 wallet is secured using cryptography and can typically be accessed only
16 with a lengthy passphrase, which is a form of strong password. The wallet
17 has an address—typically a seemingly random string of letters and
18 numbers—that can be published on the blockchain without revealing the
19 identity of the wallet-holder.

20 35. For cryptocurrency to reasonably function in a sophisticated
21 marketplace, users must transact between currencies, crypto- or
22 otherwise; must be able to lend and borrow; and must be able to earn
23 some rate of return on stored assets. Transactions like these are usually
24 executed in the traditional economy through third parties like banks. But
25 cryptocurrency transactions are increasingly conducted through “DeFi”
26 applications. DeFi stands for “Decentralized Finance” and uses emerging
27 technology to remove third-parties, like banking institutions, from
28

1 financial transactions. Thus, using DeFi protocols—such as bZx, at issue
2 here—users can engage in complicated transactions using
3 cryptocurrencies, like lending or borrowing, without interacting with
4 banks or other established, regulated intermediaries.

5 36. DeFi protocols are almost always governed as “Decentralized
6 Autonomous Organizations,” or “DAOs.” In a DAO, there is no formal
7 corporate structure, no explicit liability protection, and no distinction
8 between, say, managers and directors, or between general and limited
9 partners. Instead, holders of specific tokens—such as the BZRX token at
10 issue here—have governance rights that allow holders to suggest actions
11 that the associated DAO will take. Those suggestions are then voted on
12 and implemented if the required number of tokenholders support the
13 actions. Actions include many of those typically done by corporate
14 officers, boards, or employees, such as spending treasury funds to hire
15 people; changing organizational goals and policies; and even distributing
16 treasury assets to tokenholders, like how corporations can authorize
17 dividends. Holders of governance tokens thus may participate in the
18 governance of a protocol, they have a potential claim on its profits, and
19 they share responsibility for its liabilities.

20 **The bZx Protocol And Its Promises**

21 37. bZx is a DeFi platform describing itself as “a protocol for
22 tokenized margin trading and lending.” According to its website, “[i]t is a
23 financial primitive for shorting, leverage, borrowing, and lending that
24 empowers decentralized, efficient, and rent-free” transactions on the
25 blockchain.

26 38. There are two “products” built on the bZx protocol. The one
27 primarily used in this case is called Fulcrum, which the protocol’s website
28

1 says is a “DeFi Margin Lending and Trading Platform.” Fulcrum permits
2 users to lend tokens and earn interest on those tokens when other people
3 borrow them, like how a U.S. bank or savings-and-loan association takes
4 deposits, lends them out, and pays back depositors with interest.

5 39. The other product built on the bZx protocol is Torque, which
6 provides for “Indefinite-term Loans with Fixed Interest Rates.”

7 40. The simplest way to use these products is to navigate to the
8 website bZx.network and then select the desired product, either Fulcrum
9 or Torque. Assuming a user selects Fulcrum, the user then must choose
10 which blockchain to use to record and execute transactions. (As
11 mentioned above, bZx products work on three blockchains: Ethereum,
12 Polygon, and Binance Smart Chain.) After selecting a blockchain
13 network, a user can connect a wallet and deposit cryptocurrency or
14 otherwise interact with the protocol. On Fulcrum, users can deposit and
15 earn interest on a variety of different types of cryptocurrencies.

16 41. bZx repeatedly and prominently touts its security features.
17 bZx claims that Fulcrum is “non-custodial,” which means that “whether
18 lending or trading, [users] maintain control of [their] own keys and
19 assets.” This, supposedly, makes the platform especially secure.

20 42. In reality, a single password was sufficient to access *all* of the
21 client funds on two of the three blockchains on which Fulcrum operated.
22 The holder of that password, therefore, had custody of the client funds
23 and had a legal duty as custodian to exercise reasonable care to protect
24 the funds.

25 43. Additional promises of safety abound. A website section called
26 “how safe is it?” lists four reasons to think the protocol is quite safe,
27 including “Audited Smart Contracts” and an “Insurance fund.” An entire
28

1 tab called “security” is linked at the very top of the Fulcrum platform,
2 and the headline that appears on that linked page is “Security Is Our
3 Priority.” That page says that “bZx is committed to ensuring the security
4 of user funds.” It lists several steps the protocol has taken to supposedly
5 ensure the security of deposited cryptocurrency tokens.

6 44. That page, in turn, links to another page explaining bZx’s
7 “World Class Security.” That page claims that, as of September 2020, “all
8 issues found ha[d] been confirmed or fixed.”

9 45. Perhaps the most succinct summary of bZx’s security
10 promises can be found directly on bZx’s homepage. Under the graphic
11 “Minimized Risk,” bZx claims, “Whether you’re a lender or borrower, you
12 stay in control of your keys. Never worry about opaque centralized
13 exchanges getting hacked or stealing your funds.”

14 **The November 5, 2021 Hack And Theft**

15 46. What bZx claimed users need not worry about happened on
16 November 5, 2021. That day, the protocol was hacked and funds were
17 stolen from named Plaintiffs and the class members. The following facts
18 about the hack are taken primarily from bZx’s own statements.

19 47. On November 5, 2021, according to the anonymous bZx DAO
20 member, “[a] bZx developer was sent a phishing email to his personal
21 computer with a malicious macro in a Word document that was disguised
22 as a legitimate email attachment, which then ran a script on his Personal
23 Computer. This led to his personal mnemonic wallet phrase being
24 compromised.”

25 48. A “phishing attack” occurs when a malicious actor,
26 masquerading as a trusted entity, dupes a victim into opening an email,
27 instant message, or text message with dangerous contents. The recipient
28

1 is then tricked into clicking a malicious link or opening a malicious
2 attachment, which can lead to the installation of a virus, the freezing of
3 the system, or, as here, the revealing of sensitive information like
4 passwords.

5 49. According to the blog post from an anonymous DAO member,
6 the November 5 “phishing attack was similar to one that affected another
7 user recently named ‘mgnr.io’ This attack granted the hacker access
8 to the content of the bZx Developer[']s wallet, and also the private keys
9 to the BSC and Polygon deployment of bZx Protocol. After gaining control
10 of BSC and Polygon the hacker drained the BSC and Polygon protocol,
11 then upgraded the contract to allow draining of all tokens that the
12 contracts had given unlimited approval.”

13 50. Or, put more simply (according to a news report), “A hacker
14 stole millions after a developer at bZx, a crypto company, fell for a
15 phishing attack.” The estimated theft was \$55 million in U.S. Dollar
16 value.

17 51. The developer was working for the bZx DAO at the time of the
18 hack. His possession of the private keys (or passcodes or passphrases)
19 that enabled possession of users’ funds and that were stolen by the
20 hackers was within the scope of his employment because those keys were
21 his only means of accessing the protocol and making necessary changes
22 to it.

23 52. The problem, as the company reported it, was that—despite
24 the protocol’s promises to the contrary—the protocol’s implementation on
25 two of the three blockchains on which it operated was insecure. That is,
26 the protocol was designed to work on the Ethereum blockchain, the
27
28

1 Polygon blockchain, and the Binance Smart Chain blockchain, but only
2 its operations on the Ethereum blockchain were secure.

3 53. Here is how bZx itself put it shortly after the theft, with
4 Plaintiffs' explanatory comments in brackets. (Punctuation has been
5 slightly cleaned up.)

6 The BSC and Polygon implementation
7 administrative private keys have not yet been
8 transferred to the DAO yet. [As of the date of the
9 hack, an important measure for securing secret
10 information had not yet been taken with respect to
11 the Binance Smart Chain and Polygon
12 blockchains.]

13 Therefore the BSC and Polygon Deployment did
14 not have the protection of the DAO. [The Binance
15 and Polygon blockchains were less secure than the
16 Ethereum blockchain.]

17 When the developer's private keys were
18 compromised in a phishing attack, the hacker
19 gained access to not only the individual developer's
20 personal funds, but also gained access to the bZx
21 deployment on BSC and Polygon. [When the bZx
22 developer's password was hacked, the hacker was
23 able to steal individual funds from that developer
24 and also steal funds of others that used the
25 Binance and Polygon blockchains because the
26 important security step to secure those
27 blockchains had not yet been taken.]

28 From there, the hacker was able to upgrade the
contract and perform an attack on users of the
protocol and funds held within the protocol. [Once
the hackers had the password, they could use it to
drain funds from bZx users on the Binance and
Polygon blockchains.]

1 54. The report also stated that some things “went right.” In
2 particular, the “bZx treasury on Ethereum DAO is safe on the Ethereum
3 deployment because [bZx] had already fully decentralized there.” In other
4 words, funds held on the Ethereum blockchain were not impacted
5 because the protocol’s operations on that blockchain were more secure
6 than the Polygon and Binance blockchains. That is cold comfort to these
7 Plaintiffs, but it means that all funds that had used the protocol were not
8 entirely wiped out, and it shows conclusively that bZx failed to meet its
9 *own* standards for safety, let alone reasonable industry standards.

10 55. The stolen tokens appear at this point to be unrecoverable.

11 56. This was not the first hack of this protocol. In 2020, bZx
12 suffered three hacks with total losses of approximately \$9 million,
13 although \$8 million was apparently recovered eventually. And, as bZx
14 itself mentioned, the phishing attack that one of the developers fell for
15 was similar to another one that the protocol had already received.
16 Despite these incidents, bZx, Fulcrum, and their partners and members
17 did not alter their promises of security or invulnerability from hacks.
18 Rather, they failed to take reasonable steps to secure the platform and
19 prevent the theft that actually occurred.

20 **The Inadequate Compensation Plan And Move To Ooki**

21 57. The bZx DAO has recognized its responsibility to compensate
22 the victims of the theft. Soon after the hack, a user named BadriNat
23 sketched out a first proposal on bZx’s community forum for bZx to
24 compensate victims of the attack. BadriNat appears to be a person named
25 Badri Natarajan, an attorney specializing in blockchain legal and
26 regulatory risk management. In the post, BadriNat stated that he was
27 not a member of the bZx development team and was not being paid by
28

1 the DAO. It is unclear if BadriNat had spoken to, been in contact with,
2 or been compensated by any of the named defendants here or other key
3 members of the bZx DAO and general partnership described below.

4 58. After some discussion, a proposal was put to a vote for
5 members of the DAO. BZRX tokenholders were eligible to vote. On
6 November 21, 2021, a compensation plan was adopted without any “no”
7 votes.

8 59. The compensation plan was divided into two parts. In the first
9 part, the DAO determined that all who lost the BZRX token would be
10 compensated in full directly from the bZx DAO by either replacing that
11 token on a 1-to-1 ratio with what had been lost or, for some users,
12 replacing the lost tokens with a version of BZRX token that would fully
13 vest over time. Full compensation was made possible in part because the
14 BZRX token is issued by the bZx DAO itself, and there were some
15 unassigned BZRX tokens in the DAO’s “treasury,” which is the
16 equivalent of a general partnership’s shared bank account. None of the
17 Plaintiffs or proposed class held meaningful stakes of BZRX token and so
18 did not benefit from this plan.

19 60. In the second part of the plan, the bZx DAO issued new “debt
20 tokens”—essentially, IOUs—that the DAO promised would be bought
21 back using 30% of the future revenue that comes into the DAO, which, as
22 a practical matter, means 30% of the revenue generated through certain
23 transaction fees that the protocol charges users. Although bZx promised
24 that “in this way, [the DAO] will eventually reimburse all losses suffered
25 as a result of the incident,” the word “eventually” must be given a very
26 generous reading: at the current buyback rate, full repayment will take
27 thousands of years.
28

61. In December 2021, several weeks after the hack, the bZx protocol encouraged users to transfer to a successor platform called Ooki. Many BZRX tokens were transformed into OOKI tokens; an Ooki DAO was created, with control rights given to those OOKI tokenholders (many of whom received OOKI tokens as a direct result of the conversion from BZRX); and the Ooki platform was launched with much of the same functionality as Fulcrum and Torque. Thus, while Fulcrum, Torque, and bZx still exist, Ooki is a direct successor to that network and platform.

The bZx DAO And Successor Ooki DAO Are General Partnerships

62. The bZx Protocol and the platforms built on top of it, including Fulcrum, were originally controlled at least in part by two LLCs: bZeroX LLC and Leveragebox LLC. These LLCs appear to have been largely controlled by co-founders Tom Bean and Kyle Kistner.

63. In August 2021, several months before the hack, bZx outlined plans to transition both revenue from the protocol and control of aspects of the protocol to the bZx DAO. That is, “armed with tens of millions of dollars, [the DAO] will take up the task of maintaining the protocol, building new products, marketing the brand, and managing the community.” At that time, the bZx treasury held approximately \$80 million worth of assets. When the transition was completed “the legal entity bZeroX LLC [ceased] to exist, and in its place the DAO . . . remain[ed].” Still, despite the change, “[t]he core team [maintained] a strong desire to continue working on the project and welcomes this new chapter as the start of something even greater than what came before.”

64. The bZx DAO is controlled by those who hold the BZRX token. That is, “the keys to the bZx treasury, [were] turned over to the DAO,

1 and bZx tokenholders [became] the main drivers of governance and
 2 decision making of the bZx platform going forward.” The way this works
 3 is that bZx tokenholders—that is, those who own the BZRX token—can
 4 both suggest and vote on governance proposals. If the proposals pass, the
 5 DAO takes the action. In that way, the tokenholders could, for instance,
 6 implement the compensation plan whereby BZRX tokenholders were
 7 fully compensated from the DAO treasury for the hack but Plaintiffs and
 8 others who used different tokens on the protocol were given IOUs but
 9 little chance of repayment.

10 65. The Ooki DAO is a direct successor DAO to bZx because many
 11 BZRX tokens were directly converted to OOKI tokens in December 2021.

12 66. Given their structures and the way they operate, the bZx and
 13 Ooki DAOs are general partnerships among tokenholders. That is, they
 14 are associations of two or more persons (the tokenholders and investors),
 15 to carry on as co-owners (of the bZx and Ooki DAOs, with shared control
 16 of the bZx and Ooki treasury funds, among other assets), of a business
 17 for profit (the bZx and Ooki protocols and related products built on them,
 18 with the profits being the right to funds held in the respective treasuries).
 19 Although DAOs seem novel, many legal observers who have analyzed
 20 them have reached the same conclusion.²

21
 22 ² For example:

- 23 • “[T]he U.S. legal system must clarify the legal status of these organizations and as such
 24 should classify the DAO as a general partnership.” Laila Metjahic, *Deconstructing the*
 25 *DAO...*, 39 Cardozo L. Rev. 1533, 1536 (2018).
- 26 • “[A] DAO’s decision to not create a legal entity does not offer protection from responsibilities
 27 that may arise in the operation of a DAO. From a legal perspective, when two or more
 28 individuals are engaged in even a tenuous business relationship, the imputed structure is
 that of a general partnership.” David Kerr & Miles Jennings, *A Legal Framework for*
Decentralized Autonomous Organizations v2, A16Z White Paper, <https://bit.ly/3jYfILt>.
- “[E]xisting corporate law dictates that what the members of [a] DAO have formed is a
 general partnership.” Dave Rodman, *DAOs: A Legal Analysis*, JD Supra (Apr. 1, 2021)
<https://bit.ly/3jYjnZI>.

Each Defendant's Partnership Activities

67. Defendant Kyle Kistner is a self-professed co-founder of the bZx protocol and is still listed as being employed at bZx. During the relevant time, he participated in decisionmaking of the bZx protocol and its successor the Ooki protocol. Kistner made many of the decisions from in or around San Diego, California, where he lives.

68. Defendant Tom Bean is a self-professed co-founder of the bZx protocol. During the relevant time, he participated in the decisionmaking of the bZx protocol and its successor the Ooki protocol. He was aware that Kistner moved to California and intentionally communicated with Kistner in California about partnership business.

69. Defendant Hashed International LLC is a stated investor in the bZx protocol. During the relevant time, it and its members or principals participated in the decisionmaking of the bZx protocol and its successor the Ooki protocol. It has publicly disclosed that it “supported the [bZx] team,” “actually witness[ed] how this team solved” a security issue, and invested in the protocol and the BZRX token.

70. Defendant AGE Crypto GP, LLC is a stated investor in the bZx protocol. During the relevant period, it and its members or principals participated in the decisionmaking of the bZx protocol and its successor the Ooki protocol. It has stated offices in Reno, Nevada, but it is likely controlled by its founder from in or around Los Angeles, California.

71. Defendant bZx DAO is a purported Decentralized Autonomous Organization that is a general partnership. Its members determine the governance of the bZx protocol, supervise those responsible for securing the protocol, and making distributions from the treasury, among other tasks.

1 72. Defendant Ooki DAO is a purported Decentralized
2 Autonomous Organization that is a general partnership. Its members
3 determine the governance of the Ooki protocol, supervise those
4 responsible for securing the protocol, and making distributions from the
5 treasury, among other tasks. The Ooki protocol is a direct successor to
6 the bZx protocol.

7 73. Defendant Leveragebox LLC operated the Fulcrum trading
8 platform during the relevant time and may continue to operate that
9 platform.

10 74. Defendant bZeroX LLC created the bZx protocol and, until
11 August 2021, controlled the protocol. At that time, it purportedly
12 transferred its assets to the bZx DAO.

13 **Class Action Allegations**

14 75. Plaintiff proposes to move to certify the following class: All
15 people who delivered cryptocurrency tokens to the bZx protocol and had
16 any amount of funds stolen in the theft reported on November 5, 2021,
17 except for people whose only cryptocurrency stolen was the BZRX token.

18 76. The proposed class meets Federal Rule of Civil Procedure 23's
19 requirements, called respectively numerosity, commonality, typicality,
20 adequacy, predominance, and superiority.

21 ***Numerosity***

22 77. The class is so large that joinder of all parties would be
23 impracticable. The total loss amount was approximately \$40 million, and
24 it is estimated to have been held by thousands of different people.

25 ***Commonality***

26 78. There are questions of law and fact common to members of
27 the class.
28

1 85. Both founding partners of Gerstein Harrow have significant
2 experience litigating complex cases, including major class actions, and
3 cases involving cryptocurrency.

4 86. Charles Gerstein has, among other things, served as lead
5 counsel in a class action case against the City of Houston that recently
6 settled for \$1.175 million, and has served as counsel or lead counsel in
7 several complex class actions seeking prospective relief against public
8 entities and officers throughout the country. As a law clerk for the U.S.
9 District Court of the Southern District of New York and the U.S. Court
10 of Appeals for the Second Circuit, Gerstein advised the courts on several
11 complex class-action cases.

12 87. Jason Harrow has litigated complex cases on behalf of New
13 York State and its agencies as an Assistant Solicitor General, as an
14 associate at the national law firm Davis Wright Tremaine, LLP, and as
15 lead counsel in the U.S. Supreme Court in *Colorado Dep't of State v. Baca*,
16 No. 19-518 (argued May 13, 2020; decided July 6, 2020). As a law clerk
17 for the U.S. District Court for the Southern District of New York and the
18 U.S. Court of Appeals for the Ninth Circuit, Harrow advised the courts
19 on several complex class-action cases.

20 88. In addition, Gerstein and Harrow are lead counsel in a
21 different major case regarding cryptocurrency, *Kent v. PoolTogether Inc.*,
22 docketed as 21-cv-6025 in the U.S. District Court for the Eastern District
23 of New York. That case presents some overlapping issues with this one,
24 including regarding the liability of DAOs and their general partners.
25 Their experience there can thus inform their experience in this matter.

26 89. Class counsel will fairly and adequately represent the
27 interests of the class.
28

1 ***Predominance and Superiority***

2 90. The questions of fact and law common to the class
3 predominate in this Action over any questions affecting only individual
4 members of the class.

5 91. In fact, there will be no individual questions of law or fact for
6 any of the members of the class and damages will be trivially easy to
7 assess: Each class member delivered money to bZx and then lost it in the
8 November 5, 2021, theft. Those are the only requirements necessary to
9 succeed on these claims.

10 92. The classes in this case will be easily managed and
11 ascertained. The bZx protocol and the blockchains used keep a publicly
12 accessible record of every transaction any user has ever executed, and
13 each account is assigned a unique identification code. Thus, although the
14 Defendants may not know the legal identities of most of their users, they
15 can communicate with (and therefore ensure the provision of notice to)
16 all their users; they can (and indeed have) determined the amount each
17 is owed; and they can pay the money it owed them easily by crediting the
18 accounts associated with each identification number.

19 **Claims for Relief**

20 ***Count One: Negligence***

21 93. Plaintiffs incorporate all prior paragraphs by reference.

22 94. The bZx protocol and its partners owed Plaintiffs a duty to
23 maintain the security of the funds deposited using the bZx protocol,
24 including but not limited to putting in place procedures such that a
25 phishing attack on a single developer would not result in a multi-million
26 dollar theft; it breached that duty; and Defendants' actions in breaching
27
28

1 their duty were the proximate and but-for cause of an injury—namely,
2 the loss of funds deposited with the bZx protocol.

3 95. The bZx protocol and its partners also owed Plaintiffs a duty
4 to supervise developers and those working on the protocol such that
5 important passwords or security details could not be revealed through
6 the actions of a single developer; it breached that duty; and Defendants’
7 actions in breaching their duty were the proximate and but-for cause of
8 an injury—namely, the loss of funds deposited with the bZx protocol.

9 96. The unnamed developer working on behalf of bZx owed
10 Plaintiffs a duty to secure against malicious attacks passwords that could
11 result in theft of millions of dollars of assets; the developer breached that
12 duty; and the developer’s actions in breaching that duty were the
13 proximate and but-for cause of an injury—namely, the loss of funds
14 deposited with the bZx protocol. The Defendants answer as *respondeat*
15 *superior* to the negligence of the developer they employed or contracted
16 with.

17 97. Defendants are therefore jointly and severally liable for
18 Plaintiffs’ injuries.

19 **Prayer for Relief**

20 Plaintiffs respectfully request:

- 21 • An order certifying an appropriate class;
- 22 • An award of compensatory damages to Plaintiffs and the
- 23 proposed class in an amount that fully compensates Plaintiffs
- 24 and the proposed class for all lost funds;
- 25 • Punitive damages as appropriate;
- 26
- 27
- 28

- Allowable costs and attorney's fees pursuant to Federal Rule of Civil Procedure 54, or any other applicable provision or principle of law; and
- Any other relief deemed just and proper.

Respectfully submitted,

/s/ Jason Harrow

Jason Harrow

(Cal. Bar No. 308560)

Charles Gerstein

(pro hac vice application forthcoming)

GERSTEIN HARROW LLP

3243B S. La Cienega Blvd.

Los Angeles, CA 90016

jason@gerstein-harrow.com

(323) 744-5293

Attorneys for Plaintiffs