Gild Lab.

Semi Fungible Tokens
The How It Works Manual

GILD LAB LIMITED
Company number 13684709
Address Unit 8, 28 Mill Street, Ottery St. Mary, England, EX11 1AD

Contents

GILD LAB LIMITED
Company number 13684709
71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ

Simple introduction

Semi-Fungible Tokens (SFT) are assets like gold, silver, carbon credits which are broadly similar, with common properties but where the units are not completely interchangeable.

There is demand to bring SFTs onchain because asset holders are looking for new liquidity e.g. rewards for holding gold, new markets for carbon credits; and want to benefit from the low transaction cost, global footprint and fractionalisation of the crypto ecosystem and cryptocurrency holders are looking for asset / revenue backed yields for their stablecoins; they are cash rich and looking for diversification.

Example, LOVE TO Be Bright Green & ecological improvement

If land regeneration is measured and valued we can turn it into a financial product that rewards farmers (Producers) for the good work they've done, so that they can do more.
Producers don't have to own land in order to improve it. Often land is generational so the land and the ecological improvement are never really their asset to sell. But they can sell their ecological improvement work as a product just the same as they can sell their pumpkins, wheat or cattle,
A new market for ecological improvement is being developed. Now there are carbon credits and biodiversity credits. These are offsets for bad performance (grower +1, industry -1). If a company can't meet ecological improvement requirements, it needs to purchase offsets (carbon or biodiversity credits).
LOVE TO Be Bright Green is selling a product called ecological improvement (product produced by a farmer that has a market) and sells this to the capital market.
The assets backing the company are ecological improvement, verified by Producer Investment Evaluation (PIE) certificates.

Mutual creates value on top of ecological improvement through data etc

Love To & Gild Lab, through SFA creates a liquidity bridge offering exposure to physical assets in the form of commonly traded crypto asset investments.

SFT creates a decentralised link between real world semi-fungible assets, a community property they hold, e.g. income, and the decentralised finance community.

How does it work?

- The underlying asset, e.g. a particular warehouse, is represented with a non-fungible token (an ERC1155).
- A common property across all underlying assets, e.g. income from all warehouses, is represented with a fungible token, because it is shared (an ERC20)
- Asset holders receive the ERC1155 and sell the ERC20
- Cryptocurrency holders buy the ERC20

- Rewards earned are distributed to ERC20 holders
- Assets represent a closed ecosystem e.g. UK vaulted gold only, where there are no toxic assets that devalue the entire system
- Assets e.g. UK vaulted gold, vs Swiss vaulted gold can be traded / arbitraged as well as linked in baskets.

The custodian of an asset can only burn its onchain NFT by burning an equivalent amount of the fungible ERC20 token in the same transaction. This ensures that in aggregate the total supply of ERC20 tokens is always exactly the weight/content/revenue/valuations/etc. across all existing NFTs.

To do this we provide an audit layer, with clearly defined administration of both real world assets, and on chain replication:

- Professional advisors to validate, revalue, and audit the underlying asset.
- Technology to reflect changes in underlying asset or income generation within the cryptoasset tokens
- Reactionary governance set for movements in underlying assets including both solvent and insolvent liquidation events.

To establish trustworthiness between the custodians and non-custodians, a set of certifiers must be appointed. The certifiers audit and certify the claims made by each minted NFT against the assets in the real world. This could be a physical audit such as commodities in a vault/warehouse, financial audit of a business, fine art appraisal or anything else. The certifier publishes their certification that expires at a specific date/time. If the system does not receive a new certification before the expiry then all onchain assets are immediately frozen until a certifier signs off on an extension. The system freeze eliminates the ability for the custodian to arbitrage or collect other fees, so they are strongly incentivised to maintain the system through audit cycles.

In the case of a system wide freeze it is likely that some limited transactions will be needed to repair the internal ledger to a state that a certifier will be willing to unfreeze. A set of handlers can be appointed to receive and send frozen funds in a controlled way. Ideally handlers are rules-based smart contracts, but can also be trusted entities controlling a wallet directly.

What does our system provide that others don't:

- All documents for audit are visible to public, full transparency
- Orderbook offers algorithmic primary market, not reliant on liquidity of secondary markets for tokenomics
- No undercollateralisation
- Orderbook offers multi-token cyclic trading between like assets
- ERC 4626 compatibility
- General public can run data availability, indexing and consensus nodes for both tokens and audit data

- Fully open source and audited contracts.

Example, LOVE TO Be Bright Green customer benefit

For Love To Be Bright Green this means:

- Ability to transact in the onchain ecological improvement economy with the highest quality system
- Provide access to ecological improvement options for all
- All options issued are backed by audited ecological improvement generated
- Fully open source and audited contracts
- General public can run data availability, indexing and consensus nodes for both tokens and audit data
- Systems can adopt Love To ecological improvement options as standard, or at least if less reputable ecological improvement vendors in the future are exposed, Love To ecological improvement options stand independent as high quality
- Ecological improvement offered into the market have an algorithmic primary market, not reliant on liquidity of secondary markets for tokenomics which means no ponzinomics (traditional market, but decentralised)

Hasn’t this been done before?

Realt - Series LLC

Only works in very specific jurisdictions, they work on what is called a "series LLC" and they've many times looked into other jurisdictions and haven't found much traction, they offer direct ownership in a business that in turn owns a thing, so your token is a proxy for literal shares in a company-house, realt company is then appointed as manager.

PAXG/USDT

Neither Paxg or usdt offer any services that allow customers to spin up their own competing tokens to paxg/usdt, our system establishes a credibly neutral permissionless way for people to mint their own "proof of X" onchain and for the general public to not only consume but maintain mirrors/copies of these proofs, this is "vertically scaling" (everyone trusts one token to be the biggest and best and we all live and die by their liquidity, e.g. UST) vs. "horizontally scaling" (everyone can create tokens for themselves, and liquidity comes from free market behaviours rather than more eggs in the same basket).

Purpose build blockchains

The mere representation of something, a ledger, or a data structure, etc. is necessary but not sufficient for liquidity, blockchains live and die by their network effect not their apparent "technological superiority", taking assets to where buyers are is the reason to issue tokens in the first place, otherwise a centralised database may as well be employed as it is a far better representation/storage system than any blockchain.

Failed projects

Projects fail for many reasons, common issues are misplaced trust, failure to attract and retain liquidity, smart contract failures, "smart" tokenomics that turn out to be very dumb, etc.

Misplaced trust: we are building an open system, there will be many untrustworthy tokens and scams, the goal is to present an interface that effectively juxtaposes what a trustworthy token looks like (clean audits, quality assets, strong jurisdiction, etc.) against the scams so that end users can educate themselves and vote for the best tokens with their money. This isn't possible in a world of 2-3 liquid "trust us" style tokens.

Attract liquidity: typically smart contracts don't do primary marketplaces well, something as simple as the yearn buyback system is being hailed as somehow revolutionary, relying on secondary marketplaces means that secondary incentives need to be invented (e.g. "liquidity mining") and centralised primary marketplaces are entirely web2.0. We are collaborating/ leveraging the rain orderbook to allow onchain primary marketplaces to be defined via. the scriptable order book.

Smart contract failures: we have a permissionless factory model, which means every SFT deployed under the same factory has the same bytecode, the factory has no ability to be upgraded, which means that the contracts accrue "lindy" over time, which means that the longer they are not hacked at the code level, the longer we can expect them to continue to not be hacked. This means that the system becomes stronger as more liquidity "scales in" to it (upgradeable contracts do not have this property as new bugs/vulnerabilities can be introduced with every upgrade).

"Smart tokenomics": SFT has zero tokenomics beyond the onchain/offchain value binding via the NFT receipt and audit system. There are no fees, liquidity mining or other systems that often end up being intentional or unintentional ponzis that ultimately implode. Even the PAXG fee structure runs counter to the use of gold as a store of value, as fees are only accrued to the issuer when the tokens are transferred, etc. The primary utility/value for custodians of an SFT is liquidity+arbitrage. It takes custodians to a new market and gives them first seat at the table for onchain/offchain arbitrage against their own peg.

Getting introduced and prepared

Building context, getting prepared and ideating prior to the design session.

Introduction

Semi Fungible Tokens is a solution to connect sets of custodial assets to decentralised fungible tokens. The price of the fungible token is primarily set by the custodian's ability to arbitrage onchain and off chain simultaneously.

The assets themselves can be arbitrarily non-fungible but need to have some property that is fungible between them. It could be anything from weight, pure chemical/elemental content, revenue, etc. but there must be ONE common measure. This common measurement is used to mint ERC20 fungible tokens in the same transaction as the NFT in the same ERC1155 amount of the NFT.

Importantly the fungible property must have a liquid off chain market. Precious metals are a great example. They can already be valued, bought and sold by their pure weight in established and deep global markets. Numismatic coins on the other hand may have a pure gold/silver weight equivalent price but typically their offchain market price is determined by their collectible value, and a specific coin is not readily bought/sold for a clear spot price.

These requirements exist because the price of the fungible token is primarily set by the custodian's ability to arbitrage onchain and off chain simultaneously. If the offchain assets cannot be readily bought/sold for a clear price that is measured in the same way as the fungible tokens minted by the custodians, then there is no way for the onchain tokens to maintain price stability against the offchain assets. This model does NOT imply or require that end-user token holders have any rights or claim over the underlying assets, or physical delivery, etc. That "direct ownership" model would require users to be doing onchain/offchain arbitrage themselves, which presents logistical, regulatory, and liquidity problems that the custodian can avoid or manage themselves.

There IS a form of physical allocation in that the NFT audits force the custodian to have any/all physical assets they mint fungible tokens against, but the allocation by the custodian doesn't imply ownership for the end-user.

The vault can't complete an audit without either all the gold bars the NFTs they hold say they should have in their vault and they can't burn NFTs without the FTs they minted. Nobody seems to own the gold in that scenario. the game/incentives seem to line up, the vault wants to pass audit or their fees will be accruing in a worthless ERC20. but i don't know if holding the FT constitutes "ownership" or just an implied threat of failed audit if something goes missing decentralised audit accountability, or something…

Within the ecosystem there are issuers, auditors, end-users

- Issuers have the right to mint/burn NFTs that represent something physical
- Auditors have the right to approve the NFTs to extend the system freeze (kind of like the difficulty bomb in Ethereum itself)
- End users are the ppl who have the 20 and are the one's that get frozen if no auditor extends the time
- A DAO might be able to add/remove issuers and auditors over time, for example

Example, Audit failure

> So say one issuer couldn't pass audit and there was 1 bar missing, another issuer could buy enough 20 on the open market to buy them out and burn the bad NFT and the issuers would have to work as a team. Even if the system was frozen for end users the issuers themselves could trade against an AMM, but ideally they'd resolve issues before the freeze actually kicks in, if the freeze kicks in and there's no liquidity for issuers to access, they're kinda fucked if they can't convince an auditor to extend… but that's the teeth in the system that lets end users trust it.

Preparation

Read system design

Read use cases

Ideation

- Before the design meeting
- Describe your product or service
- Identify the value of creating a digital currency
- Identify what you think a common property across your assets might be
- Identify how an audit might look - who, how, when, where, what
- Identify the unique assets you want to tokenise

Description Asset Class ERC1155

- ERC1155 generated for each asset class (agri, hotel, residential, commercial)
- ERC1155 can be added for individual assets if required
- 1155 can't hold any info onchain, it passes info through to the subgraph to point to this info on IPFS, essentially 1155 is used to track audits
- 1155 natively supports an amount (721 every NFT is itself); 1155 is a hybrid - ID and amount every 1155 has its own balance
- The 1155 amount minted/burned matches 20 mints/burns (see next page for table).

Issuance	ERC1155 is issued by IFL LLC when a new asset or asset class is purchased which will generate income for fixed income holders
Transaction	ERC1155 is not designed to be tradeable as a speculative asset, it is generated, audited, updated and burned; there are no taxes or limitations on the ERC1155. The ERC1155 represents auditable onchain evidence of the ability and responsibility to pay the dividend commitments of the associated ERC20 circulating supply.
Interplay	ERC1155 'metadata' is updated by auditors confirming information like income, valuation
Retirement	When the asset or asset class is disposed of the ERC1155 is burned

Description Asset Class ERC20

- ERC20 generated for each $1 income generated by the NFT collection in its entirety
- ERC20 represents fixed income, the ERC20 should have a fairly stable value - whatever people believe; Potentially valued something like bonds but not exactly because they aren't debt interest or time bound, rather they are backed by existing revenue producing assets. (See below).

Issuance	ERC20 is issued by BVI foundation when new income is added to the system through the form of an audited ERC1155, which signals that more fixed income is able to be generated by the system and sold. The smart contract automatically and unavoidably mints and burns the ERC20 tokens in lockstep with ERC1155 token amounts.
Transaction	ERC20 is tradable for any other ERC20 token; ERC20 is used as a 'token' to claim income produced by the system
Interplay	ERC20 can be bridged across different blockchains and can be traded by CEX, DEX, direct transfer or other means
Retirement	When NFT collection income is less than the total ERC20's in circulation then ERC20's need to be burned so the relationship between audited income on the NFTs and ERC20's in circulation is always consistent

There are different ways the value of the ERC20 can be expressed. For example these are options put to Sark.

Ideation Option 1 - Fixed income

- Rather than maintaining a price peg on the mint/burn, we impose a legal restriction that the asset cannot be sold as long as tokens are outstanding (simplification), and then somehow the % APY for each asset becomes what makes the tokens fungible.
    - Product: Fixed income product, legally guarantee people get a certain amount with a buffer.
- Innovation: APY becomes a fungible asset, this gets around the issue with property where assets are not fungible on asset price.
- Issuer: So rather than issuing $100M worth of tokens, say the asset will bring in $10M a year of profit, so let's issue 10M tokens
- Purchase price & payback: Like any fixed income product, $1 purchase would generate $0.10 a year (issue ERC20 tokens at 10x value), payback over 10 year period.
- Value: Basically like a bond - value of the bond, tracking how much people value fixed income, bearish product; Track inversely to stock market.
- Asset owner: Asset owner generates addition returns above the fixed income which are its profits, plus it needs funds to maintain fixed income payment in case of asset or income issues.

Option 1A - Fixed income + Collateralisation

Given the fixed income product is government backed and fully insured

We can partner with onchain collateralisation provider and support users to collateralise this fixed income product

Assets back the collateralisation given they are providing this revenue

Option 1B - Fixed income + Borrow & Buy Back

- Participants in the fixed income product can also borrow against the product and have it automatically paid back
- Buy 100K of the ERC20
- Borrow 20% on the ERC20
- Pay off the debt automatically
    - Participants in the fixed income product can also borrow against the product and have it automatically paid back
- Buy 100K of the ERC20
    - Borrow 20% on the ERC20
    - Pay off the debt automatically

Option 1C - Fixed token buyback

- Same issuance structure, but the audited income is used to buy back tokens rather than distribute income
- Buybacks have two issues:

1. They change the price of the thing being bought in an unpredictable way, so how to audit that?

2. They assume liquidity, which assumes fungibility and available pairs

- The challenge with a buyback is it turns the ecosystem into speculation, rather the supporting the regeneration of the assets

Option 1D - Indefinite buybacks and resale algorithmically

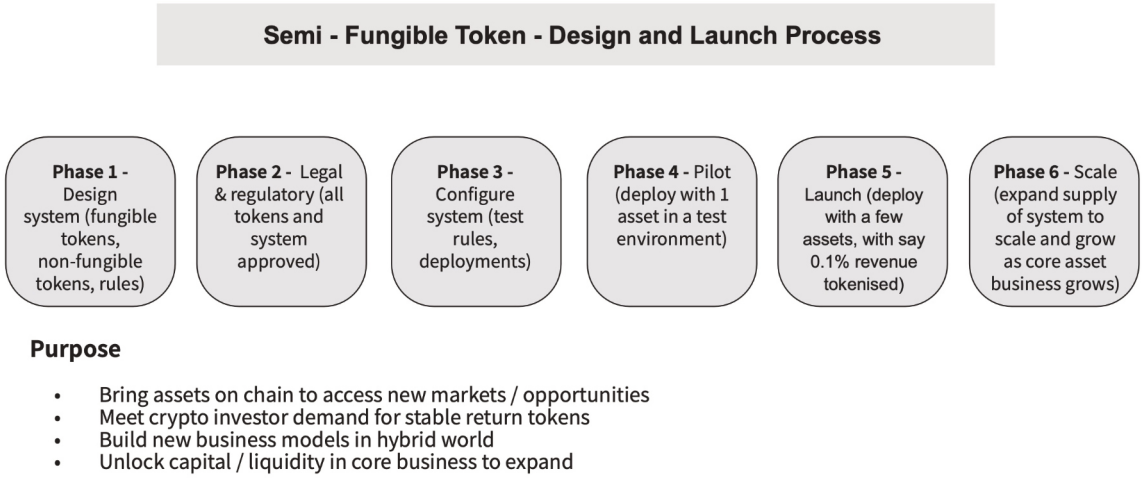
- We wouldn't even try to setup LP pairs we would just dump rent into the vending machine
- Basically ppl would expect when they buy a minted token to be able to sell it back for a higher price later as rent comes in
- You sell 1000 tokens for $1000 each and raise a mill
- dump whatever revenue you are getting in the vending machine at $1100 per token
- have the vending machine impose a cap so that it never takes in more $ than tokens are outstanding
- it's still a "fixed ROI" product
- concerned that infrastructure projects turn into ghost towns full of half finished concrete shells if their funding dumps too hard
- this model is better for buying and flipping as a one time thing

Question, how do I make money?

Once the requirements are met for an asset, the custodian can profit simply by arbitraging price divergences. There is no need for additional fees from the custodian to the end user to cover costs. For example, if the price of the offchain asset is higher than the onchain token, the custodian has sole right (enforced by the contract) to buy back the token and burn it, then sell the assets in custody for profit. The reverse is also true. If the off chain price is cheaper than the onchain token, the custodian can purchase additional stock and sell newly minted tokens for a profit until the price normalises.

Getting started

System phases



Purpose

- Bring assets on chain to access new markets / opportunities
- Meet crypto investor demand for stable return tokens
- Build new business models in hybrid world
- Unlock capital / liquidity in core business to expand

Design phase

Beginning the design phase

Step	Design	Outcome
Define common property	Brainstorm possible common properties e.g. income, yield, weight. Does your industry have a common property standard?What is the liquid off chain market for the fungible property?Check whether you are double counting tokens. Check the relationship between the common property and the unique asset, are they being double counted? Plan token listing strategy on DEX (AMM) and CEX (Order book) or Gild Labs DCEX (Decentralised OrderBook). Define units of common property per 1 TKN. Define TKNs per $1 value. Name	
Define unique assets	Specify end-user token holders have any rights or claim over the underlying assets, or physical delivery (if any)	
Define audit process		
Arbitrage	Design and establish arbitrage system (custodian can profit simply by arbitraging price divergences)	

Example, Future Grow Cannabis

> Let’s take this example, FutureGrow, cannabis producer. What is fungible, for example for cannabis is THC level fungible? Is the final product weight fungible?
>
> Naively we would expect it to be THC as that's the most low level chemical, like pure alcohol content, it's the thing that ends up being equal. Put it in the context of gold, it's the purity at a certain weight -- as prescribed by the LBMA (industry standard). So cannabis would be THC level at a certain weight -- but no industry standard so we'll have to establish that standard?
>
> When they mint a new plant they have a forecast on what they plan to extract from it, and i'm sure that at the end of the process they very carefully measure everything during extraction. Is it "pure THC" that is the fungible bit? because if so, that's what the ERC20 represents.

Develop & test phase

Work with our initial design

- Figma
- Github
- Web

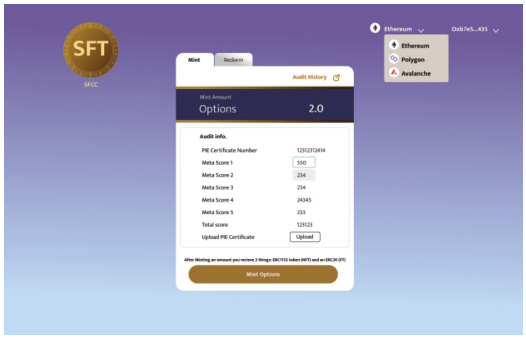
Create your screens especially focussing on

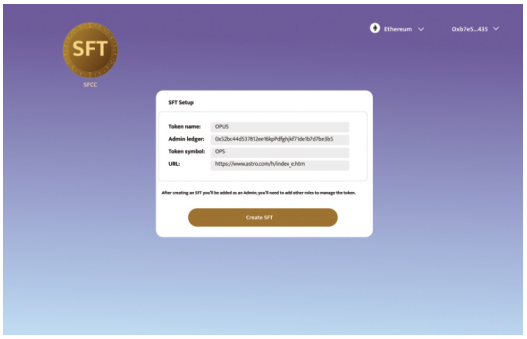
- 1155 design
- 20 name and details
- Look and feel

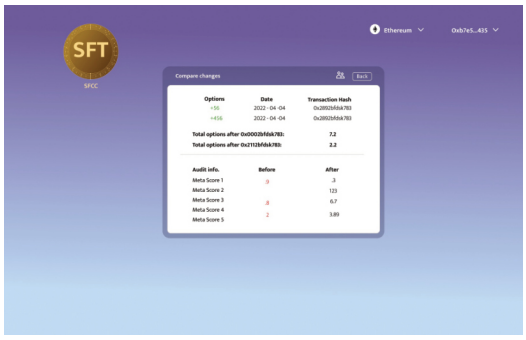
Can use our template or new template you create

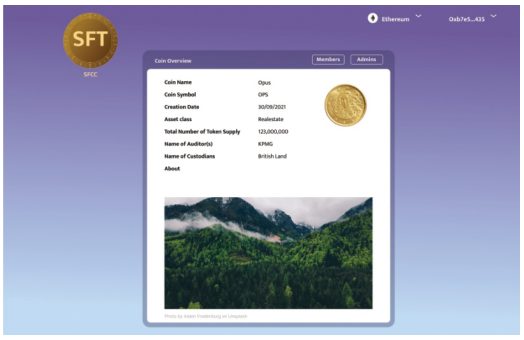
Step	Details	Outcome
Review Gild Labs screens	What questions do you have? Are you clear what first, where? Are you clear how you will design your system?	
Being to build your screens	Use our SDK	
Connect your infrastructure	Your screens + subgraph + IPFS (we set up for you)	
Deploy test	Deploy on testnet and begin to test with your ecosystem	

Some example screens









Legals & Regulatory

Getting legal and regulatory right is crucial to the system's success

Step	Details	Outcome
Legal	How are the ERC20s treated? How are the ERC1155s treated? If ERC20s are a security, how are these regulated? Who can purchase, what are the conditions and how is KYC done?	
Regulatory	Which jurisdiction?	
Audits	What audits happening? On what levels?	

Example, LOVE TO Be Bright Green

We concluded that there are two levels of audit happening: (1) the audit that results in a PIE certificate; and (2) the audit that lines up the shares sitting on top of the PIE certificate with the blockchain (de-identified PIE certificates end up on chain?).

They worried out loud a lot that the crypto they issue would end up in the hands of investors in countries that they haven't done the regulatory work for.

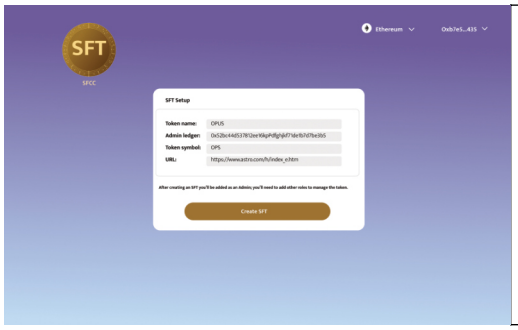
They are working with McMahon Clarke for their regulatory work (ASIC forms etc). Their lawyer, Langton Clarke, who they have a long relationship with, doesn't know anything about crypto.

We aren't sure how to manage AFSL licensing obligations for our SFT system (called Moneybox). It contains off chain assets which are issued by a Mutual (public) company. These have price discovery and some liquidity though listed markets or private (pre-IPO) markets. The securities are issued to Producers who then sell or keep the assets – so the market is really dealing in secondary sales, even at IPO stage. The MCIs have a face value of $100 and are issued to Producers based on the value of their regenerative work. Producers may be Producer Members of the (Australian) Mutual from anywhere in the world. Likewise, Investors may operate in any jurisdiction. The Mutual needs to comply with Australian law at issuance and for direct sales where we are marketing only our own securities. We aren't sure if wrapping these in a Moneybox constitutes a new security, and therefore what regulatory regime is required to do this in any nation using a platform that may not have Australian jurisdiction.

Roles

The Super Admin role

When a new CertifiedAssetConnect contract is deployed, an initial admin can be set that is the admin for every role. Initially there are no executors. **It is strongly recommended that the initial admin delegates each of the admin roles to more appropriate addresses and renounces its "superadmin" powers** as soon as possible.



Super admin is set on setup screen

The Admin Role

An admin of a role appoints/revokes executors and other admins, including themselves. This means that any admin can unilaterally and permanently remove all other admins, or even all admins entirely for their role. Clearly the private keys for admin roles must be handled very

securely such as an M of N multisignature setup or even a formal governance contract that can only action the results of onchain voting.

E.g.

DEPOSITOR_ADMIN
WITHDRAWER_ADMIN
CERTIFIER_ADMIN
HANDLER_ADMIN
ERC20TIERER_ADMIN
ERC1155TIERER_ADMIN
ERC20SNAPSHOTTER_ADMIN
CONFISCATOR_ADMIN

The Executor role

The executor of a role merely executes the day to day operations associated with that role. Connectors connect, certifiers certify, etc. There can be many executors assigned to any role, as set by the role admin(s). **Executors generally share responsibility over their task**, a single rogue connector can poison the contract with forgeries, a single rogue certifier can freeze the system, etc. As it is entirely possible to achieve M of N control over private keys, this is expected to be achieved outside the logic of the contract. A single executor key may represent a group of many off-chain entities. An executor may also be a formal governance contract enforcing arbitrary workflows for actions.

Information is onchain

All the role admins and executors, as well as the configuration that they set is all public information onchain. **This allows token holders to always review for themselves how centralised or decentralised a given CertifiedAssetConnect contract is**.

Depositor

Connectors "connect" off-chain assets to onchain tokens. I.e. They mint matching 1155 NFTs and ERC20 tokens.

There is a single connect function on the contract that takes an amount of 1155/20 to mint and some data that feeds into audit reports for certifiers to review. Most likely the data would be something like an IPFS hash that can be fetched and processed by scripts rather than literal audit data.

For example, say a connector was minting a barrel of whiskey in a warehouse. The data about the barrel could contain all kinds of information relevant to an audit, but only the LPA (litres of pure alcohol) amount would be used to mint the 1155/20 tokens.

Typically a connector would also be a disconnector but it is not required.

`Withdrawer`

The opposite of a connector. They "disconnect" off-chain assets by burning onchain assets.

The disconnector must hold both the NFT and enough ERC20 tokens to cover the full amount associated with the NFT in order to complete the burn. This guarantees that the aggregate amounts across all NFTs and issued ERC20 tokens are 1:1 at all times.

Disconnecting an asset is permanent/irreversible but a connector can always reconnect a previously disconnected asset with a new amount and associated audit data. In this way connected assets cannot be changed but they can be burned and re-minted with updated information prior to audit.

Partial disconnections are disallowed so it is recommended to connect assets in the size and configurations that they are typically acquired and disposed of. For example, a real estate fund would be better served connecting/disconnecting houses than entire suburbs.

Typically a disconnector would also be a connector but it is not required.

`Certifier`

The certifier can call the certify function to either extend or override the current certification period. By default a new certification will only maintain or increase the current certification expiry date, but a certifier may pass an additional parameter to force a specific (potentially shorter or even past) date.

Certifiers are expected to pass in additional data to reference an audit report that justifies their certification.

An audit process would typically look like:

- The certifier runs a script to extract auditable information from the blockchain logs for all connects and disconnects
- The certifier performs a real world audit of the offchain assets against the extract
- The result of the audit is posted onchain with the certify function

Multiple parallel audits are supported as each certifier can submit their own reports without interfering with each other's logs (with the exception of the forced expiry override described above).

If the certification ever expires then all assets are immediately frozen for all participants except handlers. This includes a freeze on connecting and disconnecting and for all admins!

Typically a certifier is only a certifier. They should be an "arms length" participant that can be trusted to be impartial. An impartial entity probably should not hold assets or other privileged roles as this could be seen as a conflict of interest.

Handler

Handlers are the only accounts that can send and receive either the NFT or ERC20 tokens in the event of a system freeze due to lapse in certification.

A handler need not be appointed immediately or ideally ever. In the case that the audit process breaks down and the certification cannot be granted the certifier should provide a remediation plan. The remediation plan should list a minimal set of actions that a handler can take to restore the system to a certifiable state as quickly and directly as possible.

The handler can be either a nominated EOA (externally owned account) or a smart contract. The latter could be more trustworthy as it is purely rules based, but the former may be more practical in a time sensitive situation.

It may be required that the handler is also appointed as a connector and/or disconnector to repair discrepancies in the onchain and off-chain overall asset supply.

Once the system is repaired and certified the handler role should be revoked/renounced.

Tierer

Tierers can define (or remove) standard Rain protocol ITier restrictions on transfers for both the NFT and associated ERC20.

ITier is an interface that allows for up to 8 membership levels (e.g. bronze, silver, gold, etc.) to be assigned efficiently to any address.

One common use case for custodial assets is to handle regulatory requirements such as KYC/AML restrictions. Rain protocol provides a standard Verify contract that is backend-agnostic to allow KYC/AML approvals to feed into ITier contracts.

ITier can also function as a "block list" rather than an "approve list" for more decentralised asset management. For example, USDC adopts this model, allowing all addresses to transfer by default and freezing only accounts explicitly flagged by law enforcement.

If a user already holds tokens and is removed from the requisite tier, either because they lost the tier or the tier contract itself changed, then they can send but not receive tokens.

Tierers do not themselves define the users who can interact with the tokens, rather they define the contracts that do implement access restrictions, and the minimum tier that must be held for access.

A highly centralised system can tightly control and even change their tiering logic over time. A more decentralised system can set up tiering and then renounce the admins, or even completely remove tier restrictions.

ERC20TIERER
ERC1155TIERER
ERC20SNAPSHOTTER

Confiscator

As all offchain assets have some custodian there will be some regulatory environment that the custodian operates within. Typically this implies the possibility of legal actions such as sanctions being placed on token holders. Under extreme circumstances it may not be enough to simply freeze assets by removing the holder from the relevant tier contract. In some cases the assets may need to be confiscated from the token holder then somehow processed (e.g. burned, set aside or redistributed) by the custodian.

There is a confiscator role that can forcibly take frozen tokens, both the ERC20 and ERC1155. This is obviously a highly sensitive role and action so confiscators cannot forcibly take tokens from unfrozen assets. This provides some protection against some malicious actor compromising the confiscator and arbitrarily stealing assets from users. First some attacker must compromise the tier handling before they could manipulate the confiscation process. Ideally the real world entities managing the confiscation and tiering are independent and arms length for maximum security. If there is no tier contract set then the confiscator is free to confiscate any asset from any address, so this is potentially a less secure configuration.

Confiscation is a simple transfer, the confiscator calls the relevant function on the smart contract and the assets are transferred to themselves. Confiscation bypasses normal transfer access requirements so confiscations are still possible during a failed audit. The best defence against a rogue confiscator is a well maintained tier contract.

Go Live

Achieving liquid markets for any asset is non-trivial in general and out of scope of this document. If an off-chain liquid market already exists, then an on-chain market can be established through either a standard LP based DEX (requires correlated token pairs) or a rain DEX order book (requires a market making strategy). For example, if the custodian is willing to use or provide a price oracle they can create a rain order that automatically tracks a spread of +/- some % around the oracle price. This will buy and sell onchain around the peg without any further management by the custodian (e.g. no need for bots etc.). If the peg breaks completely through the onchain

order due to exhausting the custodian's funds in the order, the custodian can continually withdraw from the DEX, then buy/sell off chain, then deposit more funds from the off chain trade until the peg is restored (at a profit for the custodian defined by their order spread).

There's no assumption that the fungible ERC20 tokens maintain a price peg with the off-chain markets for the assets in custody. It is definitely implied and expected due to the profitable arbitrage both above and below the peg for the custodian, but the fidelity of the peg relies on the actions of the custodian. This may be a desirable property of the system so it is achievable given some additional conditions:

There is a liquid secondary market for the ERC20 token that allows efficient arbitrage

The custodians can participate in profitable arbitrage through off-chain markets for the assets in custody

The custodian actually does take an active role in buying and selling the offchain assets on the time scale that the peg is expected to be maintained over

The final point is important. It is entirely possible that a custodian has the ability to buy and sell off chain assets reliably over days/months/years but no ability to maintain a spot price over minutes/hours/days. In this case the price will fluctuate organically as traders speculate against each other between the orders placed by the custodian.

Example, LOVE TO Be Bright Green

- LOVE TO are concerned about primary and secondary market sales:
- Sell SFT via treasury to investors; at this stage all understand it’s got limited liquidity
- Limit supply of sold SFTs to business needs so to not flood market with supply
- In parallel to listing options / shares on any regulatory sandbox or stock exchange which will only enhance the SFT and it’s liquidity
- After a period of the SFT live but no liquidity launch a marketplace which gives possibility of liquidity and choose tokens to trade the SFT against
- Treasury issue supply at discretion through this period
- Support LOVE TO and users to do price discovery on this order book
- Scale up price discovery as SFT develops the offchain market

Audit

We will need to build an auditing system for onboarding the physical gold and tokenising each as an NFT; and the ERC20 gold coins backed to each NFT; and the entire back-office to mint and burn, and even insure the accounting of all of these tokens along with the auditors…

Ideally the auditor does their normal audit, then does "export to csv", then runs the script against a recent blockchain snapshot.

If they have more than enough money, great; if they don’t have enough money, if you are short you have to buy the tokens back off the market and burn them to cover the audit.

- Auditor gets data, assets have to be able to make commitments
- If auditor is happy, call the certify function
- If happy call until function, to continue operating the system
- Pass in data that goes with the certification
- Whole system freezes itself if certification runs out

Seriously how would the monthly audits tie into this? Do we or should we tie the audits into this?

1. Each month the auditor signs off on an extension to the system
2. Exactly like how PCI-DSS audits work
3. If you don't pass audit you're not legally allowed to continue processing payments

If they are doing monthly audits maybe the auditor signs off on a 3 month extension or something; do we can build in some buffer, but at some point there has to be a consequence of NFTs onchain that aren't in the vault. This is also how Ethereum itself works btw, if all the nodes don't hard fork periodically with a new version of the core code then the whole blockchain stops.

Maybe a very tiny buffer but is it necessary?

Only necessary to the point that ppl tend to be disorganised. If an auditor gets covid and can't come in for a few weeks we don't want that to blow up the system.

Maintain / scale

Offchain Asset Vault

Enables curators of offchain assets to create a token that they can arbitrage offchain assets against onchain assets. This allows them to maintain a peg between offchain and onchain markets.

At a high level this works because the custodian can always profitably trade the peg against offchain markets in both directions.

Price is higher onchain: Custodian can buy/produce assets offchain and mint tokens then sell the tokens for more than the assets would sell for offchain thus making a profit. The sale of the tokens brings the onchain price down. Price is higher offchain: Custodian can sell assets offchain and buyback+burn tokens onchain for less than the offchain sale, thus making a profit. The token purchase brings the onchain price up.

In contrast to pure algorithmic tokens and sentiment based stablecoins, a competent custodian can profit "infinitely" to maintain the peg no matter how badly the peg breaks. As long as every

token is fully collateralised by liquid offchain assets tokens can be profitably bought and burned by the custodian all the way to 0 token supply.

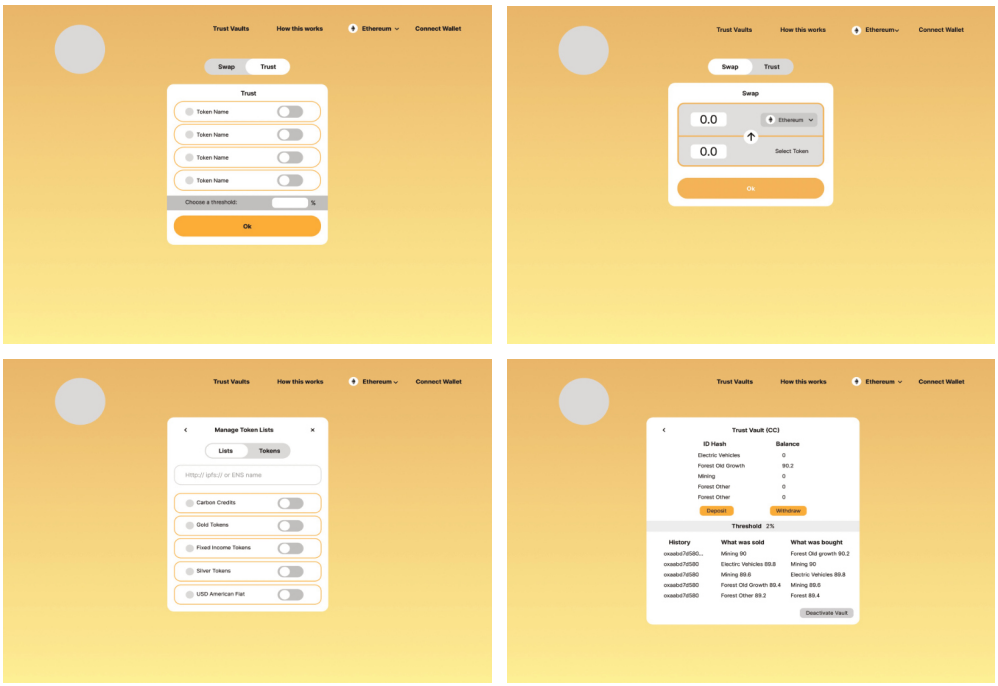
This model is contingent on existing onchain and offchain liquidity and the custodian being competent. These requirements are non-trivial. There are far more incompetent and malicious custodians than competent ones. Only so many bars of gold can fit in a vault, and only so many trees that can live in a forest.

This contract does not attempt to solve for liquidity and trustworthiness, it only seeks to provide baseline functionality that a competent custodian will need to tackle the problem. The implementation provides:

- ReceiptVault base that allows a transparent onchain/offchain audit history
- Certifier role that allows for audits of offchain assets that can fail
- KYC/membership lists that can restrict who can hold/transfer assets
- Ability to comply with sanctions/regulators by confiscating assets
- ERC20 shares in the vault that can be traded minted/burned to track a peg
- ERC4626 compliant vault interface (inherited from ReceiptVault)

Fine grained standard Open Zeppelin access control for all system roles

Some screens for trading



What if one asset is underperforming?

If one asset is underperforming, it can be propped up by another asset, You can also buy back the tokens

- In aggregate across all ERC20s, this is how much money everybody is entitled to get that number, here is our commitment across all constituent assets
- Model can continue to scale with each new income generating asset increasing the supply of the ERC20
- And each asset disposal or income reduction decreasing the supply of the ERC20

Step	Details	Outcome
Time period		
Removing ERC20s from circulation	Bn	
ERC1155 planning		
ERC20 planning		

One way of maintaining the peg is where people are choosing which tokens they believe are equal quality. Drawing from parallels with USDT/USDC/DAI they pick tokens and a threshold to defend the peg. Everyone chooses for themselves which pegs they are willing to be buyers/sellers of 24/7 and if a peg breaks, game over. It has the potential to give custodians a lot of liquidity for their tokens, because they all have full access to any capital sandbox they are included in.

Future, maintaining an open marketplace built on the rain order book themed by asset class.

People can place orders defined in terms of oracle prices for the assets like "buy/sell +/- X% from the CC price oracle" and bots will just maintain the peg. Any time someone wants to know where an asset comes from they just click the audit history and it's all there right down to the certification batch from the EV machine.

Cycling assets or maintaining the system

Custodians may not hold perfectly static eternal assets. While a gold bar in a vault or a house may be easy to consider, there are many assets such as agricultural crops that have natural life cycles.

At first glance it may seem easy for connectors and disconnectors to work together to buy back ERC20 assets from the market, burn the NFTs for the old assets and connect new assets for new assets. The problem with this is that liquidity for any tradable asset starts high and then quickly drops as the market runs dry, leading to huge price spikes.

Said another way, as the ERC20 holders notice what is happening, they have every incentive to ask for astronomical prices knowing that the old NFTs cannot be disconnected until the disconnector holds enough ERC20 tokens to cover the NFTs being burned.

This can be solved very simply by ensuring the connection of new assets happens first before old assets are disconnected. In this case the newly minted ERC20 tokens can simply be handed from the connector to the disconnector directly without ever touching the secondary market.

The key here is to ensure that the connector and disconnector can coordinate the cycling before the next certification audit.

The primary risk is that the minting and burning will not be complete before the next audit, forcing the system into an uncertifiable state until all the previous cycle's NFTs are disconnected.

Wind down

It is not required that the custodial assets are held "forever". It is entirely possible that the custodian may only mint and manage offchain and onchain assets for a specific period of time, a season, year, decade etc.

For example, barrels of whiskey mature over the course of 8-12 years typically. The custodian may hold the barrels in a bonded warehouse until maturation but fully intends to sell 100% of all barrels at a specified maturation date to an offchain buyer (for a profit that more than covers the storage costs over the prior decade).

This presents a problem for the fungible tokens on the secondary market. The custodian wants to distribute profits by buying tokens back at, for example, 2x their original sale cost. Secondary markets for crypto assets are typically powered by price curves rather than order book style where the buyer/seller can dictate a specific price.

The custodian needs to establish a primary market for the fungible tokens where the price per token is:

- Fixed according to the final sale price of the offchain assets, e.g. 2x mint cost
- Respected so that speculators cannot manipulate the price by pumping and dumping liquidity on an AMM style DEX
- Will be permanent and always available to FT token holders even if they want to sell into the offer several years after the offchain sale has been finalised by the custodian, without further effort/permission on behalf of the custodian.

In this case the Rain DEX can be used exactly as in the case of total asset wipeout, but the funds for the order are backed by the total revenue of the offchain sale (minus the custodian's cut) rather than a fractional insurance payout. The order can be placed by a smart contract that itself has no logic or ability to remove the order, this means the end-users are fully protected once the revenue funds are deposited onchain.

The mechanics are exactly the same as the insurance recovery:

Price per token = total revenue / total tokens in circulation

The difference is that here we expect the price per token to be greater than the cost the end-users paid for the tokens when they were minted (profit!) whereas in the insurance case we expect the price per token to be less than or equal to the mint cost.

The custodian after making the offchain sale can immediately mint new tokens for a new batch of replacement barrels to mature in the same warehouse space. These new custodial tokens are a completely new contract, with a new (or identical) set of users and contracts for all the management roles, and can be put up for sale in a standard Rain sale. The end users holding the old tokens can immediately sell their old tokens into the DEX order, then roll as many or as few funds from their sale into buying new tokens from the new contract or just exit (to be replaced by new users hopefully).

Buying / selling of the ERC20's by the ERC1155 holders should only ever happen to maintain the peg or meet audit requirements in case of an NFT deficit. A simple wind down mechanism would be what we discussed with a vending machine that takes 20 and gives USDC at a fixed rate, and the LLC dumps USDC = total 20 supply * price into the vending machine after which the ERC20 tokens are trapped in the vending machine, so the system will never again be eligible to pass any further audits.

Step	Detail	Outcome
Time period		
Removing ERC20s from circulation	Buyback Fair value distribution Agreed value distribution	
ERC1155 planning		
ERC20 planning		

Scenarios

Scenario	Remediation
Rogue admin allows excess minting of ERC20s	
Tsunami damages large % of folio	
LLC cycles many underlying assets without spare capital to cover erc20 buyback	
Auditor incorrectly freezes system	
Auditor mistakenly values ERC1155 incorrectly	
Users challenge authenticity of underlying assets	
Country shuts down ERC20 trading	
Custodian can’t meet obligations for fixed or variable income products	
Russian oligrach buys ERC20	

Questions

Should we have a single, industry token, or ERC20s for different producers?

Different producers have different ERC20s. There isn't a clear reason where we try to make 20s from different organisations equivalent whether its gold or cannabis or anything else because the "thing" might be fungible (gold bars) but the counterparty risk that we're trusting/auditing (vaults/growers) is not equivalent.

How we should treat people that become blocked due to being removed from a tier?

They hold assets. We could have a role that can seize assets from users that are NOT meeting the minimum tier requirements, for example we know that USDC can freeze onchain assets... but we have no idea what that means for $ in their bank account because there's no onchain record of the bank $ only the USDC token. We have to assume that at some point in some situations they can mint new USDC rather than indefinitely having $ set aside in the bank against frozen funds. How that works is opaque, but for us it has to be represented and handled onchain in the contracts, there's just no way to burn the NFTs without some kind of clawback of the FTs.

Underlying asset is illiquid not liquid

Take the gold case, to arb the peg:

- If token trades below peg then NFT owners can buy token cheaper than spot price of physical asset, so can burn X NFT ounces for $Y and then sell X physical ounces for $Y + $Z
- If token trades above peg then NFT minters can buy X physical ounces for $Y and then mint and sell X NFT ounces for $Y + $Z

So there's a profitable mint/burn in each direction, just like arbitraging USDT by depositing and withdrawing $ from a bank account. If a token for a single asset trades above peg, there's nowhere to get additional stock of the same asset.

How to handle illegal money?

Needs to look and feel like it is anything but a vehicle for dubious money to be flowing around the system. This means we have the regulatory side nailed down as much as possible. It will be important that we have something that allows us to invest money into the portfolio and build on the portfolio over time because of the investment needed in the assets plus there are additional assets we could acquire for similarly attractive returns. We also want to bring returns to the island. Playing around with structure, bulk of return will come from capital appreciation.

How to KYC wallets?

SFT & Rain can extend to KYC providers to validate wallet activity. SFT purchase or trade can be restricted based on KYC if custodian desires.
/// This contract does not attempt to solve for liquidity and trustworthiness,
/// it only seeks to provide baseline functionality that a competent custodian
/// will need to tackle the problem. The implementation provides:
/// - ReceiptVault base that allows a transparent onchain/offchain audit history
/// - Certifier role that allows for audits of offchain assets that can fail
/// - KYC/membership lists that can restrict who can hold/transfer assets
/// - Ability to comply with sanctions/regulators by confiscating assets
/// - ERC20 shares in the vault that can be traded minted/burned to track a peg
/// - ERC4626 compliant vault interface (inherited from ReceiptVault)
/// - Fine grained standard Open Zeppelin access control for all system roles

What if the offchain market collapses?

If the offchain market for the asset collapses e.g. the offchain market for USD or Carbon Credits or Gold collapses then the custodian will not make money from arbitrage / maintaining peg and the system will collapse with it.

What if the offchain market is only emerging?

It's important to use FT minting to engage in price discovery. Flooding a nascent offchain market with assets (like ICO/IDO) does not allow enough time for a meaningful offchain market to emerge.

How do you maintain a peg (minting/burning selling/buying)?

Answered elsewhere

How do you deal with recoverable losses of custodial assets (buy 20 and burn)?

Needs answer

How do you deal with unrecoverable losses/wind-down (rain DEX buyback auction with remaining funds)?

Needs answer

It's tokenising physical assets... but we can maintain our own vernacular to stay consistent if it's helpful??

"Tokenising physical asset" is vague to me, because to me it implies that if i hold the token i somehow own the asset, that's not what is happening here.

One part is right? The NFT is ownership? Not unless we spin up some legal framework around it

The 20s are just fractionalizing the NFTs?

Fractionalizing and pooling and fungibilising. In a very abstract sense, the ERC20 represents ownership of the integrity of future audits, if it's ownership of anything. The assets cannot not be owned in a vault. Even during transfer from cage to cage, ownership is in place until it's in the cage when ownership simultaneous transfers...

The ERC1155 is just there to make our break the audit?

The thing is that trying to make an onchain token literally be and replace legal title/ownership of something is really problematic. USDT isn't legal ownership of USD. It's a claim for a USD and there exists some small group of sophisticated investors with business relationship with tether who can send/receive $ to mint/burn USDT. It’s not available for the general public and certainly not permissionlessly, you'll be doing at the very least some KYC.

It’s just like the $ used to be a claim on gold theoretically but i doubt the average person really had a way to take gold out of fort Knox and even if it is a claim/coupon that's still not actually ownership, it's just a thing that could be potentially traded for the real thing.

Like the old grain coupons, only as good as the army that protects the granary. The coupons with the same face value that were issued by the stronger army were worth more in trade.

What does ownership mean here?

"ownership" means two fundamentally different and incompatible things in tradfi and crypto.

- ownership in tradfi => the local nation state gives me exclusive permission to X, through violence to enforce exclusivity
- ownership in crypto => i give myself permission to X, through exclusive knowledge of a secret

Simply minting a token and saying "now you own X" is super ambiguous and doesn't really work except in very limited cases like Realt where they've discovered some specific local legal structures like a "series LLC" allow it in a limited capacity.

How does arbitrage work with Semi-Fungible tokens?

All that matters to crypto ppl is that there's a believable arbitrage model that maintains a price peg. Tether works because of arbitrage, not because an individual can redeem their USDT coupons for $ in a personal bank account or, in other words, the ppl who can own and deposit/withdraw gold in the vault can profitably do so by buying/selling the gold token onchain and minting/burning it. If it is trading above peg they can go buy physical gold, issue tokens and sell them for more than the gold cost. If it trades below peg they can buy back tokens and burn NFTs and sell the underlying gold for profit.

How do you minimise issues between audits?

Enforcing the serial numbers on the NFT can minimise issues between audits, e.g. good luck getting all the exact same gold bars undetected if you sell them then try to buy back again later just before audit. Ownership happens between lawyers and on pieces of paper, not onchain.

How does the ERC20 and ERC1155 interact?

Their harvest token would be the 20. They want their HRVT to be "backed" by one pound of cannabis. An NFT can mint fractions of an ERC20, we just need to decide one thing about the NFT that determines the amount of FT literally, "what is fungible about these plants?"

How does the audit work?

Technically the SFT system uses the blockchain in a way we can scrape the blockchain logs in a subgraph and hand a report to an auditor that they can review. Then they say yes/no and for how long to the whole thing in bulk and sign off on it.

Does the NFT represent ownership?

We are not trying to make a statement regarding ownership, e.g. "this NFT gives you ownership of a plant" because "ownership" isn't even a consistent concept legally across different jurisdictions globally.

The main thing that makes these use cases work is that all the NFTs are for something that has some fungible property.

For gold bars it is their pure gold equivalent weight. For plants it is their weight. If we did barrels of whiskey it would be their pure alcohol equivalent (which goes down each year as some evaporates in the barrel).

The NFT or ERC20 do not represent ownership, they represent "something that can be audited" and then on top of that we can layer things like "revenue/profit share"

If you own shares in a company that are worth as much as a table, that doesn't mean you actually own a table and can go into the office and take home a table just because you decide to burn a share.

How does this vary across industry?

Gold bars are consistent -- physically (within certain industry acceptable variance) and from producer to producer. With cannabis, each plant is different and uncontrollable and each producer will be different.

If there's nothing about the produce that can be considered fungible then you can't issue fungible tokens.

Are we creating industry standards?

Different producers have different 20s. We are not imagining a setup where we try to make 20s from different organisations equivalent whether its gold or cannabis or anything else because the "thing" might be fungible (gold bars) but the counterparty risk that we're trusting/auditing (vaults/growers) is not equivalent.

"what happens when i cycle revenue from one crop directly into a new crop?"

"what happens when a plant dies or underperforms?"

"what happens when i want to distribute profit rather than reinvesting into new plants?"

What if there is not yet an industry standard common property?

In the cannabis ecosystem, we'd expect the common property to be THC as that's the most low level chemical. Like pure alcohol content, it's the thing that ends up being equal. Put it in the context of gold, it's the purity at a certain weight -- as prescribed by the LBMA (industry standard). So cannabis would be THC level at a certain weight -- but no industry standard so we'll have to establish that standard.

How might this work for the agricultural cycle?

When they mint a new plant they have a forecast on what they plan to extract from it, and i'm sure that at the end of the process they very carefully measure everything during extraction, cannabis is highly regulated after all, plants can't just "go missing". What i don't know is if/when/how it is monitored between those two points in time.

Can an ERC20 e.g. HRVT can function like the gold ERC20 token (Unum) where it serves as a means or trade between businesses?

In theory yes, in practise we'll probably need it to be relatively long-lived if yes which if we have "like for like" NFT mint/burn might work.

How would a "like for like" work?

You could burn the old NFT when you mint a new one, and gain/lose the difference in ERC20

So when you burn the NFT the corresponding erc20 is also burned?

Say you had a 2 ounce gold bar, you could burn it to mint a 1 ounce gold bar if you also burned 1 ounce of 20, the difference would need to burn/mint. This would allow you to rotate through crop cycles without recalling all the outstanding 20 first, also if you had a 1 ounce gold bar you could burn it to mint a 2 ounce bar and you'd mint 1 ounce of 20.

Isn't the NFT linked to the corresponding 20s?

No, not at all. There is a shared contract but within a contract all the 20s are the same.

How does minting and burning work?

Ok I understand this math here. Could you just burn 1oz of gold without taking subsequent actions? If you burn 1 oz gold NFT you also must burn 1 oz gold FT. Ok that's what I was trying to get at. yeah so it is linked in that the math has to add up.

How do you burn the FT?

The smart contract handles that, you just need to have enough balance in your wallet when you call the function

Ok so the grower would need to have the requisite FTs in his wallet already or acquire them?

Yes, that's why i'm saying the grower will get extorted by their users if they have to recall all outstanding 20's to make the system work. But if the grower can burn old NFTs by issuing new equivalent NFTs then the 20s can stay in the hands of the end-users.

Got it. So the grower is more like recycling the NFTs, which makes sense since a farm only has a certain fixed capacity. This could also mitigate growers scamming by minting plants they don't really have.

Recycling NFTs is a good way to look at it, it's not title on the blockchain though, it's more like the tether model where the custodian can arbitrage the token. The token tracks the asset price due to arbitrage not title. The problem with title is that it doesn't really scale globally and it's not really clear how enforceable it is but arbitrage always works if there's a market.

Can this become a ponzi?

Could be ponzi'd as you had outlined earlier? Ah i mean offchain market. Tether works because there's an offchain market for the $ and "cash equivalent" assets that they hold so if the tether token goes above or below the value of those assets they can go and dispose or acquire more of those assets offchain buy buying/selling the token. so say the FT for the cannabis crashed massively, it would actually be profitable for the grower to buy back the token, burn the NFT and then sell the plant on offchain markets and if it moons they can mint more plants and sell them more onchain than they can offchain. It's the offchain/onchain arbitrage that gives buyers of the FT price assurance, not direct "ownership" of the asset.

I don't think they're financially savvy enough to do all of that background stuff to make it "stable".

We can help them by setting up long lived orders on the order book that sit either side of where the cannabis price "should be" and if the price completely smashes through that they can withdraw from the orderbook and go do something offchain then come back.

Generally what happens is that the issuer doesn't have to do all the work, they are the buyer/seller of last resort when things get largely out of whack, and then users trade between themselves to front run that event.

So only the ones who are bridging this onchain/offchain world can benefit "front run"? Can't insiders rig the situation?

The custodians are the ones that arbitrage the onchain/offchain which is why the audit trail is so important because partially collateralised arbitrage based systems collapse when they get a "bank run", but fully collateralised arbitrage can profit from stabilising the price all the way to $0. That's why we freeze the system when the audit fails, because freezing tokens prevents the custodians from doing the onchain/offchain arbitrage but assuming all the assets are there according to audits, then we _want_ the custodians to profit from arbitrage because the profitable trade in both directions brings the FT price back to "peg".

The ppl minting/burning tether to maintain that peg are playing this game on the order of billions of $ it's also why i was saying earlier that someone doing a gold FT doesn't necessarily need fees because they can make money arbing their own peg, just buying and selling the FT every time it goes above/below the spot price. The more usage and distribution their token has, the bigger the arbs they can do, so low/zero fees can be more than made up for in larger arb profits.

Why can't we be the custodians then?

We can be if we want to handle the physical assets and interact with offchain markets for effective arbitrage. Literally anyone with some asset that can be tracked with NFTs and has some offchain market FT value, that can be readily bought/sold, can be a custodian and mint it, as long as they can get someone to audit their stock and then if/when there are many of these contracts there's a layer of arbitrage between these tokens that can also be facilitated onchain to keep the token prices in line with each other across contracts. So then if liquidity leaves one token it can be "topped up" from another similar token.

This is also why the biggest risk to the system is someone getting private keys that can mint, because they can fraudulently mint infinite FT and dump them, basically stealing from and corrupting the whole system - so that's why i was suggesting minter-DAO for maximum security. So if we held tokens in the minter-DAO then we'd be participating in the custodial minting process without actually being the vault/farm/reit/etc. Ourselves.

Also the DAO can vote on deploying the orderbook price algorithms so someone could propose a fixed fee and someone could propose an auction and the dao could choose which one to deploy.

Yes that will make it "less" corruptible not "uncorruptible" buy as close as possible with power residing in the dao holders. Right, the fully decentralised option is the non-custodial contracts we already have, but it's only suitable for onchain assets. For offchain assets we have the custodial contracts, and they are centralisation-agnostic. Everything ranging from fully DAO-operated through to a single address minting and "auditing" everything themselves.

So the other thing about the standard DAO governance contracts is that they have a time lock/ delay on them so _in theory_ if the DAO voted to fraudulently mint say a quadrillion tokens, then that proposal sits on the public blockchain for say, 48 hours before it can be executed. So then anyone who is paying attention can pre-dump their tokens before the DAO can and there's a disincentive for the DAO to be fraudulent because they will crash the token price before they can execute their trade. Maybe it's a big assumption that ppl are paying attention, but this is the mechanism.

Does the SFT system apply to…?

The EV chargers generate credits every time a car is charged and once it hits 1 ton of CO2 prevented, one credit is earned...And this is perpetual for the life of the machine. And the CO2 calculation model has to be certified before the credits can be earned and trades/sold.

How would that fit our existing model?Perpetually generating credits means we need to keep minting NFTs?

Yeah if they want, no reason they can't. That means FTs too then… And they can issue the tokens to finance each machine?

So basically they have a warchest of carbon credits and $. They bootstrap their FT by settings aside some credits to mint NFTs. They sell the FT, the FT trades speculatively and they have more credits coming in from their EV periodically then they can look at their FT price on the market, and the CC price on established markets at that time if the FT price is higher, they set aside some CC and mint more FT and if it's lower they sell some CC and buy back an equal amount of FT. They either make the same amount they would selling on existing CC market (FT is exactly at peg) or they make a profit by arbing their FT.

So the CC are never sold into the market? Held as NFT and to arb against the FT?

If the FT is e.g. 0.9 CC they sell the CC into the existing CC markets for 1 then buy their FT for 0.9 and in doing so unlock 1 previously set aside CC and pocket 0.1 $. Some amount of CC is set aside when you mint the NFT, to collateralize the peg, every time the peg breaks downwards they can unlock it so it's like "we're setting aside this at 1 and will free it up any time the FT trades below 1".

Would it be systematic that when a CC is sold, the NFT and FT need to be rebalanced/recalibrated?

Only if the CC sold is to be taken from the set aside stock, they're free to do whatever they want with their CC that was never minted against.

Here's some WIP screens on the audit history, might make it clearer.

So they'd have asset IDs that represent each time they set aside a batch of CC, it's actually quite convenient if this is certified in batches, because they can treat each batch as an NFT.

Each certificate has a serial number.

So they bootstrap some liquidity into the FT system with the first few certificates then they just arb from there. Every time a new certificate comes in they have a very simple decision tree.

Would there be a component where the FT can be issued to acquire the machines?

If FT >= CC mint, else sell CC+burn

The machines are the CC generating asset

Seems like a rabbit hole trying to tokenise them vs. just putting FT up for the CC because if we have other CC producing clients all of a sudden we have an ecosystem of FTs, for example. I think there's a lot of power in just honing in on the most fungible aspect of the market and leaving everything else e.g. as soon as we started getting cute with gold in the ground on the mining thing, it derailed the convo a lot imo vs just saying "look, you either make the same amount of money or more..."

If you're in the situation that there's a peg you can arb, and a reason for demand to exist on your token that's a mega priviledged position to print money. The reason for token demand can be as simple as "retail doesn't have direct access to the CC market that the EV company does".

How might a marketplace work?

I think it's really easy to imagine for us maintaining an open marketplace built on the rain orderbook themed by asset class. People can place orders defined in terms of oracle prices for the assets like "buy/sell +/- X% from the CC price oracle", bots will just maintain the peg, any time someone wants to know where an asset comes from they just click the audit history and it's all there right down to the certification batch from the EV machine].

Each CC certificate they upload is an NFT, in the case of g they can't withdraw without it, in the case of SFT the tokens all freeze if the audit fails.

So it's 1:1 NFT to FT? Yes but the key thing isn't the upload of the certificate, it's them setting aside the CC that were certified and promising not to "double spend" them on the offchain market.

How can we assure this can't/won't happen?

The audits, that's what is being audited.

Automated audits possible? Or has to be manual for now -- human error, collusion... just thinking of the worst case

It doesn't really matter because ultimately the nature of the audit feeds into the trustworthyness of the token. People choose for themselves what they are willing to trust and it's not our place to say.

A true capitalistic and democratic market

Plenty of room for custodians to differentiate themselves within a commoditized space

What are we doing again?

What we're trying to do specifically is create aribtrage based fully collateralised peg tokens with audit trails.

Why EVM?

Liquidity is super important. How do you get liquidity on a network separate to the evm chains?

Would there ever be point where it's beneficial to run an EVM node? And the side chains we're using?

The subgraph pulls data from both evm nodes and also ipfs and combines them into the final audit report. We don't have to be validating, just keeping our own copy of the data to read from.

How do we enforce producers to perform audits?

If they sell their offchain CCs... the only process we have now is freeze them, right? And their tokens would be killed in our marketplace. That seems extreme if it's just human error??

They can unfreeze it when they pass audit.If a producer is fraudulent about their audits then we have a copy of all their audit transparency docs on IPFS so someone can take them to court.

I could ask similar questions like, "how do we enforce that governments don't change CC policy?"

Glossary

Introduction to Blockchain

Blockchain

A digital ledger where data is recorded in a chronological order. In Bitcoin's case, it is a decentralized, public ledger which contains transactional information. Users can verify that transactions have occurred simply by looking at the data that is publicized on the Bitcoin network. In a blockchain, the next piece of information that will be added is always linked to a previous, already confirmed information of the blockchain through the use of a hash which describes the past content. With the hash, every block of information in a blockchain becomes referenced with one another, and cannot be easily swapped out, thereby qualifying as an immutable ledger.

Smart contracts

Smart contracts are a relatively new concept due to the impossibility of a decentralized and unsupervised self executing contract prior to the creation of public blockchains. Unlike traditional contracts that relies on its participant's good faith to act on or enforced by a witness or notary, Smart contracts will execute its predetermined function as soon as its contract conditions are met. Just as cryptocurrencies made counter-party risk obsolete, smart contract removes the risk of contract defaults because it will execute autonomously and transparently.

Block

In the context of blockchain, block refers to the collection of transactional data or information that are bundled together in a predetermined size. Information within a block gets added to the blockchain and becomes part of a blockchain permanently once the data is verified through pre-determined rules/protocols.

Decentralized

Describes a system where there are no centralized points of failure (eg. a pillar that holds an entire structure up), or an organization that has no central authority figure. Bitcoin is an example of a decentralized system.

Distributed Ledger

Ledgers whose data is stored and synced across a network of nodes. A distributed ledger is not limited to cryptocurrency (transactional data) and can store many other kinds of data. It can also be set up to be permission and private.

Open Source

Open-source software is a type of software released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose. It is also a philosophy, with participants believing in the free and open sharing of information in pursuit of the greater common good.

Immutable

A property characterized by inability to be changed and stays unchanged over time.

DAO

A decentralized autonomous organization (DAO) is an emerging form of legal structure. With no central governing body, every member within a DAO typically shares a common goal and attempt to act in the best interest of the entity. Popularized through cryptocurrency enthusiasts and blockchain technology, DAOs are used to make decisions in a bottoms-up management approach.

Tokens & token standards

Immutable

Due to decentralization, security, immutability, Blockchain is considered to be the perfect technology for managing all types of digital assets. But with such interchangeable tokens, this would not be possible. Such tokens work fine for cryptocurrencies, and in fact, fungibility is the fundamental feature of any currency. Such tokens are built in such a way that each fraction of a token is equivalent to the next. For instance, Bitcoin, the most popular cryptocurrency, is fungible, which means one Bitcoin is equal to one Bitcoin, and it's equal to all other Bitcoins. Such tokens are assumed to be interchangeable and divisible too. In simpler words, these are types of cryptographic tokens that are basically identical or uniform and can be interchanged with other fungible tokens of the same type without any issues. Such tokens relate to the things we use every day, and it applies to real-world well as digital assets.

Non-fungible tokens (NFTs)

Non-fungible tokens are special tokens that represent unique, collectible items. They are unique in the sense that they cannot be split or exactly changed for other non-fungible tokens of the same type. You can consider NFTs as tokens with no fungibility that offer a variety of unique opportunities for using blockchain technology. Crypto Kitties is the most popular example of non-fungible, collectible tokens. Every CryptoKitty is unique, and no two CryptoKitties are the same; these are impracticable to break a CryptoKitty into smaller pieces, trade them, and reassemble them to create an equally valuable CryptoKitty, unlike fungible assets like Bitcoin.

Differences between fungible and non-fungible tokens

Fungible are Interchangeable As we already mentioned, such tokens are interchangeable and can be exchanged with any other token of the equivalent kind. Fiat currencies are fungible. For example, $50 notes are interchangeable with other $50 notes. Similarly, one Bitcoin value can be exchanged with another Bitcoin, which makes no difference for holders.

Non-Fungible are Non-Interchangeable Unlike Fungible tokens, such tokens are non-interchangeable as they cannot be replaced with the non-fungible token of the same type.

Fungible Tokens are Divisible These tokens can be divisible into smaller units, and one can get any number of units, and it does not matter to holders as long as the value remains the same.

Non-Fungible Tokens are Non-Divisible These tokens cannot be divided in any sense.

Fungible Tokens are Uniform All tokens of each type are identical in specification, and each token is identical to each other.

Non-Fungible Tokens are Unique Each token is different from all other tokens of the same type.

ERC20

ERC-20 is the technical standard for fungible tokens created using the Ethereum blockchain. A fungible token is one that is interchangeable with another token—whereas the well-known non-fungible tokens (NFTs) are not interchangeable. ERC-20 allows different smart-contract enabled tokens a way to be exchanged. Tokens, in this regard, are a representation of an asset, right, ownership, access, cryptocurrency, or anything else that is not unique in and of itself but can be transferred. The standard allows tokens representing one of these factors—along with smart contracts—to be exchanged for a token that represents another. Smart contracts are conditions written into the coding that execute different aspects of a transaction between parties.

https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

ERC1155

ERC-1155 token standard allows each token ID to represent both non-fungible (NFTs) and fungible tokens which may have their metadata, token supply and other attributes. It is used to promote efficiency in batch token transfers, and it allows many types of NFTs to be created with a single contract.

https://www.coingecko.com/en/glossary/erc-1155

Burned Tokens

Tokens which have been sent to addresses whose private key are not known, effectively becoming unusable. Example burn addresses include 1BitcoinEaterAddressDontSendf59kuE on Bitcoin or 0x0000000000000000000000000000000000000000 on Ethereum.

Infrastructure systems

IPFS

IPFS is a distributed system for storing and accessing files, websites, applications, and data. IPFS makes it possible to download a file from many locations that aren't managed by one organization.

Supports a resilient internet. If someone attacks Wikipedia's web servers or an engineer at Wikipedia makes a big mistake that causes their servers to catch fire, you can still get the same webpages from somewhere else.

Makes it harder to censor content. Because files on IPFS can come from many places, it's harder for anyone (whether they're states, corporations, or someone else) to block things. We hope IPFS can help provide ways to circumvent actions like these when they happen.

Can speed up the web when you're far away or disconnected. If you can retrieve a file from someone nearby instead of hundreds or thousands of miles away, you can often get it faster. This is especially valuable if your community is networked locally but doesn't have a good connection to the wider internet. (Well-funded organizations with technical expertise do this today by using multiple data centers or CDNs — content distribution networks That last point is actually where IPFS gets its full name: the **InterPlanetary File System**. We're striving to build a system that works across places as disconnected or as far apart as planets. While that's an idealistic goal, it keeps us working and thinking hard, and almost everything we create in pursuit of that goal is also useful here at home. https://docs.ipfs.tech/concepts/what-is-ipfs/

In a global namespace linking all computing devices, IPFS employs content-addressing to uniquely identify each file. Rather than relying on a single server like BitTorrent, IPFS is based on a decentralized system of user-operators who each hold a fraction of the overall data, resulting in a robust file storage and sharing system. Using a distributed hash table (DHT), any user in the network can serve a file by its content address, and other peers in the network can find and request that content from any node that has it.

Subgraph

What is The Graph? Most applications on the Web do not exist in a vacuum and use data, interfaces and features from other sources, sites and apps. Same goes for the Web3, but in addition to the blockchain interoperability problem there is also pervasiveness of centralized services, legacy of the Web2.0.

The Graph offers an answer to both of these problems: instead of having to set up a centralized server or database, its users can plug into open APIs called subgraphs to query data. The Graph's solution, called subgraphs, is an open API in The Graph ecosystem that can automatically perform processes like a normal API. For instance, a Uniswap subgraph can be used to query trade volumes and is integratable in applications, such as wallets.

How Does It Work?

The Graph is powered by an open data layer on Ethereum. To extract and read the blockchain data, subgraphs abstract interacting with Ethereum's JSON-RPC API. Pulling data from the blockchain directly and not from an in-house indexing database significantly increases the application loading speed and eliminates a single point of failure. All subgraphs are open-source and written in GraphQL, a common language for Web2.0 apps. It makes the subgraphs open, accessible and easy to work with.

LP

To best understand liquidity providers, it helps to have a strong grasp on how liquidity pools function. The purpose of a Liquidity Pool is to allow the trade of crypto assets on a decentralized exchange market. To set up the decentralized crypto exchange market the first liquidity provider will make an initial stake with their own crypto assets. This stake will be set at an equal rate between the two exchanging tokens. The purpose of this equal exchange rate is to prevent arbitrage.

This initial stake into the pool will earn the provider a fee of 0.3% in the form of a 'provider token' for each trade conducted on the platform based upon the strength of the liquidity pool. This incentivizes further stakeholders to invest into the pool, to gain a portion of the 0.3% fee. As more stakeholders grow the pool, more trades can be conducted of its strength. Thus creating a positive 'feedback loop' of users and providers.

After each successful cryptocurrency token exchange on the platform, a price adjustment will take place. Attempting to best represent the ongoing value of the tokens. This is conducted by a deterministic algorithm called an Automated Market Maker or 'AMM.' Different exchange platforms with different Liqiuidty Pools and Providers use different AMMs to adjust value and provide incentives for stakeholders. Some examples of these different AMMs are Curve, Uniswap, and Balancer.

DEX

A decentralized exchange (or DEX) is a peer-to-peer marketplace where transactions occur directly between crypto traders. DEXs fulfill one of crypto's core possibilities: fostering financial transactions that aren't officiated by banks, brokers, or any other intermediary. Many popular DEXs, like Uniswap and Sushiwap, run on the Ethereum blockchain.

Block Explorer

Block explorer refers to application or websites which display information and status of transactions of a given public blockchain network. They usually do this by running their own nodes (they become part of the network), and then index information that may be relevant to the users. This opens up access to the data of a blockchain and allows regular users to look at progress of transactions or verify that a transaction has occurred without needing to run a node themselves.

Bots

Refers to software or programmes that automatically trade based on preset behaviors (eg. buy @ $100, sell at $102, and then repeat). Bots have the advantage of being extremely quick and can react almost instantaneously.

Frontrun

In traditional finance, frontrunning or tailgating is a practice where traders or brokers execute a trade before a prior large order is executed. The said trader or broker will then sell their trades higher to the large order, owing to the order's slippage tolerance. This is highly illegal and unethical in the traditional finance. In the cryptocurrency context, frontrunning works the same but in DEX's where orders made are broadcasted to the blockchain for all to see, a frontrunner will attempt to listen to the blockchain to pick up suitable orders to frontrun by orders on the market and placing enough fees to have the transaction mined faster than the target's orders.

Gas

A unit of measurement of the computational effort in conducting transactions or smart contracts on Ethereum blockchain. It is equivalent to 'fuel' - how much fuel (gas) does it take to conduct the requested transaction on Ethereum network.

Gas Price

A term refers to the amount of price user is willing to pay for a transaction on Ethereum blockchain.Gas price is denominated in Gwei.

Buy/Sell Tax

It is possible to code a smart contract token to have an innate on-chain "tax" whenever someone wants to buy or sell the tokens. The way it works is that a percentage of the tokens being bought or sold is transferred to a preset address - essentially "taxing" the buyer and seller and thus discourage wash trading. However, this code function can be abused where the tax rate is unreasonable, making it a Honeypot.

Wallet

Analogous to an online bank account or an email client software. Cryptocurrency wallets is an interface that lets users store, send and receive cryptocurrencies. There are 3 popular categories of wallets, "Custodial" - where private key security (and by proxy, the cryptocurrencies themselves) is handled by a third party, "Hot" - wallets that is meant for frequent use, and "Cold" - wallets that is meant for secure and long term storage.

Wallet Address

Wallet Addresses, also plainly referred to as Addresses, is the string of alphanumeric where your cryptocurrencies are stored. An example of a wallet address on the Bitcoin Protocol is "3KJmVaMzKRxKbKTMQmfnKzecpsExs8tbkk" (CoinGecko's Bitcoin Donation address). Where the beginning "3" signifies that the addresses uses P2SH encoding, which is cheaper that sending to "1" addresses whilst still support "bc" addresses.

Whitelist

In the context of the cryptocurrency industry, a trader will be placed in a whitelist after completing some form of KYC checks, which will allow the trader early access to a token sale event. Typically, traders wants to be placed in a whitelist as that puts them in a potential advantage as they can purchase the token prior to a public token sale at which the coin will be sold at a higher price to the public.

Total Supply

The total number of coins or tokens that are in existence, including those circulating in the public market and those that are locked or reserved.

Order Book

An electronic list of all buy and sell orders in an exchange.

Oracles

In the context of crypto, oracles refers to services which verify real-world and provide data to blockchains/smart contracts. Oracles are needed for decentralized programmes to function trustlessly as using data from a centralized source would cause a programme to have a weak spot that can be easily manipulated.

Option

It is a financial instrument that refers to a contract that offers the buyer the right to buy or sell an underlying asset at a specified price and time.

Protocol

The set of rules that define interactions on a network, usually involving consensus, transaction validation, and network participation on a blockchain.

Infrastructure systems 2

Custody & custodial assets

In the context of cryptocurrency, a "custodial" asset means an asset is placed under the care of a third party. This is similar to how banks have custody over their customer's funds. A Custodial Wallet refers to a wallet whose private key management falls under the care of a company. Examples of Custodial wallets include Coinbase, Nexo and other wallets where users do not have access to their private keys.

Asset custodians

Asset custodianship has traditionally been associated with capital market financial institutions that are responsible for the safeguarding of investors' assets as well as providing other services like trade settlement, exchange, clearing, and corporate action execution. These custodians are temporarily entrusted with assets and are expected to minimise the risk of fraud, theft or loss to those assets. In line with accelerating investment into the crypto space, the demand for digital asset custodianship has grown tremendously. However, this has proven to be a space that is vastly different from traditional asset custodianship, hence the plethora of new players and technologies that are emerging all the time.

Like their traditional capital market counterparts, digital asset custodians are also responsible for the safekeeping of a client's crypto assets, however the difference is that these custodians do not hold the asset itself but are responsible for the custody of the keys to these assets. Through safe key management, digital assets are cryptographically secured and the custodian, therefore, ensures that the asset cannot be accessed by any other party. For a family office to have transactional access to an asset, both a public and private key needs to be used.

Impermanent Loss

Impermanent loss may occur when you provide liquidity to the AMMs. Impermanent loss is similar to measuring your opportunity cost of holding the token within the pools versus holding them in your wallet. Note: the loss is not realized until you remove your tokens from the liquidity pool. The higher the divergence between the value of holding your tokens in the pool and wallet, the higher is the impermanent loss.

Liquidity

It often refers to market activity in trading the cryptocurrencies. It signifies the speed of the buy and sell of the traded assets. The higher the liquidity, the less affected is the trading activity when price changes.

Market Maker

A market maker places prices that differ from the current market price for the orders. A market maker would typically want to sell at a higher price, and purchase at a lower price.

Market capitalization (market cap)

Traditionally, it refers to the monetary market value of a company based on outstanding shares of stock. Market capitalization is used to show the size of the company. in Crypto, market cap is measured by multiplication of the circulating supply of tokens or currency and its current price.

Node

Within the blockchain network, the nodes are computers that connect to the network and have an updated copy of the blockchain. Together with the miners they are the guarantors that the network works properly. The nodes in Bitcoin are very important because they help the mission of keeping the network decentralized.

Non-custodial

It is a decentralized type-of-wallet, where the users owns its private keys. Having the private keys equals to you owning full control of your funds but the danger is if you lose your private keys, you will lose your funds forever.

Off-chain

It refers to transactions occuring outside the blockchain and executed instantly. There are a number of methods to do off-chain transactions, eg, two interested parties do a transfer agreement. Next, a third party faciliatetes the transaction by becoming the guarantor in it.

Circulating Supply

Circulating supply can be defined as the supply that is currently in the hands of the general public.In the case of fairly mined proof-of-work systems (eg. Bitcoin), the total supply is approximately equivalent to the circulating supply, as there are no token generation events which puts large amounts of tokens in the hands of a select few. On the contrary, initial coin offering (ICO) which have token generation events typically have a lower circulating supply vs. the total supply, such that: Circulating supply = Total Supply - Team tokens - Foundation tokens - Locked tokens.

Algorithm

Algorithm is a set of rules to follow to solve a problem or conduct a task. In computer or programming, an algorithm is needed for a computer to do its task accordingly. It is not a computer code and it needs to be converted to the language where the computer can understand.

Arbitrage

A practice of taking advantage of differences in price of the same commodity in two or more markets or exchanges. For example, cryptocurrency prices on Korean exchanges can be different from those on US exchanges. An arbitrage trader would be in both markets in order to buy in one and sell in another for profit.

Decentralized Autonomous Organization (DAO)

Open source and decentralized systems that do not require centralized operators or controllers. A decentralized autonomous organization can vote on various aspects of a system without the need of central controller. Members of a decentralized autonomous organization are typically made up of token holders whose voting strength are proportional to their holdings relative to the whole ecosystem.