

ARKHAM

REPORT ON THE INTERNET COMPUTER TOKEN

28 JUNE, 2021

As of this writing, the Internet Computer token (ICP) has lost 95% of its value from its launch event in May, dropping from $730 to $30, and wiping out over $300 billion dollars of value based on ICP's total supply.[1] These are astounding numbers in the crypto world and financial world overall, even with the current market's volatile prices and soaring valuations. At its peak, ICP was the third most valuable crypto-asset, behind Bitcoin and Ethereum, and was worth as much by market cap as Mastercard, Bank of America, and PayPal. In its first month ICP's price decreased more than any other top 100 token by a good margin. Altogether retail investors who bought ICP on Coinbase or other major crypto exchanges have lost millions if not billions of dollars.

Investors deserve an explanation, which this report aims to provide by illuminating some activity surrounding ICP and the organization behind it, Dfinity. Our analysis has led us to believe that possible insiders connected to Dfinity have been dumping billions of dollars of ICP on exchanges at the expense of small early supporters and retail investors.

Summary of findings

- Addresses we suspect belong to the Dfinity treasury and project insiders have deposited 18.9 million ICP, worth ~$3.6 billion at time of deposit, to exchanges.[2]
    - The Treasury has directly deposited 8.3 million ICP, worth ~$2 billion at time of deposit, 94% of which was on two days: listing day of May 10th (3.1mm) and June 15 (4.7mm).
    - The Treasury sent 34.1 million ICP to 34 suspected insider addresses. These addresses have deposited 10.7 million ICP, also worth ~$1.6 billion at time of deposit, intermittently over the weeks since listing.
    - Deposits from the Treasury plus suspected insiders account for approximately 75% of total ICP deposits to exchanges.
- Based on a review of their public materials, Dfinity has not followed industry practices meant to demonstrate good faith and assure investors that project insiders won't trigger a price collapse through massive selling.
    - Dfinity has not been transparent about token allocation and unlocking, unlike other major projects.
    - It has nonetheless come out that Dfinity imposed 4-year vesting on small seed supporters, who collectively own about 25% of the ICP supply, while having no vesting for the Dfinity foundation, which also reportedly owns about 25% of the ICP supply.
    - Many of these small seed supporters say they have found it extremely difficult, if not effectively impossible, to access their tokens.

[1] CoinMarketCap, Internet Computer
[2] All numbers in this report are based on analysis of the ICP blockchain as of 26 June. The numbers in our video differ because they are as of 17 June.



On-Chain Analysis

Address Identification

Our analysis identified addresses likely belonging to the following entities:

- Dfinity
- Exchanges, namely Coinbase, Binance, Huobi, and OKEx
- Suspected insiders coordinated with Dfinity

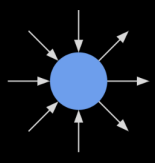
What we will call the Treasury is the key address we believe belongs to Dfinity. The Treasury received about 107 million ICP from the mint at genesis, almost a quarter of the total ICP supply of about 470 million. This made it by far the largest holder of ICP on the blockchain. Dfinity should be the largest single holder of ICP at genesis because they were entitled to all tokens not allocated to the multitude of financial backers, team members, and small airdrop recipients.

There are two types of exchange addresses that are important for this analysis: central addresses and deposit addresses. Central addresses are the locus of exchange activity. They are the central pot of ICP for the exchange. They send out tokens withdrawn from the exchange, and receive tokens deposited to it. However, before deposited tokens reach the central address, they first go to deposit addresses.

Deposit addresses are unique to particular exchange accounts belonging to external people or organizations who use the exchange. In this sense they're similar to bank accounts. When someone wants to deposit their ICP to an exchange, they send it to their unique deposit address. Once the ICP hits the deposit address, the exchange generally transfers it from the deposit address to a central address within 30 minutes, sort of like the bank taking a depositor's cash and putting it in their ATM.

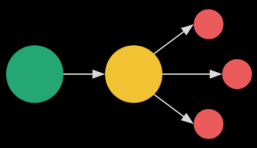
Suspected insiders are addresses that have been linked to the Treasury in one of two ways: they received ICP from the Treasury, or they deposited ICP to an exchange deposit address also used by the Treasury.

Exchange Central Addresses



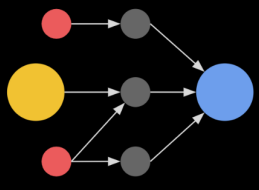
Receive exchange deposits and send withdrawals

Treasury & Insiders



Treasury received enormous transfer from mint and distributed tokens to insiders

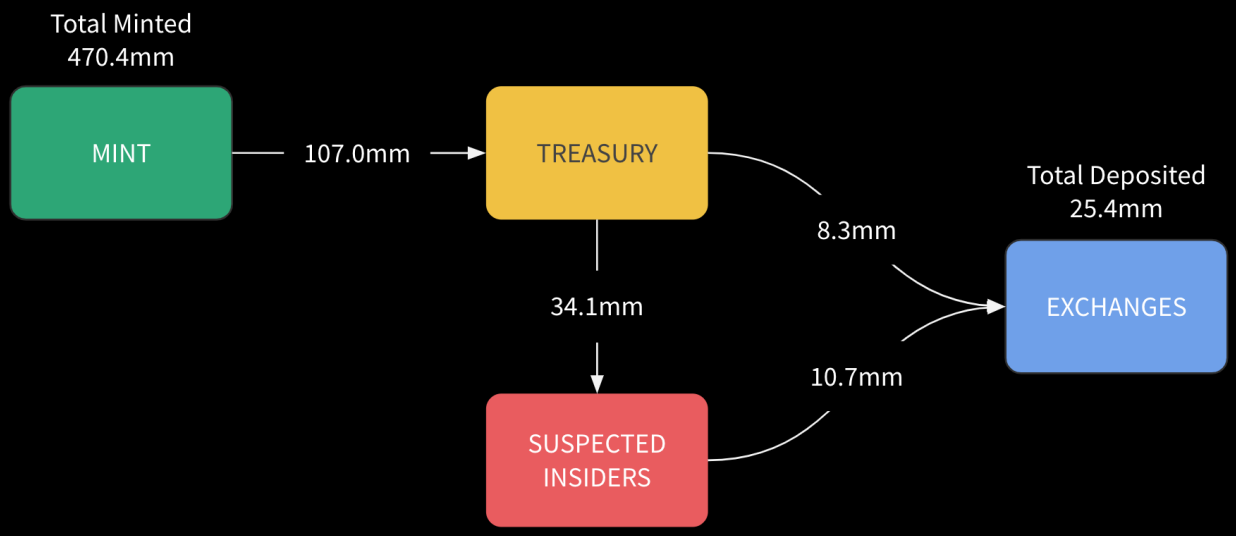
Exchange Deposit Addresses



Receive deposits and send to exchange central wallet

Token flows

Having identified addresses likely belonging to these key entities, we then tracked token flows between them:



Treasury to Exchanges: 8.3mm ICP worth ~$2B at time of deposit

94% of the 8.3 million in ICP deposits from the Treasury to exchanges occurred on two days: 3.1 million on May 10th (listing day) and 4.7 million on June 15th.

Deposits on listing day were spread over the course of the day, with 60% occurring before trading opened on Coinbase and 40% after. Deposits were made to all four exchanges, though heavily concentrated on Coinbase:

- 2mm ICP to 7 Coinbase deposit addresses
- 550k to 3 Huobi deposit addresses
- 350k to 3 Binance deposit addresses
- 250k to 3 OKEx deposit addresses

Listing day Treasury deposits to Coinbase:

- 25k at 1202 UTC 10 May to address 1
- 25k at 1202 to address 2
- 120k at 1205 to address 3
- 750k at 1306 to address 4
- 200k at 1308 to address 5
- 80k at 1311 to address 3
- 40k at 1312 to address 6
- Trading begins at 1600 UTC on 10 May
- 75k at 1607 to address 2
- 627k at 1610 to address 7

This overall pattern for listing day deposits suggests that they were for the purpose of providing initial liquidity on exchanges. The same cannot be said of the deposit of 4.7 million ICP on 15 June, at the time over $250 million, which was made in two installments to the same Coinbase deposit address. These are the Treasury's most recent transactions.

Treasury to Suspected Insiders: 34.1mm ICP

We have identified 34 addresses linked to the Treasury that have also deposited large amounts of ICP to exchanges, either directly or through intermediaries. We suspect that these addresses belong either to Dfinity itself or to insiders coordinated with Dfinity. They are linked to the Treasury in that they have either received tokens directly from the Treasury, or sent tokens to deposit addresses also used by the Treasury.

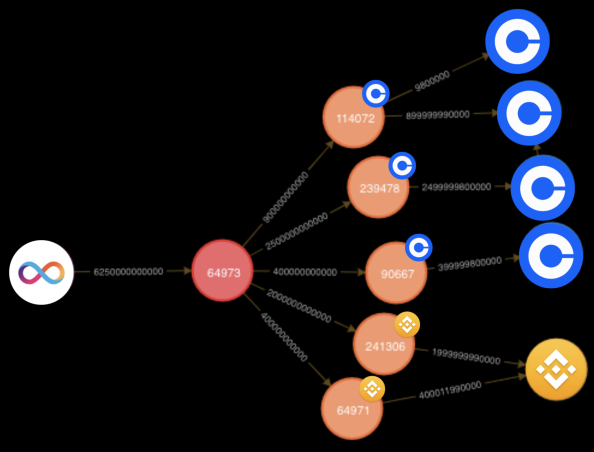
The Treasury has sent 34.1 million ICP in total to these suspected insiders. About 75% of these transfers occurred within three hours of Coinbase trading open.

Suspected Insiders to Exchanges: 10.7mm ICP worth ~$1.6B at time of deposit

In contrast to the Treasury, suspected insiders have deposited tokens continually in the weeks since listing, with no extreme concentration on any particular day. Addresses vary in their pattern of deposit, suggesting that they belong to separate entities. Some deposit all of their tokens at once, others incrementally. Some incremental depositors always use the same size increment, others use various sizes. Some use test transactions, others do not. Some deposit only to Coinbase, others only to Binance, and others to multiple exchanges. Some don't deposit directly to exchanges, but send tokens to intermediary addresses which then deposit directly. There is no unifying system, leading us to believe that there is no single underlying entity. There may however be fewer than 34 underlying entities, which we suspect given that they sometimes share deposit addresses, even with the Treasury as noted above.

Despite this variance, there is a simple fundamental pattern of activity shared by many suspected insiders: a large transfer from the Treasury on listing day, followed by intermittent exchange deposits post-listing. Suspected Insider 23 fits this basic pattern:

1. Treasury sends 62.5k ICP to Suspected Insider 23 two hours prior to trading open.
2. Suspected Insider 23 sends 62k ICP to deposit addresses on Coinbase and Binance over 5 days after trading open in increments of 4-25k.
3. Exchanges move ICP from those deposit addresses to exchange central addresses within 20 min of deposit.



Implications

The Treasury and suspected insiders have continually sent millions of ICP worth billions of dollars to exchanges, totaling 75% of the total deposited, possibly driving ICP's price collapse. We do not have clear and direct evidence that these deposited tokens were sold. But deposits to exchanges and trading platforms are generally for the purpose of selling. After all, facilitating selling is what exchanges are for.

One could argue that an ICP holder might want to use an exchange, especially Coinbase, for secure token custody, but this is unlikely in this case for a few reasons. For one, surely Dfinity itself has the funding and technical capabilities to securely store its own tokens, and the general view in crypto is that self-storage is preferable to third-party storage given the proper precautions are taken—"not your keys, not your coins"—making exchange custody unlikely at least in the case of treasury deposits.

Secondly, if a holder wanted to custody their tokens with Coinbase, they would presumably send all of their tokens there in one or a small number of transfers, but this is generally not what we see. Instead, most of the addresses in question deposit only a portion of their total ICP holdings incrementally over the course of days or weeks, often across multiple exchanges

The Internet Computer protocol also distributes ICP rewards to holders who lock their tokens in the network.[3] So if you do not intend to sell your tokens, it is in your financial interest to keep them locked up earning rewards rather than on exchanges.

Finally, the exceptional decrease in the price of ICP since listing is indicative of massive selling, which would likely be coming from these deposits, seeing as, based on our analysis, they are the source of the vast majority of the ICP deposited to exchanges.

If all or most of the ICP deposited by these addresses was in fact sold, this would exert massive downward pressure on the price of ICP, and would go a long way towards explaining its exceptional decrease since listing.

[3] Dfinity on Medium, "Earn Substantial Voting Rewards by Staking in the Network Nervous System"



Off-Chain Analysis

Apparent Lack of Transparency on Token Allocation and Unlocking

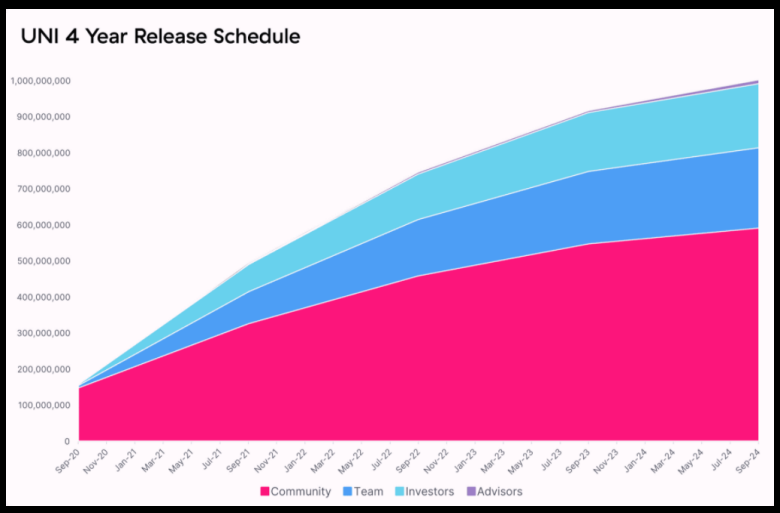
After seeing this activity by the Treasury and insiders connected to it, it is natural to wonder what was said publicly about how many tokens Dfinity and project insiders were entitled to and what their unlocking schedules were. But based on our review of Dfinity's public materials, there was no widely distributed public statement with this information. It appears Dfinity was not transparent about how tokens were distributed and when they would be unlocked, contrary to industry best practices.

Uniswap is a good example of crypto best practices on communicating about tokenomics. When the UNI token launched in 2020, Uniswap published an article on their website clearly describing token allocation and unlocking. Below are some excerpts from the post.

After a short introduction, there is a straightforward breakdown of percentage allocation by category of holders, along with unlocking schedules for each category:

> **UNI Allocation**
>
> 1 billion UNI have been minted at genesis and will become accessible over the course of 4 years. The initial four year allocation is as follows:
>
> - 60.00% to Uniswap community members `600,000,000 UNI`
> - 21.266% to team members and future employees with 4-year vesting `212,660,000 UNI`
> - 18.044% to investors with 4-year vesting `180,440,000 UNI`
> - 0.69% to advisors with 4-year vesting `6,900,000 UNI`

Later there is a graph illustrating unlocking schedules for the different categories over time:



Next there is a breakdown of unlocking for the treasury:

UNI will vest to the governance treasury on a continuous basis according to the following schedule. Governance will have access to vested UNI starting October 18 2020 12:00am UTC.

Year	Community Treasury	Distribution %
Year 1	172,000,000 UNI	40%
Year 2	129,000,000 UNI	30%
Year 3	86,000,000 UNI	20%
Year 4	43,000,000 UNI	10%

Team, investor, and advisor UNI allocations will have tokens locked up on an identical schedule.

And at the end are posted links to the token contracts on etherscan, including one to the treasury address:

Contracts

UNI Token:

https://etherscan.io/token/0x1f9840a85d5af5bf1d1762f925bdaddc4201f984

Liquidity mining:

Tether Liquidity Mining Pool

USDC Mining Pool

DAI Mining Pool

WBTC Mining Pool

Governance:

https://etherscan.io/address/0x5e4be8Bc9637f0EAA1A755019e06A68ce081D58F

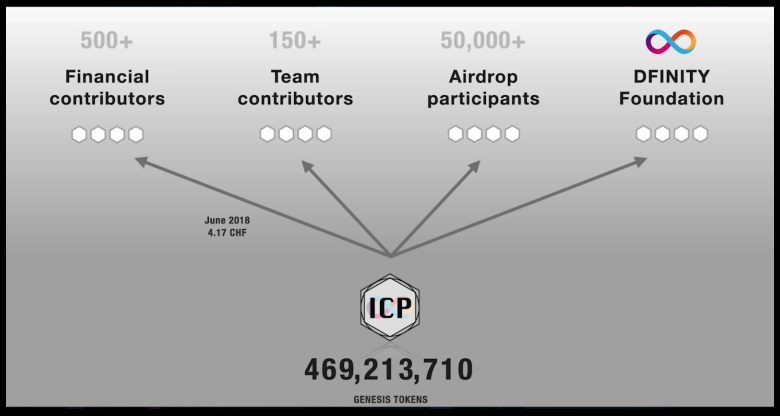
Timelock:

https://etherscan.io/address/0x1a9c8182c09f50c8318d769245bea52c32be35bc

Uniswap is not unique in this practice. At Reserve, a project co-founded by Miguel Morel, the CEO of Arkham, token allocation and unlocking for the project's RSR token were also clearly described in a short post on the Reserve website. Reserve took the extra step of locking all insider tokens until a major project milestone was hit, and they're still locked today, 2 years later. Reserve was also clear about the locking and locking of Treasury tokens at launch, and required any unlocking to be announced in advance with a written explanation from the team.



There wasn't any similar breakdown from Dfinity in any of the public materials we reviewed. What we did find was the following graphic from a tokenomics video posted to Dfinity's YouTube channel seven months before launch:



There is no clear and detailed breakdown of token allocation and unlocking, only the total supply of tokens and the names of different categories of holders. Later in the video, there is some discussion of 24 month "dissolve delays" in relation to claiming tokens from the ICP system, but how unlocking will actually play out for each category of holders is not put forth in simple terms like it was for UNI and RSR.

Dfinity's founder, Dominic Williams, did provide some further clarity a few weeks after launch in response to a request on Twitter for exactly the kind of tokenomics breakdown we've been discussing:



Unfortunately he did not provide the summary requested, but he did reveal that the Dfinity foundation (i.e. the treasury) tokens had no vesting.

These practices are not up to the standard set by the most respected and legitimate projects in crypto. Such standards exist in order to demonstrate good faith on the part of the project and assure community members and retail investors that project insiders will not risk collapsing the token's price by selling large amounts of tokens—what's known in crypto as a "rug pull", "team dump" or "VC dump". These

insider-driven price collapses happen sometimes, and getting caught in one is the biggest fear of many retail investors, leading legitimate projects like Uniswap and Reserve to do everything they can to demonstrate that there is no dump coming.

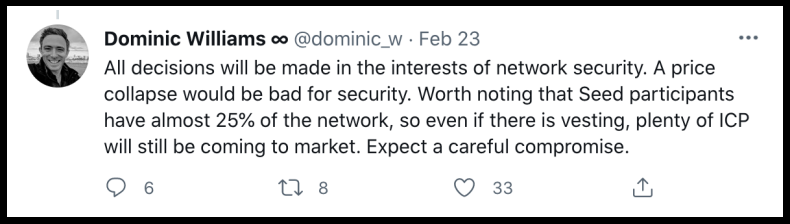
Seed Supporters' Struggles

In early 2017, Dfinity conducted a seed crowdraise, where normal supporters could "donate" a small amount in exchange for the promise of ICP when the token eventually launched. These early backers paid just a few cents per ICP.

By launch time, these seed supporters were collectively entitled to about a quarter of the ICP supply. If you were a project insider intending to make millions by selling your ICP post-listing, you might not want these supporters to be able to access their tokens, because if they could, their selling could make the price of ICP drop, which would devalue your own holdings if you were not able to sell before them, resulting in you making less money. And because these investors had such a low cost basis on their ICP, you would expect many of them to sell a large portion of their tokens to lock in those massive gains.

In response to a community member's tweet a few months before launch, which noted that no vesting schedule had been announced for seed tokens, Dominic Williams himself implied that seed token liquidity could risk a "price collapse" and that there may be vesting.



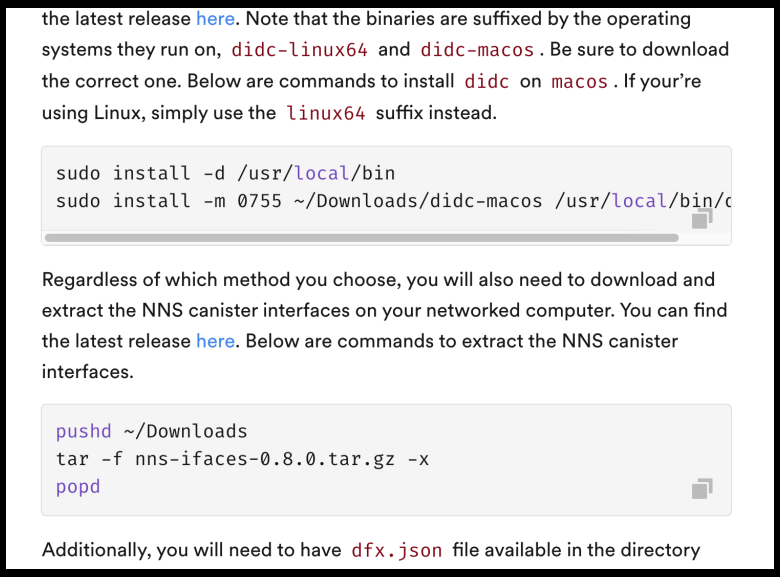


Seed supporters seem to have remained in the dark about token unlocking and access until the day of listing, when Dfinity published an article on Medium on accessing seed tokens. The article says in rather unclear fashion that seed investors will be effectively subject to a 4-year unlocking schedule. Compare the paragraph on seed unlocking below with the clear descriptions and illustrations from the Uniswap post (there's no need for screenshots because the article has no graphics):

> *Seed donors will receive all of their ICP tokens at Genesis Unlock, but these will be staked inside 49 voting neurons within the NNS. Each neuron that is delivered will have a different "dissolve delay" configured by the NNS. This configures the minimum period required to unlock the ICP tokens staked*

> *inside. One of their neurons will have a dissolve delay of 0 days, allowing the staked ICP tokens to be unlocked immediately, if desired (subject to applicable AML/KYC verification). Another will have a dissolve delay of approximately 30 days, another of 60 days, another of 90 days, and so on.(Note: Configured dissolve delays may have some small random number of days added or subtracted by the NNS).*

At the end, the article links to token access instructions. Seed supporters who viewed them eager to claim their tokens were confronted with pages of complicated technical steps that many say they weren't able to complete. The process couldn't even be done on a Windows computer or newer Macs built with Apple M1 chips.

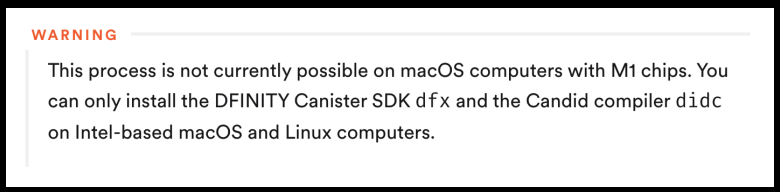

the latest release here. Note that the binaries are suffixed by the operating systems they run on, `didc-linux64` and `didc-macos`. Be sure to download the correct one. Below are commands to install `didc` on `macos`. If your're using Linux, simply use the `linux64` suffix instead.

```
sudo install -d /usr/local/bin
sudo install -m 0755 ~/Downloads/didc-macos /usr/local/bin/d
```

Regardless of which method you choose, you will also need to download and extract the NNS canister interfaces on your networked computer. You can find the latest release here. Below are commands to extract the NNS canister interfaces.

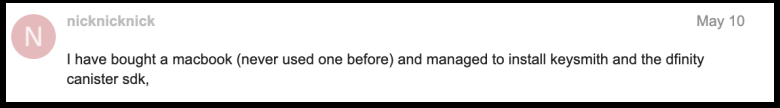
```
pushd ~/Downloads
tar -f nns-ifaces-0.8.0.tar.gz -x
popd
```

Additionally, you will need to have `dfx.json` file available in the directory

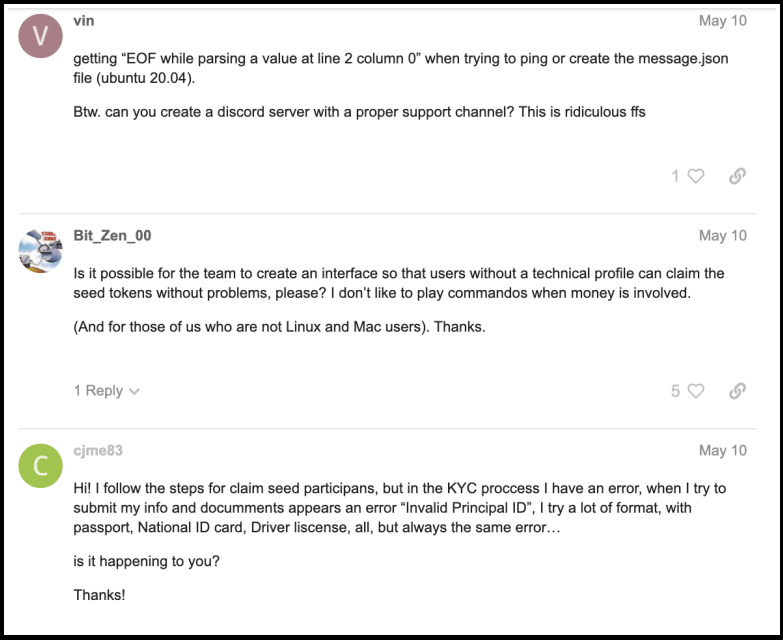

WARNING

This process is not currently possible on macOS computers with M1 chips. You can only install the DFINITY Canister SDK `dfx` and the Candid compiler `didc` on Intel-based macOS and Linux computers.

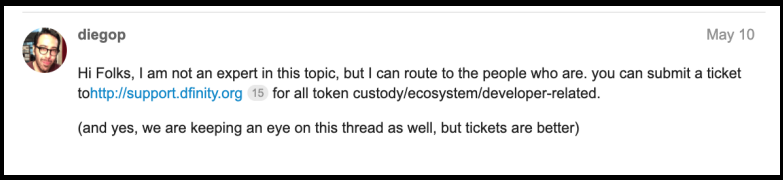
Besides being highly technical, the process appears to have been buggy. Many seed supporters who could decipher the steps say they ran into errors. You can see their desperation in the all time most popular post on the Dfinity forum, where they attempt to troubleshoot errors, beg for support from Dfinity, and commiserate over their shared predicament. One person says they bought a macbook just to access their tokens.


N nicknicknick May 10

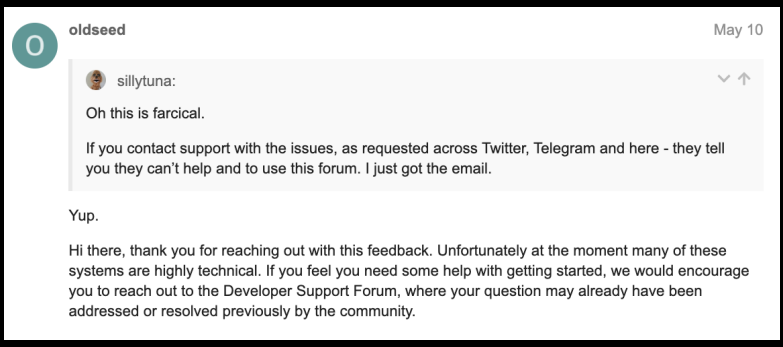
I have bought a macbook (never used one before) and managed to install keysmith and the dfinity canister sdk,



Amidst all this, Dfinity appears to have provided little help. A Dfinity team member advised people to submit "support tickets" rather than use the forum.

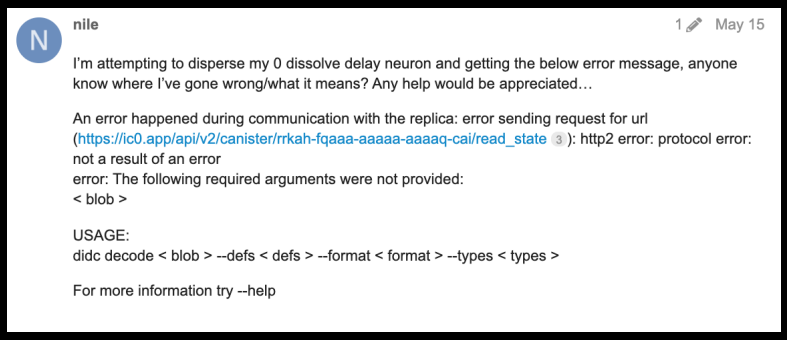


But upon submitting support tickets, apparently they were told to use the forum instead.



It appears the process wasn't made simpler after listing day either. People continue to post about bugs and ask for a simpler process, with little visible response from Dfinity.





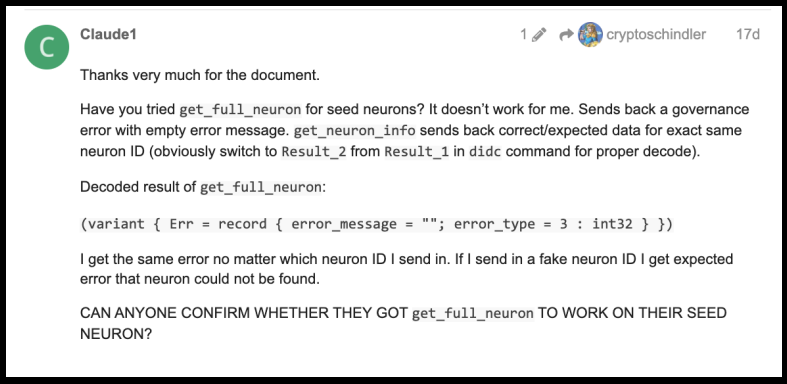
nile 1 May 15

I'm attempting to disperse my 0 dissolve delay neuron and getting the below error message, anyone know where I've gone wrong/what it means? Any help would be appreciated…

An error happened during communication with the replica: error sending request for url (https://ic0.app/api/v2/canister/rrkah-fqaaa-aaaaa-aaaaq-cai/read_state 3): http2 error: protocol error: not a result of an error
error: The following required arguments were not provided:
< blob >

USAGE:
didc decode < blob > --defs < defs > --format < format > --types < types >

For more information try --help



Claude1 1 cryptoschindler 17d

Thanks very much for the document.

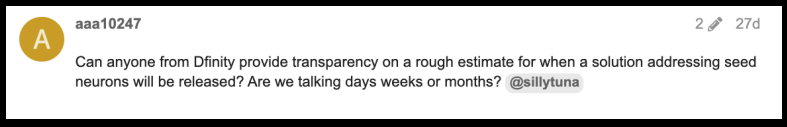
Have you tried `get_full_neuron` for seed neurons? It doesn't work for me. Sends back a governance error with empty error message. `get_neuron_info` sends back correct/expected data for exact same neuron ID (obviously switch to `Result_2` from `Result_1` in `didc` command for proper decode).

Decoded result of `get_full_neuron`:

```
(variant { Err = record { error_message = ""; error_type = 3 : int32 } })
```

I get the same error no matter which neuron ID I send in. If I send in a fake neuron ID I get expected error that neuron could not be found.

CAN ANYONE CONFIRM WHETHER THEY GOT `get_full_neuron` TO WORK ON THEIR SEED NEURON?



aaa10247 2 27d

Can anyone from Dfinity provide transparency on a rough estimate for when a solution addressing seed neurons will be released? Are we talking days weeks or months? @sillytuna

All of this raises questions. Dfinity has over 100 team members and 9 figures of funding, and they've been working on the ICP project for years. Why did they leave seed supporters in the dark about token unlocking and access until the day of listing? Why were the instructions so difficult? Why didn't they provide them with more support in the process?

For many of these supporters, buying ICP in 2017 may have been the best financial decision of their lives, and accessing their tokens could be life-changing. One can only imagine the frustration of watching a small fortune slip away while trying to wade through Dfinity's complicated instructions with minimal support.

The result of all this appears to be that seed investors were severely limited in their ability to sell their ICP, and this is reflected in our analysis of the ICP blockchain, according to which the vast majority of the 25 million ICP deposited to exchanges has come from the Treasury and suspected insiders linked to it.

If ICP insiders did intend to dump billions of dollars of ICP, then it would have made sense for them to make token access difficult for seed supporters, who could be the biggest group of rival sellers. By preventing or delaying their selling, downward price pressure would likely be greatly reduced, allowing insiders to get a better price for their ICP and take home more money.



Implications

Putting together the pieces of this analysis—large deposits to exchanges from the Treasury and suspected insiders, lack of transparency on token distribution, a byzantine process for outside supporters to claim tokens, and an ICP price collapse—an overall picture emerges. It appears that Dfinity insiders made billions of dollars dumping ICP on the market while making it difficult for their biggest potential rival sellers to dump theirs. It appears they tried to prevent outsiders from uncovering this activity through a lack of transparency about Dfinity's token allocation and unlocking. And it appears that their activity drove a massive crash in the price of ICP. When considering the dollar amounts involved, it might come to be viewed as one of the biggest financial controversies ever.

We must note that we cannot definitively say that ICP insiders carried out a pump-and-dump or a rug pull. We do not have direct confirmation that the addresses in question belong to ICP insiders or the project itself, or that the ICP tokens deposited to exchanges were sold. We have presented publicly in this report only what we consider to be the most indisputable and suggestive of the information that we've collected. We believe that taken together it suggests activity by ICP insiders that many would view very negatively.

That this happened shows the need for better intelligence and analytics on cryptocurrencies. If ICP buyers had known about these suspicious token flows and the accompanying off-chain activity, they would have been able to adjust their positions and protect their investments. Instead, many have suffered catastrophic losses.

Applications for this kind of intelligence go beyond uncovering potential insider selling. Traders can use it to collect many different types of price signals. Law enforcement can use it to detect criminals using crypto and bring them to justice. Researchers can use it to develop our understanding of markets. Intelligence tools are valuable for anyone interacting with cryptocurrencies, a group that is exponentially growing.

Like ICP, most blockchains remain murky. The expansion of crypto intelligence over the coming years will bring light to this shadowy world, allowing for better navigation of it. The implications of this coming transformation are manifold. Volatility could be greatly dampened because traders will have better information. Rug pulls could become a thing of the past. Criminals will no longer be able to hide in crypto because law enforcement will be able to detect them. All of this makes crypto healthier, giving it the strength to continue developing into a core part of the global technological system.

