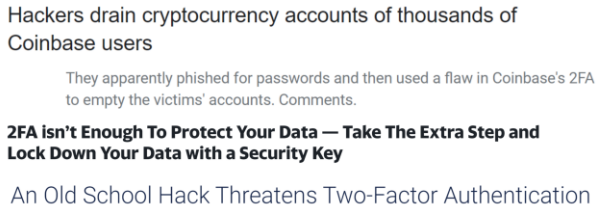
Deep Freeze – A DeFi Patience Primitive

Deep Freeze – A DeFi Patience Primitive

Intro

People are losing their crypto & NFTs to bad wallet security practices. It's too easy to reveal your seed phrase on screenshare (common social engineering attack) and hardware wallets (while not yet hacked) have had the manufacturers hacked, leaking tons of customer data that has led to more social engineering attacks and fake devices being sold second-hand. Having multiple wallets is an administrative headache and over-engineered solution to the real need: on-chain safe deposit boxes; or what we're calling "freezers" for on-chain cold storage.

Current Landscape



Hardware wallets work, they keep your seed phrase and private key completely separated from the computer they're placed into. Centralized solutions like keeping your assets on Coinbase work too. Multi-Signature wallets also work but can be pricy and are more suited for coordinating expenses across a group's shared assets.

What doesn't work, is the human factor. Humans get lazy and don't want to plug in their wallets so they use in-browser ones. They make a life-changing amount of money off NFTs and fall for over the counter (OTC) swap social engineering tricks. They use insecure authentication methods like text messaging. They're doing things *mostly* right and still losing.

It's become a meme that Bored Ape Yacht Club owners are especially hackable, but realistically, it's because it's one of the largest, most public, high value NFT communities so they are disproportionately targeted.

Deep Freeze – A DeFi Patience Primitive

Proposal

Deep Freeze will combine the best of custodial 2FA and hardware wallet support: a fully decentralized (no reliance on real world hardware device), non-custodial (no reliance on Coinbase or other corporation) protocol for creating smart contracts that accept deposits, but lock withdrawals behind a user defined password-hash pair. We expect users to continue using "hot" wallets for everyday trading and acquiring assets, but every user can and should have a safe deposit box ("freezer") for their long-term holdings (they can also accept deposits directly there to bypass their hot wallet).

An interesting side effect of having a password-hash pair that enables conditional locking of funds, is that it also solves 2 related problems in the asset security space: OTC swaps and intrinsic yield.

In review-

Deep Freeze gives additional security for long term holdings purely on-chain

Alice generates a freezer. She chooses to use the **optional** "hint" feature. She thinks of something unique but memorable and remembers that in 3rd grade there was a food fight in school and she got hit in the head by an apple. She makes the hint: What happened in 3rd grade with the apple?

Hint
What happened in 3rd grade with the apple?

She then uses an **unaffiliated** Keccak hash calculator (we don't want Alice to have to trust our Deep Freeze website isn't keylogging her or recording calculator inputs!) to get her password-hash pair.

Answer	Hash
I got hit in the head	876009e5f4588d510c19fc1e9abb92464eb54cd2e975f2099d4c10a6dd035e65

She then gives the Deep Freeze **only the hash** (and optionally, the hint too) – **not the password**.

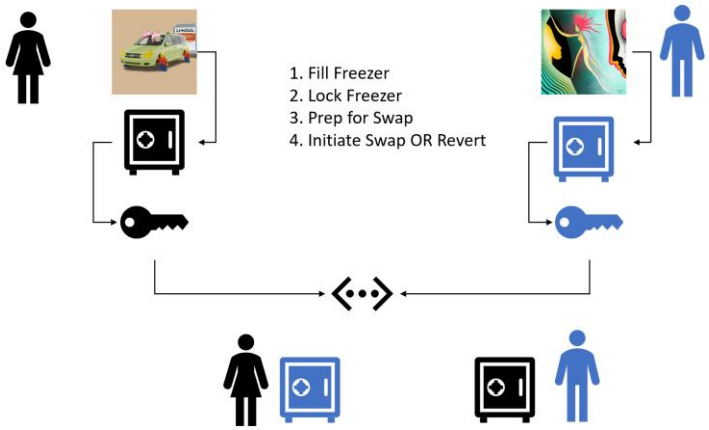
Her Freezer is now behind 2 layers of security- only she, the owner, can withdraw from the freezer AND in order to withdraw from the freezer, she must input a string that the smart contract independently hashes to match 876…e65 – the hash she provided originally.

By default, her freezer can accept the native blockchain asset (ETH on Ethereum, MATIC on Polygon, etc.), but freezers can also be coded to accept other assets (including NFTs and yield bearing assets!).

Deep Freeze – A DeFi Patience Primitive

Deep Freeze enables trustless OTC swaps

Alice and Bob want to swap NFTs, but they don't trust each other enough for either to send them first. They agree to use Deep Freeze to swap freezers containing their NFTs in a trustless way. To do this with absolutely zero trust requires a few checks. First, they fill their own freezers with the NFT. They then lock the freezers to disallow withdrawals for an agreed upon number of blocks (let's say 20 minutes). They then exchange freezer *contract addresses* so they can independently verify the freezers contain the asset they expect (note: they should **not** trust just the NFT image, but also verify the contract address of the NFT within the freezer) and that the freezer is locked. Finally, they initiate a swap and transfer their freezer to the Deep Freeze Swapper contract with their own freezer and the freezer they expect to own.



The Deep Freeze Swapper contract can be initiated once it controls both the expected freezers and confirms both freezers are locked. It then swaps the owner of those freezers and relinquishes control. If a freezer(s) provided are not locked or their lock(s) expire prior to swap, the swapper reverts ownership.

This generalized method allows for complex mixes of swaps, including both fungible and non-fungible tokens, while being fully trustless.

Password-Hash pairs can be optionally integrated to lock and unlock freezers. This may be useful for lower cost semi-trusted swaps, for example, locking freezers with a password-hash pair, changing ownership to the other party, and then waiting until the freezers have been exchanged to exchange passwords that unlock the freezers. The trustless swap avoids situations where one party receives access to the assets they expect but refuses to provide the password for the other party, effectively resulting in a "burn" of assets that can't be accessed by the owner without finding a hash collision.

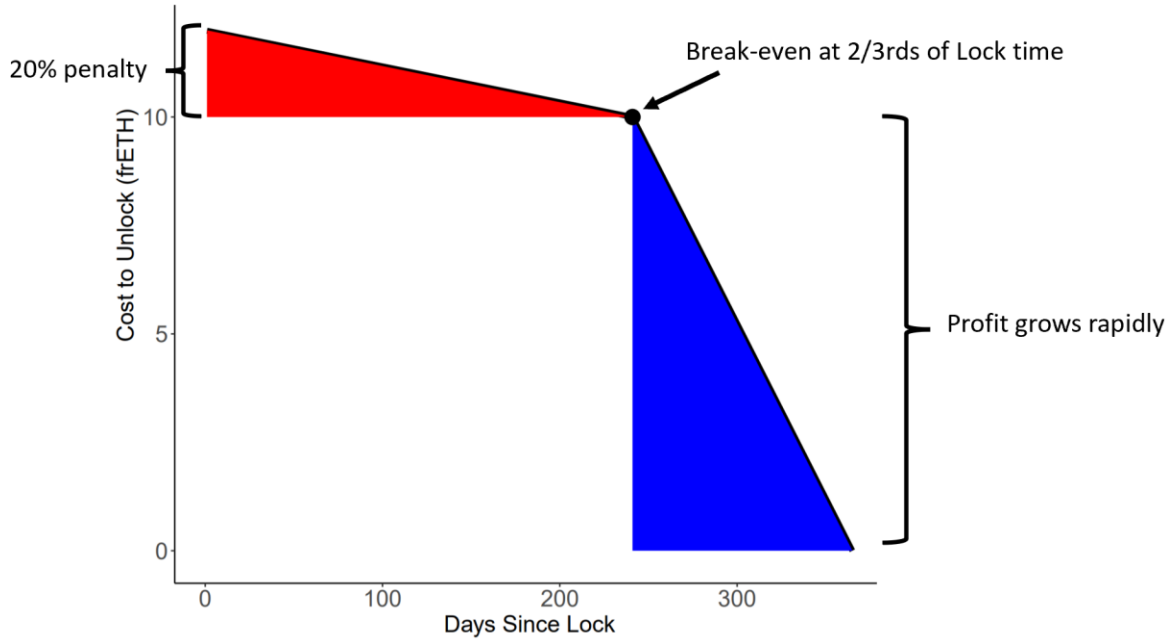
Deep Freeze – A DeFi Patience Primitive

Deep Freeze enables intrinsic yield paid upfront for turning patience into profit

Alice has some ETH she wants to secure long-term, but she also wants to generate yield. Her external yield options (those whose yield is paid by a function of other market participants) include blue chip protocols like AAVE, staking the ETH either herself or with a custodian to generate proof of stake yield (after the merge), and/or using other possibly riskier protocols along with an insurance provider like Nexus to cover smart contract risk. Given that this is her long term holdings, she doesn't want to rely on AAVE ETH (aETH) or Lido staked ETH (stETH) experiencing zero problems over the course of her deposit (not only loss of funds risk but also risk to her yield such as a contract migration that changes the market, e.g., AAVE V3 reducing yield for AAVE V2 deposits).

Deep Freeze enables her to lock her ETH for any desired amount of time and receive the frozen version of her asset – frETH. This works smoothly for any blockchain native asset (e.g., frozen MATIC on Polygon or frozen AVAX on Avalanche). For example, let's say she locks 10 ETH for 1 year. She receives 10 frETH in exchange.

This yield is *intrinsic* and paid upfront. To unlock her frozen ETH she can either wait the full year or pay some function of frETH to unlock it early based on how long she has left. For a 10 ETH deposit locked for 365 days, she is given 10 frETH. To unlock it immediately requires a 20% penalty (12 frETH). This cost falls every day until the break-even date (67% of the lock time), where it would cost 10 frETH to unlock. To incentivize waiting the full time period, the profit increases rapidly in the final 33% of lock time until it cost 0 frETH to unlock her ETH.

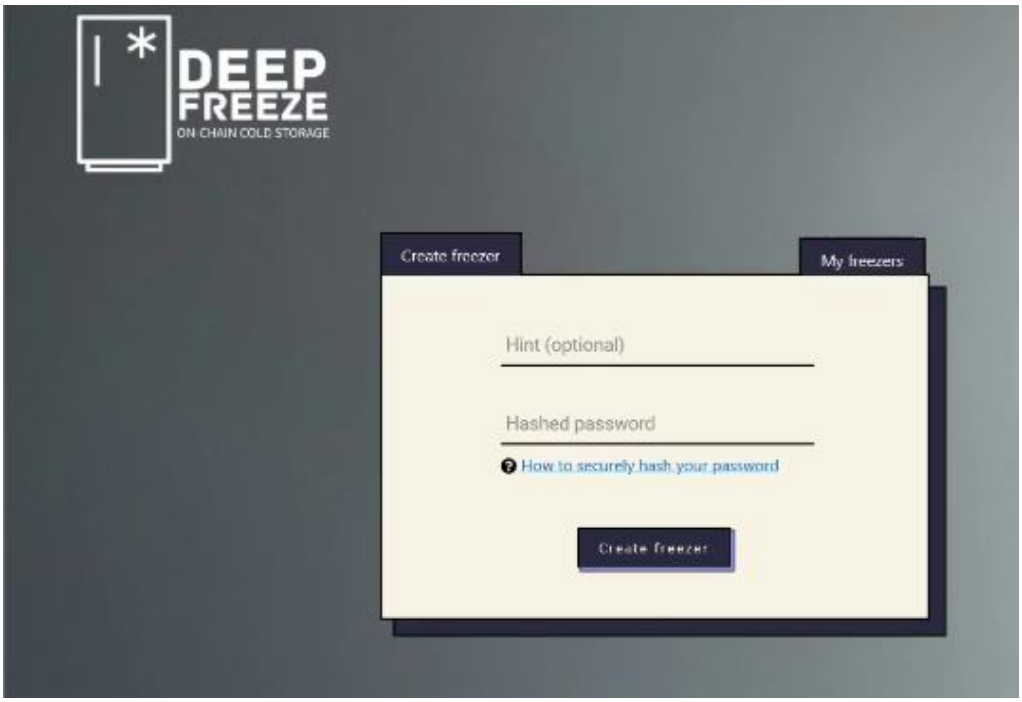


This creates a pure free market for tokenized *patience* itself. Non-users of Deep Freeze can engage in this market, hoard frETH, and increase the cost of impatience (and profit if doing so reduces the supply of ETH available in other markets- similar to how staked ETH is expected to reduce the circulating supply of ETH).

Deep Freeze – A DeFi Patience Primitive

Version 0

A Version 0 of Deep Freeze contains the 1st feature: password-hash protected freezers for the blockchain native asset (i.e., ETH on Ethereum). It is live on Rinkeby and has passed initial tests. A beta test with capped deposits will be released for community feedback prior to a full launch of Version 0 as an uncapped permanently free standalone protocol.



Version 1

Version 1 will be the fully developed vision of Deep Freeze containing password-hash protected freezers, OTC swaps, and intrinsic yield. There will be NFT freezers and blockchain native asset freezers (i.e., ETH on mainnet & Arbitrum, MATIC on Polygon, AVAX on Avalanche).

Revenue / Governance

Deep Freeze will be a 0 governance, 0 administrative protocol. It will be immutable upon launch with a fixed fee to generate revenue. Uncapped password-hash protected freezers (“Version 0”) will be made available on every chain it is launched with no cost (and will include blockchain native assets and NFTs). OTC swaps, being designed for NFTs (and thus, the freezer may not have a blockchain native asset balance to charge a fee to), will also be costless.

Intrinsic yield generates 2 revenue opportunities:

1. frETH penalties

frETH is minted upon locks and burned upon early unlocks. The frETH penalty above deposit (i.e., the 20% fee that is reduced until the breakeven point) is frETH taken out of the market (it only exists because someone has locked ETH and made their frETH available for purchase). This frETH can be paid to stakers of the Deep Freeze revenue token FRZ.

2. ETH withdrawals

To further incentivize patience, a small fee (e.g., 0.5%) can be applied to early withdrawals and paid to stakers of the Deep Freeze revenue token.

Next Steps

In Q1 2022 CharlieDAO is launching Deep Freeze V0 on its own website prior to spinning it out into a distinct entity and monetizing. Once spun-out, Deep Freeze V1’s features (OTC swaps and intrinsic yield) will be developed and tested. A formal launch of Deep Freeze V1 and the FRZ token will follow.

To speed up development, 20% of FRZ is anticipated to be allocated to the core team and early funders. If this project interests you as a developer and/or funder, please reach out to discuss more!