A Crash-Course on Forward Contracts: Commentary on Urbit's Mayflower Proposal

~diblud-ricbet (Izaac Mammadov)

~2024.08.24 (Draft V1)

Abstract

The Urbit Foundation have recently proposed a new set of crypto-assets, whose tickers are yet to be decided, but under the project codename "Mayflower". Details are sparse and no whitepaper is out, but from the information that has been released, I will try my best to chime in from my speciality which is crypto-asset and derivatives trading. I come at it from the perspective of someone who has worked as a quant trader for one of the largest crypto market-makers in the world, and currently work as a quant trading volatility derivatives in trad-fi. Thus the topic bias is going to be towards Maths and Finance-theory, as opposed to the best way to pump this token to the moon. Comments, corrections, forks and complaints to this document are always very welcome at it's GitHub page accessible here.

Contents

1 Mayflower Proposal

1.1 Current State of Urbit Address Space

Currently, identity (and by extension, access) to Urbit is governed by an Ethereum smart-contract called "Azimuth".[1] As a short summary, there are 256 "galaxy" NFTs, each of which can issue 255 "star" NFTs. Galaxies and Stars can each issue 65,535 "planet" NFTs. This hierarchical sructure is currently central to Urbit. Galaxy-holders form one of the governance structures of Urbit (the "Galactic Senate"), and Star-holders have the right to provide imporant infrastructure duties in Urbit networking. Planets are currently the minimum level of status you need to functionally get-by as an end-user of Urbit. `~sorreg-namtyv` commonly states that the intention is for every "responsible adult on earth" to own a planet.[2] Currently, planets are available free-of-charge to anyone on a one-planet-per-person basis from companies RedHorizon and Tlon. Although in recent days, there are plans being floated to make planets less essential than they currently are.[3]

The Urbit Foundation has a significant portion of its balance sheet made up of these NFTs and has suffered greatly in the drop in price and liquidity of galaxies/stars. The goal of Mayflower is to increase demand, increase liquidity and reduce supply of the Urbit Azimuth space, without greatly disadvantaging or diluting current Azimuth NFT holders.

1.2 Mayflower Overview

This subsections below are liable to change rapidly as there are no concrete whitepapers yet. The Mayflower proposal, as best I understand it, is summarised below:

1. Remove the right of Star and Galaxy holders to freely issue their 65,535 planets. (Existing issued planets will be grandfathered in.)

2. Create a fungible token (henceforth, for lack of an agreed ticker, called `URB`) which can be traded in for an arbitrary planet NFT.

3. Provide a mechanism for Star and Galaxy holders to trade in their planet-issuing rights in exchange for a corresponding number of `URB` tokens with a time-locking mechanism.

For example, a star can "release" its 65,535 planets into the smart-contract, which provides the star with 65,535, varyingly time-locked `URB` tokens. The number of `URB` tokens is always equal to (or less than or equal to if you don't

[1] *Azimuth (Urbit ID)*. Urbit Foundation. URL: https://docs.urbit.org/courses/hoon-school/C-azimuth (visited on 24/08/2024).

[2] `~sorreg-namtyv`. *So maybe you have some Urbit questions...* 21st Aug. 2024. URL: https://threadreaderapp.com/thread/1826372024002130061.html (visited on 24/08/2024).

[3] `~tondes-sitrym`. *GroundWire 01*. 22nd Aug. 2024. URL: https://straylight.network/groundwire/groundwire-01 (visited on 24/08/2024).

count time-locked URB) the number of planets that the smart-contract has available to issue. Thus URB holders are always guaranteed the right to trade-in for a planet.

1.3 Timelocking Mechanism

The currently propsed time-lock mechanism, as I understand it, for URB tokens (again, very liable to rapid change) is that for a given number of planets that a Star or Galaxy relinquishes into the contract, they receive:

1. 5% of their URB tokens immediately,
2. 10% of their URB tokens in one-year,
3. 10% of their URB tokens in two-years,
4. 25% of their URB tokens in five-years,
5. 50% of their URB tokens in ten-years.

Thus after ten-years, they will cumulatively receive a number of URB tokens equal to the number of planets they relinquished. I'll take this opportunity to stress the importance in auditing and fuzz-testing the rounding calculations for the above percentages, as (more high-risk) crypto projects have lost millions in hacks due to specific input numbers leading to rounding-errors.

However, as opposed to a traditional time-lock mechanism, the proposal plans to create ancillary tokens that represent the right to receive a certain number of URB tokens at a specified future date. Thus instead of being stuck to having to wait the full time-period, there is an option to sell the right to receive future URB tokens and cash-out immediately.

1.4 Advantages of the Proposal

In terms of improving liquidity, it is absolutely clear that fungible tokens always win. With a fungible token, you can get listed on centralised/decentralised exchanges. On centralised exchanges, limit order books will form passive liquidity and on decentralised exchanges, AMMs can be funded by liquidity providers, also leading to liquidity. Achieving the same with NFTs is not impossible, but an absolute nightmare. An older token, called WSTR, aimed to achieve only this on its own by a simple wrapping/unwrapping mechanism of arbitrary stars. It didn't take off significantly and didn't get listed on any centralised exchanges.

Secondly, removing the right to freely issue planets, certainly reduces supply of planets somewhat. There is a question as to the scale and significance of the reduction in supply relative to number of to-be-grandfathered-in planets.

Thirdly, a new token launch is always a buzz-generating event. Combined with the rest of the events in recent days, it is very fair to say that the token will generate interest and excitement at least in the short-term.

2 Forward Contracts

2.1 Definition

Given these rights to a certain number of `URB` tokens in the future, will itself be tokenised/tradeable, it's imperative to properly understand them. Clearly, their value very strongly depends on the value of `URB`. That fact on its own make them a derivative (the scary D-word!).[4] Some people have referred to these derivatives as being "like zero-coupon bonds". That's true in the same way that pizzas are like pancakes. I think it's ~`sorreg-namtyv`'s extensive research and writing into monetary policy and duration transformation that makes him see everything as a bond. These rights are actually forward contracts. A forward contract "is an agreement to buy or sell an asset at a certain future time for a certain price."[5] In this case, from the perspective of the smart contract, it is an agreement to sell `URB` in a certain number of years, at the price of 0.

Granted, it is rare for forward contracts to have an exercise price/strike price of 0. Usually participants drawing up a forward contract aim to do so in a way that neither party is significantly advantaged over the other. In this case however, the smart contract trades a very disadvantageous forward contract in exchange for the planets relinquished. Or from the star/galaxy holder's perspective, they receive a very favourable forward contract in exchange for relinquishing their planets.

2.2 Pricing Derivatives in General

Forward contracts currently exist all throughout traditional finance, although very rarely in crypto. Forward contracts are incredibly similar to their much more famous cousin, futures contracts. So much so, some people use the terms interchangeably. However since the plans proposed are very clearly forward and not futures contracts, I will focus all discussion on solely forward contracts.

For any type of derivative that exists in traditional-finance, uncountably many 120-IQ-man-hours have been spent (or perhaps wasted) on figuring out what the correct price for them should be. The notion of "correct" price is quite nuanced, but here are two common notions of "correctness":

1. No-Arbitrage Pricing: You make the assumption that nobody would leave risk-free money on the table. If a set of prices leads to a risk-free profitable trade being possible, those prices are "incorrect". The risk-free profit is called an arbitrage.[6]

2. Rational Pricing: You assume that things which are roughly the same are worth roughly the same. Things that are exactly the same, should be worth exactly the same. There shouldn't be any super "easy-money" to

[4] John C. Hull. *Options, Futures, and Other Derivatives.* 2022 (11th edition), p. 23.
[5] Hull, see n. 4, p. 28.
[6] Hull, see n. 4, p. 126.

be made, even if it's not risk-free. Things should be worth what they've historically been worth.

In practice, prices in liquid traditional-finance derivatives will only break no-arbitrage rules (in other words, arbitrage only exists) for a maximum of a few milliseconds (because who doesn't want risk-free money). On the other hand, markets tend to stick to pricing assets rationally, but without an arbitrage, the price for assets can behave irrationally for any length of time.

2.3 Pricing Forwards

Under no-arbitrage assumptions, for an underlying that provides no income, the correct price of a long forward contract f is given by:

$$f = (F - K)\mathrm{e}^{-rT}, \tag{1}$$

where F is the exercise price that a forward contract, with same expiry, of 0 value (to the people going long or short) would have, K is the exercise price of the forward (in our case, 0), and e^{-rT} is a discounting term meant to represent that ten dollars in 10 years isn't worth as much as ten dollars now. Specifically, r is the continuously compounded risk-free interest rate that financial institutions can borrow/lend money at between each other with low/no-risk, and T is the time until expiry for the forward.[7]

Hull proves that this is the only possible no-arbitrage price with the following argument (where S_T is the price of the underlying asset at expiry) "To see why equation [1] is correct, we form a portfolio today consisting of (a) a forward contract to buy the underlying asset for K at a time T and (b) a forward contract to sell the asset for F at time T. The payoff from the portfolio at time T is $S_T - K$ from the first contract and $F - S_T$ from the second contract. The total payoff is $F - K$ and is known for certain today. The portfolio is therefore a risk-free investment and its value today is the payoff at time T discounted at the risk-free rate or $(F - K)\mathrm{e}^{-rT}$. The value of the forward contract to sell the asset for F is worth zero [by definition of F]. It follows that the value of a (long) forward contract to buy an asset for K at time T must be $(F - K)\mathrm{e}^{-rT}$."[8]

We can go further though. Again, under no-arbitrage assumptions, and assuming that the underling asset is an "investment asset", there is only one correct value for F:

$$F = S\mathrm{e}^{rT}, \tag{2}$$

where S is the current spot price of the underlying asset.[9] Combining these two, alongside $K = 0$, give us

$$f = S. \tag{3}$$

In other words, assuming no-arbitrage, and assuming the `URB` is an "investment asset", every single one of the forwards should have a price exactly equal

[7] Hull, see n. 4, p. 133.
[8] Hull, see n. 4, p. 133.
[9] Hull, see n. 4, p. 127.

to the spot URB price. This flies totally in the face of intuition. There's been a lot of talk about these assets, perhaps being able to reflect Urbit supporter's unique willingness to hold address-space long term, or having some kind of unique yield curve dynamics. Unfortunately at first glance, that seems to be totally at odds with the financial mathematics. There is one important nuance, and that is whether, for these range of forwards, does URB qualify as an "investment asset"?

2.4 What is an investment asset?

It's important to be absolutely clear here. If these forwards weren't for URB, and instead gave you the right to receive, say, a SPY ETF, or 1 million GBP, or a bar of gold, there would be no hesitation in how traditional-finance markets would price those forwards. The prices would satisfy Equation 3 with absolute precision. The forward price would equal the spot price, and have no time-dependence. It wouldn't matter whether the forwards were for 6-months, 1-year, or 5-years — the prices would be the same. There shouldn't be an intuition that some kind of time-locking automatically implies a discount over spot.

It is true that regardless of whether it's an investment asset or not, the following inequality is always true:

$$f \leq S. \tag{4}$$

[10] A time-locked asset is never going to be worth more than the non-time-locked asset. But again, that's a weak-inequality, not a strict one.

The "investment-asset" no-arbitrage argument depends on the fact that there are some number of people who are committed to holding the underlying (URB) for the duration of the forward. If those people exist and $f < S$, those people can automatically lock in a risk-free profit, by switching to holding the URB forward instead of URB itself — it makes no difference to them because they were planning to hold for the full duration anyway, and they just lock in the difference $S - f$ as pure profit.[11]

Assets are typically thought of as being investment assets, or not. For example: Gold is, Corn isn't. But in the case of URB, I think it's important to make some kind of time-scale distinction too. It seems very likely that they'll be enough people invested into URB on a one-year time frame such that under no-arbitrage assumptions, the one-year forward price must equal the spot price. But on a ten-year time-frame? Reply hazy, try again later.

2.5 Short Selling

There is also an alternative no-arbitrage argument for Equation 3 that doesn't rely on URB being an investment asset, but rather assumes that it can be short-sold freely and cheaply. What this requires is some kind of borrowing mechanism

[10] Hull, see n. 4, p. 143.
[11] Hull, see n. 4, p. 129.

for people to borrow URB tokens in a cheap way. Borrwing in crypto happens either on decentralised lending pools (like Aave), or formal lending contracts drawn up by institutions. An honourable mention also goes to perpetual futures contracts listed on centralised exchanges. While these don't give you an ability to "borrow" a token, they let you short-sell a token in effect, by shorting the perpetual and paying the funding payments as interest.

With this ability, and $f < S$, any entity can lock in a guaranteed profit by short-selling the token at a price S and buying the long-forward for a price f. This locks in a risk-free profit of $S - f$, and when the forward expires, you will receive the URB token which you can use to close up the short position. If the process of short-selling is free or negligibly cheap, then once again, Equation 3 must be true and the forward prices must equal spot.

2.6 Not investment asset, and no short selling

And so what then, if (as may be the case for the long-dated forwards) there aren't enough investors in URB for a given timeframe T to classify it as an investment asset, and short selling is either not possible or too expensive? Then all that can be said in terms of no-arbitrage pricing is the following:

$$S - (\text{Cost to short sell URB over } T) \leq f \leq S. \tag{5}$$

However, where the extent of the no-arbitrage arguments end, is where a more wishy-washy rationality argument begins. Imagine that five-year zero-strike URB forwards are trading at a 50% discount, while 0–4 year zero-strike forwards are all trading at par with spot. This may be the case for example if URB is an investment asset only out to a four-year time-frame. If I'm only interested in buying URB for one-year, buying the five-year forward (with the intention to sell it after a year), still feels incredibly lucrative to me. Why? Because over the one-year that I'm holding it for, the five-year URB forward will become a four-year URB forward. It will most likely move from the "not investment-asset" time-range to "investment-asset" time range, and as such the discount will go from 50% to 0. Again, no guarantees, this isn't a no-arbitrage argument, but a rationality one.

This is a crash-course on financial mathematics, not investment advice, and so I'm not going to enumerate all the different possibilities for the forward discounts and whether they are rational or how rational they are. But in general, the paragraph above is the style of how forward trading decisions are going to be made by sophisticated financial institutions.

Note nowhere in the calculations nor explanations did the predicted future price movements of URB enter in. Because the forward prices aren't any more a prediction of future prices than spot prices are. If I have a belief that over the next year, URB is going to pump 20% upwards, I can enter that trade, either by longing spot URB, by longing one-year URB forwards, by longing two-year URB forwards, or even longing six-month URB forwards and rolling them after six months for a further six months. The strategies will all result in

similar profits from the upwards move, but the only difference will be that when trading forwards, I'll be subject to forward discount dynamics described above (related to investment-asset / short-selling ability). Forwards don't some-how encapsulate some kind of extra information about long-term price-distribution that aren't already encapsulated in the spot price.

3 Practical Considerations and Issues

TBC

4 Advice to Current Address Space Holders

TBC

References

~sorreg-namtyv. *So maybe you have some Urbit questions...* 21st Aug. 2024. URL: https://threadreaderapp.com/thread/1826372024002130061.html (visited on 24/08/2024).

~tondes-sitrym. *GroundWire 01.* 22nd Aug. 2024. URL: https://straylight.network/groundwire/groundwire-01 (visited on 24/08/2024).

Azimuth (Urbit ID). Urbit Foundation. URL: https://docs.urbit.org/courses/hoon-school/C-azimuth (visited on 24/08/2024).

Hull, John C. *Options, Futures, and Other Derivatives.* 2022 (11th edition).