Stefan Loesch[1]
Nate Hindman[2]

Bancor Protocol v2.1

Economic and Quantitative Finance Analysis

1 stefan@topaze.blue
2 nate@bancor.network

DISCLAIMER

THIS ECONOMIC ANALYSIS IS NOT INVESTMENT ADVICE. THE BASIS OF ALL REASONING IS CLEARLY STATED OR IMPLIED AND IT IS UP TO THE READER TO ANALYSE WHETHER OR NOT TO AGREE WITH IT. NO DECISIONS SHOULD BE BASED ON THE CONTENT OF THIS PAPER WITHOUT INDEPENDENTLY ASSERTING AND VERIFYING THE FULL FACTS THAT LEAD TO THE DECISION.

WHILST CARE HAS BEEN TAKEN TO ENSURE THAT THIS PAPER IS ERROR-FREE THE READER SHOULD NOT RELY ON THIS. THE PAPER MAY CONTAIN ERRORS, FOR EXAMPLE IN THE ASSUMPTIONS OR IN THE REASONING OR IN THE PRESENTATION, OR IN ANY OTHER WAYS. NOTHING IN THIS PAPER SHOULD BE ASSUMED TO BE ERROR FREE OR RELIED UPON WITHOUT INDEPENDENT ANALYSIS.

THIS PAPER IS BASED ON THE AUTHORS' UNDERSTANDING OF THE BANCOR V2.1 MECHANISM AS IT HAS BEEN COMMUNICATED TO THEM. THE COMMUNICATION COULD HAVE BEEN ERRONEOUS, OR IT MAY HAVE BEEN MISUNDERSTOOD, OR THE CODE IMPLEMENTATION MAY DIFFER FROM WHAT IS DESCRIBED, OR THE DESCRIPTION MAY BE WRONG FOR ANY OTHER REASON. UNDER NO CIRCUMSTANCES SHOULD THIS PAPER BE INTERPRETED AS A SPECIFICATION DOCUMENT, AND NO NUMERICAL OR FORMULAIC CALCULATIONS OR EXAMPLES SHOULD BE RELIED UPON WITHOUT INDEPENDENT VERIFICATION.

THE AUTHORS OF THE DOCUMENT HAVE BEEN REMUNERATED FOR THE PRODUCTION OF THIS ANALYSIS.

Introduction

Bancor has proposed its v2.1 version of the Bancor protocol, and they have retained topaze.blue for an analysis of the economic and quantitative finance aspects of the protocol, the summary of which is described in this paper.

When performing the analysis, we have been very impressed by the senior team. As far as we know they are one of the longest serving teams in the space of Decentralized Finance ("DeFi") and Automated Market Makers ("AMMs"). We found that they have an extremely good intuitive understanding of how an AMM system behaves, and what the key pressure points are. When we were first starting to analyze the system there were a number of design choices that were not obvious from an outside-in view. However, they made a lot of sense once the senior team had explained them to us. What struck us in particular was that the senior team had an extremely sharp view on the *commercial* realities of the DeFi space, and that the system is first and foremost designed with those commercial realities in mind.

By now we are all used to unicorn ventures that are "two-sided marketplaces matching buyers and sellers", such as Uber and Lyft, AirBnB etc. Those are still the darlings of the Silicon Valley VCs. AMMs arguably push this one level higher: they are fundamentally two-sided marketplaces (matching trading customers and liquidity providers), but additionally they have to keep the arbitrageurs happy, whom they need to rebalance the pools. What we found was that the senior team identified and addressed what is in our view the most important competitive issue in the AMM space: in order to succeed, an AMM has to be attractive to liquidity providers. Moreover, sustainable success means that the attractiveness to liquidity providers cannot simply consist of paying them money or tokens. Everyone can pay liquidity providers, so according to the rules of micro-economics the protocols relying on subsidizing them will enter into a ruinous competition where they will eventually end up at the point where they pay all fees away.

In order to build a sustainable and profitable two-sided marketplace the protocol needs to offer something unique and non-replicable that the liquidity providers value more than just plain subsidies – and in our view Bancor's v2.1 protocol may have found such offering. The key distinctive value proposition offered by Bancor v2.1 to its external liquidity providers is that (a) it allows LPs to provide liquidity in a single token only, as opposed to a token-pair as is the case for other protocols, and (b) that, under certain circumstances and based on certain assumptions, it protects the liquidity provided against Impermanent Loss. This, in our view, can be an extremely interesting value proposition for HODLers who in a standard AMM protocol would suffer an Impermanent-Loss-turned-permanent if the token of their choice goes "to the moon" against the asset with which they trade. It could also, in our view, be particularly interesting for a protocol sponsor who wants to sponsor a trading venue for their asset without risking massive losses in case their asset outperforms they market, as they of course hope and expect it will.

Undoubtedly the Liquidity Protection constitutes a value transfer from the BNT token holders, to the non-BNT liquidity providers of the system. This is arguably is the cost of "doing business": liquidity providers are needed for the protocol to operate and for everyone to earn fees. The commercial reality is that all protocols pay the liquidity providers one way or the other. However, as we have seen in the recent Uniswap / Sushiswap episode it is very hard to hold on to liquidity providers in the presence of a competitor who can fork the code and offer a higher reward.

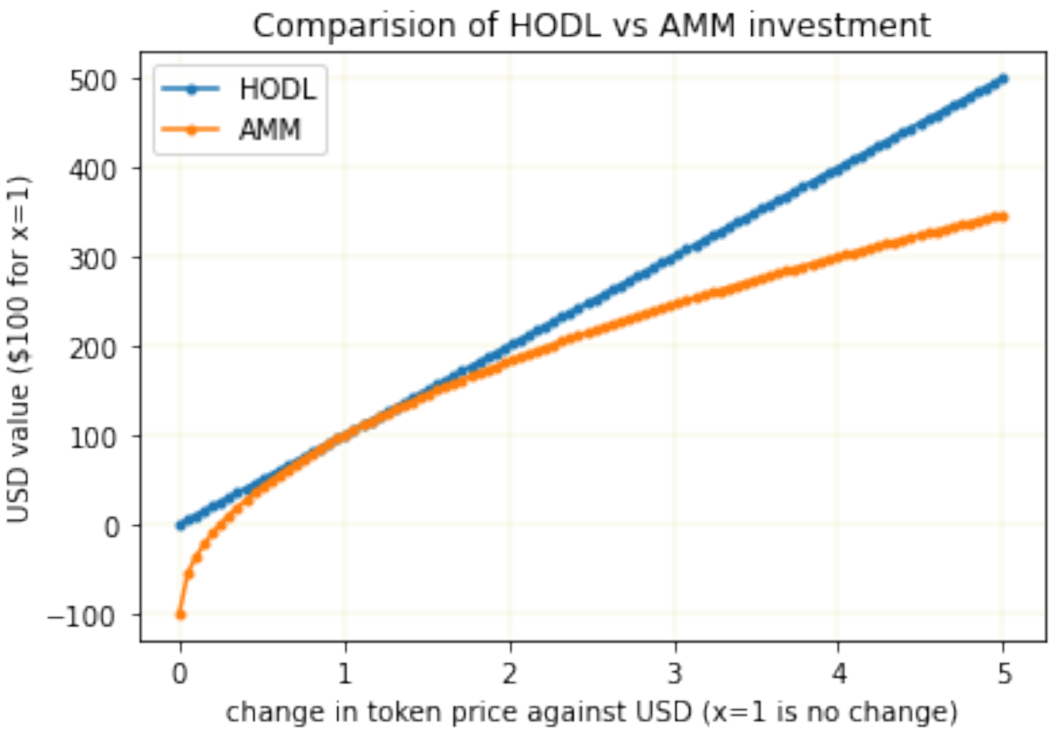
Bancor is, in our view, unique in that respect in that the BNT holders provide a real service to the protocol: via the dynamic supply mechanism they pay for the Liquidity Protection of the non-BNT liquidity providers, and in return they reap the rewards for doing so by earning part of the fees the system generates, either directly when they stake BNT in a pool, or indirectly when they benefit from the reduced overall BNT supply when the network is burning fees it earned on the BNT it staked. We have yet to see whether Bancor v2.1's value proposition is good enough for liquidity providers to flock there instead of elsewhere. In our view it should be, but this is hard to predict, especially in the current "yield farming" environment where a lot of focus seems to be on short term speculative gain, and little focus on the long-term prospect of a protocol. In our view this is where Bancor's v2.1 protocol is different. In comparison to other protocols it is hard to replicate. Whilst the code can be forked this does not replicate the existing BNT token ecosystem, and this ecosystem is crucial to how the protocol works. This, in our view, gives Bancor a good shot at being a protocol the survives and thrives in the long run.

Before we move on, we need to briefly refer to disclaimer that you can find at the beginning of the document and that you should read. Bancor v2.1, like any other AMM, is a highly complex dynamic system with a lot of feedback loops. Whilst we have made every effort to run a thorough and impartial analysis of the system, we are certainly not infallible, and we may have misunderstood what has been communicated to us, or we may simply have made mistakes within the time and budget allocated to this analysis. We believe that in this paper we have laid out how we reached our conclusions in a transparent manner. No reader should rely on any of the conclusions in this paper without independently verifying of how they have been reached. If in doubt please feel free to contact us with any questions, suggestions, or criticism. This paper does not constitute advice of any kind, and it certainly does not constitute investment advice.

Bancor's unique value proposition

Bancor is an Automated Market Maker ("AMM") protocol. This means commercially it is a three-side marketplace: in order to operate optimally its offering must be optimized at the same time for the trading end-customers, the liquidity providers, and the arbitrageurs. End-customers and arbitrageurs are relatively easy to serve: the former go to where trading is cheapest, and the latter will jump in when there is free money to be made. So, the key to optimizing an AMM's value proposition is to attract and retain liquidity providers without, and this is important, paying them too much. It is easy to attract liquidity providers by overpaying them, and this is what seems to happen in the market at the moment. For a protocol this is not a sustainable long-term value proposition. The only way for an AMM protocol to become valuable in its own right is to build a value proposition for LPs that does not hand all fees over to them, and that cannot be easily copied. In our view, the Bancor protocol has a good shot at achieving this.

In order for AMMs to function they need to hold the asset they are trading, and this is where liquidity providers come in: they are the ones who own those assets and who contribute them for the protocol to use. The issue they face is what is commonly referred to as Impermanent Loss, which is defined as the difference between what they get when they hold the asset outright, and what they get when they hold it in an AMM pool. We discuss this topic greater detail in the appendix, and here we address only the high-level results. Let's say we use USD as numeraire and $x = p/p_0$ is the price of the asset now, relative to what it was when the investment was made. The value of the HODL strategy is x and the value of the AMM strategy (where the investor borrowed the 1 USD they had to contribute to the pool) is $2\sqrt{x} - 1$. The chart below shows this relationship at an original investment of 100 USD, and it also shows the main problem of an investor who wants to contribute their assets into a liquidity pool: on the upside they earn less, and on the downside they lose more.



HODL vs AMM

This is even compounded for the typical token portfolio which is often a bet that one of the tokens will pay for all of them. For example, let's consider a portfolio of 10 tokens, with 10 USD invested in each. If they all double then the HODL portfolio goes to USD 200, whilst we can read from the graph above that the AMM portfolio goes to USD 182, ie USD 18 less. Where it gets really bad is when one of the assets goes to USD 200 and all others go to zero. The HODL portfolio goes to the same value as before, USD 200. However, the 9 AMMs corresponding to the vanishing assets go to -USD 10 each because of the money borrowed initially, so that's a total loss of -USD 90. When the asset rises 20x, the AMM portfolio goes to $2\sqrt{20} - 1$ which in this case means USD 79. Net/net the AMM portfolio has net value *loss* of USD 79 - USD 90 = -USD 11. So, whilst HODL *made* USD 100, AMM *lost* USD 111 of the original USD 100 investment. This, in a nutshell, is why it is dangerous for a HODLer to contribute their assets to an AMM.

Bancor's vision is to insure long-term liquidity providers against this Impermanent Loss, which quite often ends up being permanent. The way Bancor is planning to insure liquidity providers is described in more detail in the specifications section. On a very high level, within the Bancor system all pools operate against BNT, and the network will mint and burn those tokens as needed. Economically this means that some risk of the Impermanent Loss of the pools is moved to the BNT holders, who earn part of the fees that trading in those pools generate in return. The qualification "some" refers mostly to the fact that (a) it is a governance decision which pools are included into the protection system, (b) the insurance is only extended to long term liquidity providers, and (c) in some cases the insurance pays out in BNT as opposed to in the token deposited.

The network here is taking a certain risk, especially initially when the system is still in the testing phase. Also, arguably currently the non-BNT liquidity providers get too good a deal - they get guaranteed HODL returns plus a sizeable chunk of the fees almost regardless of what happens. This might be what is needed in the current environment to make them move into the Bancor system, but on the basis that they are guaranteed HODL returns future versions of the protocol might well make their rewards less generous, and more in line with the risks they are (not) taking.

Competitive landscape

When looking at AMMs there are three main participants who need to come together to make the business work: the trading customers, the liquidity providers, and the arbitrageurs.

Trading customers. As far as the trading customers are concerned the decision with whom to trade is very easy: everything is openly available on-chain, so apart from some esoteric front-running scenarios they will split their order and route it in a manner to minimize overall slippage and fees. There is no differentiation, no lock-in, there are no moats, and there are already aggregators that deal with optimal routing of end-customer transactions to the various available pools, so the competition on fees is intense.

Liquidity providers. End customers can only trade to the extent that there is sufficient liquidity available across the pools. If potential liquidity providers do not feel it is worth their while contributing liquidity to the system then end customers will not be able to trade, at least not without incurring unacceptable levels of slippage. This means that liquidity providers must be incentivized to provide liquidity into those pools, and this means those liquidity providers must like the pools' risk / return profile. This is often the rub: liquidity providers hold a certain asset because they like it and because they think it might go up, "to the moon" even. Moreover, they run a portfolio approach to their investments in the sense that they hold multiple tokens that they think might moon, and they are doing well if only one or two out of their entire portfolio actually do.

The issue for people with this investment strategy is that liquidity provision is the antithesis of their philosophy: once those tokens are inside a liquidity pool their returns are significantly reduced, from x to $\sqrt{x}$. So, if the asset does 100x, they get 10x. If the asset does 10,000x, they get 100x. This might still look like good returns - and they are - but it significantly changes the economics of the portfolio approach that relies on a few assets outperforming the rest if those outliers will be severely cut.

Arbitrageurs. There is a third and very important component to AMM pools, the arbitrageurs. So far in this paper we assumed a deep and liquid market against which this pool could be arbitraged. This assumption is almost certainly wrong: if there was a deep and liquid market there was no need to use the pool and pay its slippage. One could somewhat save this assumption by requiring that there is a deep and liquid market for *some* players, but this does not sound realistic, not least because those players would probably have incentive to make markets directly. So, in this sense arbitrageurs in the system might well be akin to the liquidity providers in that they hold a trading inventory and that they actively choose to intervene in the markets if they feel the economics is right. Because of this more active strategy they can choose at which point in time they want to profit from the market volatility, and at which point they want to just ride the markets directionally.

Protocol owners. Protocol owners, and we include the governance and dev team here, must ensure that the value proposition for all three “customer” stakeholders is balanced so that transaction volume and profit is optimized. Many sponsors of AMMs have found that it is not clear what exactly their value proposition, or rather their unique selling proposition, is and how they can protect it. For example, we have recently seen Uniswap being forked by Sushiswap in a cliff-hanger storyline, and it ultimately led to a significant amount of liquidity moving. We have also seen Uniswap’s business model change as a consequence of this, introducing a protocol token that would allow for yield farming. Uniswap itself is building on AMM technology that Bancor originally published in 2017.

Bancor’s take in the upcoming v2.1 release is that to remain relevant and to continue adding value to their customers, the protocol owners must provide on-going value over and beyond simply providing the code and the governance. They also must have some skin in the game and provide economic benefit for the other participants.

Bancor specification

Bancor’s upcoming v2.1 release includes a number of important features that make liquidity provision more attractive. Those features are

- **Single-Asset Contribution.** Liquidity providers can provide a single asset into a liquidity pool, and the Bancor protocol will provide the corresponding BNT.
- **BNT-Only Contribution.** To the extent that there are single asset contributions that are still being matched by the protocol, outside liquidity providers can take over those positions.
- **Liquidity Protection.** Liquidity providers of all types (single asset, BNT-only, combined) are, subject to certain schedules, protected against Impermanent Loss.

Before we can discuss these features, we need to discuss the one feature that makes the above possible, which is the **Elastic BNT supply,** where the protocol mints and burns BNT to support the functioning of the system.

Elastic BNT supply

Bancor is different from to other AMM protocols in that instead of providing pools for “crosses” (say, ETH vs WBTC) all Bancor pools have a common network token (BNT) as one of their components. From a user’s point of view this can look like a disadvantage - they pay fees twice, and they incur slippage twice – but this is not necessarily the case. The fees on Bancor will be whatever they have to be competitive with other AMMs so if the requirement is to pay fees twice instead of once there might be a fee adjustment to compensate for that (note that each pool's fees can be adjusted by liquidity providers). In terms of slippage, the big advantage of the one-pool-per-asset model is that *all* liquidity corresponding to a given token is in the same pool, and is not distributed, say, over TKN/WBTC, TKN/ETH, TKN/XXX - which is often the case in other protocols. Therefore, whilst slippage is incurred twice it might be that the slippage incurred is smaller.

However, the most important reason why Bancor is using its protocol token, BNT, as the counterpart asset in each and any of its pools is that the protocol controls its supply and it can therefore mint and burn BNT as needed to keep the system in balance. For example, when liquidity providers only want to provide liquidity in TKN but not in BNT then the network can mint the corresponding BNT. When the liquidity provider withdraw their liquidity then the network burns the corresponding amount of BNT. This looks like a zero-sum game, but on further analysis it is not: whilst the TKN and the BNT were in the pool the pool earned fees, and those fees needed to be partially paid in BNT. So, assuming that there is no Impermanent Loss (this will be discussed below) and no matching BNT contributions (ditto) the network earned BNT and therefore will end up with more than it initially contributed. When TKN liquidity is withdrawn the amount burned is larger than the amount initially minted, so net/net the BNT supplied is reduced. The tightening of supply should benefit the BNT holders as a group since the increasing scarcity of BNT should increase its price.

Another important function of the elastic BNT supply is to allow for the Liquidity Protection that is, under certain circumstances, offered to liquidity providers. If they have Liquidity Protection this means they are protected against Impermanent Loss and are paid HODL returns instead. A priori this is a transfer of value from BNT holders, who pay for this protection as a group via dilution, to the non-BNT providers of liquidity. This is a commercial decision: Bancor protocol, like any AMM protocol, needs first and foremost liquidity providers to engage, otherwise there can be no trading and therefore no fees. Competition for liquidity providers between the protocols is fierce to the extent that their associated pools provide commoditized services. Bancor's value proposition to liquidity providers in this context is different: not only does it allow for liquidity providers to maintain exposure to *only* one asset as opposed to a pair, but also, subject to certain conditions, they will be able to earn HODL returns on their chosen asset, plus fees. This should be a very attractive value proposition for those liquidity providers. On this basis, there is an argument to be made that it makes sense as a commercial decision for BNT holders as a group to provide Liquidity Protection to attract LP by providing such insurance.

As an aside – Liquidity Protection is also offered to liquidity providers who provide BNT liquidity, and it is therefore also a value transfer from non-liquidity-providing BNT holders to liquidity-providing ones. This is by design as it encourages BNT token holders to be liquidity providers and to thereby actively take part in supporting the ecosystem rather than sitting on the sidelines.

Single-asset contribution

Within the Bancor framework all pools have BNT as one counterpart, which allows for features such as the single-asset contribution described here, and the liquidity protection (aka Impermanent Loss insurance) described further below.

If a liquidity provider only wants to contribute the risk asset (we refer to it as TKN throughout) then the Bancor network will mint BNT to match that contribution. That matching happens at the currently implied pool exchange rate, meaning that the relative pool balance does not change pre and post contribution.

Whilst the respective contributions to the pool are of equal monetary value initially there is an implicit agreement between the pool and the liquidity provider that the latter is taking more of the token risk, and the former more of the BNT risk. Specifically, the pool is split in a ratio of $1{:}\,x$ between the network and the pool where, as throughout this paper, $x = p/p_0$ is the ratio between the current price of TKN expressed in BNT, and that when the liquidity was provided. In other words, the value allocated to the liquidity provider is

$$AMM_{LP} = x\frac{2\sqrt{x}}{1+x}\cdot N$$

and the value allocated to the network is

$$AMM_{NW} = \frac{2\sqrt{x}}{1+x}\cdot N$$

where N is the notional amount of BNT initially contributed to the pool by the network. This of course is equal to the initial BNT value of the stake the liquidity provider has contributed. here is some complexity with respect to how repayments are handled if the liquidity providers want to subsequently withdraw their stake. Given that at any point in time the pool consists of 50% TKN and 50% BNT the amount the liquidity provider is owed might not be available in the pool in the required form. Even if it is available it might be allocated to other liquidity providers and therefore not available for distribution. The distribution therefore is executed as follows

1. The liquidity provider gets the TKNs corresponding to their share of the pool (their pool share is given by AMM_{LP}; half of this will be in TKN and distributed, and the corresponding BNT will go to the network for burning)

2. The network liquidates pool shares it owns and distributes the corresponding TKN, up to the point where it no longer owns any pool shares; the corresponding BNT is burned

3. For the missing TKN amount, if any, the network mints BNT for the pool implied TKN price and distributes that BNT; it is then the liquidity provider’s choice to convert those into TKN at their own expense

BNT-only contribution

BNT-only can be staked at any point, but only to the extent that there are unmatched tokens available from liquidity provider who have previously staked the risk asset (TKN) alone.

Unless liquidity protection applies, BNT-only liquidity providers are exposed to Impermanent Loss as if they had staked the BNT together with TKN, where the BNT-only contribution happened

$$AMM_{LPB} = \frac{2\sqrt{x}}{1+x} \cdot N$$

It is important to understand that in this case the network is taking a basis risk. If we use p_0, p_1, p_2 for the price of TKN in BNT at times $t = 0,1,2$ then the network's position at time $t = 2$ from matching the token contributed at time $t = 0$ is

$$AMM_{NW} = \frac{2\sqrt{p_2/p_0}}{1+p_2/p_0} \cdot N$$

whilst the networks liability at $t = 2$ toward the provider of BNT liquidity at time $t = 1$ is

$$AMM_{LPB} = \frac{2\sqrt{p_2/p_1}}{1+p_2/p_1} \cdot N$$

and therefore the network's residual position is

$$AMM_{RES} = \left(\frac{2\sqrt{p_2/p_0}}{1+p_2/p_0} - \frac{2\sqrt{p_2/p_1}}{1+p_2/p_1}\right) \cdot N$$

BNT restaking

An important corollary of the above mechanism is that withdrawal and immediate restaking of BNT leads to a different result. If a BNT-only liquidity provider stakes at $t = 0$ then their staked value at time $t = 2$ is

$$AMM_{LPB} = \frac{2\sqrt{p_2/p_0}}{1+p_2/p_0} \cdot N$$

If however they withdraw and restake at time $t = 1$ then their ultimate payoff is

$$AMM_{LPB} = \frac{2\sqrt{p_2/p_1}}{1+p_2/p_1} \cdot \frac{2\sqrt{p_1/p_0}}{1+p_1/p_0} \cdot N = \frac{4N\sqrt{p2/p0}}{(1+p_2/p_1)(1+p_1/p_0)}$$

Matched staking

Liquidity providers can stake TKN and BNT on a matched basis. From a point of view of the system this is treated exactly like two separate stakes, one of TKN and one of BNT. To the extent that the stakes are perfectly matching the formula for the entire stake simplifies to

$$AMM_{LPM} = 2\sqrt{p_1/p_0} \cdot N$$

It is possible to withdraw the components of a matched stake separately, in which case the formulas provided further above apply.

Fees

So far, we have assumed no fees. Traditional market makers - especially professional ones - often do not charge fees but rely on the bid/ask spread to make money. This is not possible here: whilst AMMs can charge sizeable bid/ask spreads to their customers (because of slippage;) the bid/ask spread does not accrue to the liquidity pool, but to the arbitrageurs who bring the pool back into balance.

So, in order for the liquidity providers to earn return on their stake funds there must be explicit trading fees charged by the pool. In Bancor's case, the default fee charged for every trade is 0.2% of the traded amount and is adjustable per pool by its liquidity providers.

The way the fee is taken is specifically as follows (assume a 0.2% fee in the example below, and BNT to TKN exchange):

1. The incoming BNT amount is converted into TKN according to the formula implied by the invariant
2. The fee of 0.2% is token off the TKN amount, and the remainder is sent to the trading customer
3. The TKN fee remains in the pool

Whatever the direction of the transaction the fee is *always* taken from the target token leg, ie if TKN is converted into BNT then the fee is taken from the BNT.

The way the fee is tracked and allocated to the liquidity providers works as described below. Before we can go further, we need to introduce the *modified invariant* $\bar{k}$ that we are using instead of $k = x * y$. This invariant is

$$\bar{k} = \frac{\sqrt{x * y}}{N}$$

where x, y are the number of BNT and TKN respectively, in their native units, and N is the number of pool tokens issued. The first thing to note is that if $x * y$ is invariant then so is any function $f(x * y)$, so the square root term does not impact the result. It does however introduce better scaling properties, what we'll see below. Including N does not change anything in terms of trading and pricing as trades leave N invariant. It however ensures that now $\bar{k}$ is also invariant with respect to provision and withdrawal of liquidity.

There is one event that changes $\bar{k}$, which is when TKN and/or BNT are added without adjusting the number of pool tokens. This is the case when fees are added to the pool. The square root ensures the correct scaling: if say 1% of both BNT and TKN are added then $\bar{k}$ also increases by 1%, hence $\bar{k}$ tracks the value of the outstanding pool tokens as the pool increases in size due to fees.

Fees are implicitly allocated to pool tokens in the sense that whenever new pool tokens are added they are taking into account the increase in pool value due to fees. To give an example, let's assume that initially the pool consisted of 100 BNT and 100 BNT worth of TKN, and there have been 100 pool tokens issued against this. Let's further assume that due to fees alone the pool has grown to 110 BNT and the same value of TKN. Someone contributing 100 BNT plus 100 BNT worth of tokens would now only get $100/110 = 90.9$ freshly minted pool tokens for their contribution.

Liquidity protection

The big change in Bancor protocol v2.1 as compared to previous protocols, and also as compared to competing protocols, is the *Liquidity Protection* aka Impermanent Loss insurance. Not all liquidity is covered by this liquidity protection, and it is possible for there to be partial coverage. Under the current plans, the percentage covered under liquidity protection will be:

1. 0% for the first 30 days
2. 30% on day 30
3. Increase by 1% point per day up to 100%

This is a linear rule so we can simply assume for our calculation that liquidity providers have two types of tokens - those that are not covered by the protection scheme, and those that are 100% covered - and over time more and more tokens move from one category into the other. In what follows we will *only* deal with those imputed tokens that are 100% covered, understanding that the previously discussed rules apply for the remainder of tokens held.

The principle of the liquidity protection is very simple: a liquidity provider's contribution to the pool is protected, in whichever form contributed, ie as if the liquidity provider had followed the respective HODL strategy. Mathematically, if the investor chooses to withdraw then as a single-asset provider they get

$$AMS_{LP}^{P} = x\left(1 + \frac{2\sqrt{x}}{1+x}\phi\right) \cdot N$$

where ϕ is the fee accrued to the pool tokens as a percentage of their initial value. The corresponding formula for BNT-only contributions is

$$AMS_{LPB}^{P} = \left(1 + \frac{2\sqrt{x}}{1+x}\phi\right) \cdot N$$

and the formula for joint contributions is simply the sum

$$AMS_{LPM}^{P} = (1+x)\left(1 + \frac{2\sqrt{x}}{1+x}\phi\right) \cdot N$$

As with the single-asset payouts there are some subtleties with respect to distribution for liquidity providers who are owed TKN. Like in that case those tokens are provided

1. from the redeemed pool tokens of the liquidity provider
2. from pool tokens held by the network
3. as BNT equivalent (calculated at the current pool rate) with BNT minted from the network

Economic analysis

BNT liquidity locked in pools

With Bancor v2.1, newly minted and burned BNT is in many cases not issued directly to the price-setting external market but only to the liquidity pools. We therefore need to look at what happens to the BNT locked in those pools and in particular how it can interact with the supply and demand curve of the outside market.

In what follows we look at the key lifecycle events in an BNT/TKN pool, which consist of *market moves*, *trading,* and *provision* and *withdrawal of liquidity.*

Market moves. If significant amounts of BNT are held in pools, then this might reduce the volatility of BNT. Whenever BNT goes up against their respective TKN the pools sell BNT against TKN, and vice versa then BNT goes down. This effect is somewhat amplified in the case a significant amount of BNT in the pools is network owned.

Trading BNT for TKN (no fees). We consider the scenario where a trading customer wants to exchange BNT for TKN. On the face of it, the trade removes BNT supply from the outside markets and locks it in a pool. However, the pool will be out of kilter after this trade, and it will be reversed by an arbitrageur who will restore the pool to its original balance, and therefore also restore the BNT supply outside the pools. Net/net the pool will have intermediated the transaction between the "market" and the trading customer, where the second intermediary, the arbitrageur, will have retained a bit of the trade economics for themselves.

Trading TKN for BNT (no fees) and **Trading TKN1 for TKN2 (no fees).** The two other trading scenarios – "trading TKN for BNT", and "trading TKN1 for TKN2" by combining the two legs – lead to the same result as trading BNT for TKN: ultimately the pool will have been restored by arbitrageurs, with no change to the outside supply and demand of either BNT or TKN.

Trading (with fees). The trading scenarios above considered no fees, so now we want to analyze *only* the impact of fees. This is rather important, as ultimately Bancor's model is based on the ability to earn fees from trading. We will discuss fees in more detail below, so suffice here to say that fees are to be paid with *outside* BNT and that it is either paid to liquidity providers (TKN or BNT) or to the network. BNT paid to TKN liquidity providers is, from the BNT holders' point of view, simply as pass-through to a "business associate". BNT fees that are paid to BNT liquidity providers directly increases their holdings, and BNT fees that are paid to the network will be burned and should therefore increase the price out BNT outstanding via removal of supply.

Adding TKN liquidity. Here we consider the addition of TKN single-token liquidity. In this case the corresponding BNT liquidity is provided by the network with freshly minted tokens. For a fundamental value asset this may be considered dilution. However, we do note that this BNT goes straight from the protocol into the smart contract and it does not interact with or substitute any external supply and demand. Therefore, a good argument can be made that this particular event should be price neutral.

Adding BNT liquidity. We now consider the case of adding BNT liquidity by taking over part of the protocol's stake in a pool. The impact here is straightforward in that it removes BNT that might otherwise be available as supply on the outside market or creates additional demand if the contributed BNT has been purchased for contribution. In addition, BNT fees are burned when user-owned BNT is added to a pool and replaces protocol-owned BNT.

Removing TKN liquidity (no market moves). When removing TKN liquidity we have to consider two effects: (1) the removal of liquidity itself, and (2) the attribution of value in case of market moves. Here we concentrate on (1) and therefore assume that the withdrawal of liquidity happens at the same price level as its contribution. In this case the network gets all its BNT back, plus fees earned if any, that it duly burns. The same arguments as on the way in apply, so again a good argument can be made that the impact of this event is price neutral.

Removing BNT liquidity. When removing BNT liquidity, the BNT liquidity provider hands back their pool shares to the network and is compensated with freshly minted BNT. The network in this case holds on to the pool shares that represent both TKN and BNT. If the markets have not moved, then this simply undoes the effects of adding BNT liquidity in the first place. If markets have moved, then there is the fee and the impermanent loss to consider.

Removing TKN liquidity (TKN price went up). We are now considering the scenario where TKN went up. We have discussed above the attribution of value in this case, noting that (a) the LP's share of the pool tokens is $x/(1+x)$ where $x = p/p_0$ is the change of relative price, and (b) that the network tries to serve the withdrawal in TKN, first from the redeemed pool tokens, and then from any other pool tokens the network owns. Finally, if the network does not own sufficient pool tokens it mints BNT at the relevant exchange value. Those BNT are distributed to withdrawing liquidity provider, and they therefore can impact the supply and demand of BNT in the real world.

Removing TKN liquidity (TKN price went down). If TKN went down relative to BNT then the LP's share of the pool tokens is still $x/(1+x)$ but now $x < 1$. Assuming the one-side investment has not subsequently been taken over by a user providing BNT liquidity this means the network will have sufficient pool tokens from this part of the liquidity pool alone to pay back the withdrawing liquidity provider in tokens. If the networks stake had previously been taken over by an outside BNT liquidity provider this might not be the case and the network might have to mint BNT for the outside market. However, the newly minted BNT merely compensates for the BNT that had previously been withdrawn by depositing it into the pool, which mitigates this effect when looking at it from a longer-term point of view.

Trading per se also does not change the external market supply, on the basis that arbitrageurs will rebalance the pool and therefore the pool is only a buffer that temporarily warehouses transactions until the equal and opposite side can be found. Trading only has an impact on the pool if it leads to a persistent change in the price of the TKN vis-a-vis BNT. We have seen that in this case the pools exert a stabilizing impact on the BNT price as they are buying on downwards moves and selling on upwards moves, thereby keeping BNT volatility in check.

Liquidity protection

The protocol offers liquidity protection to long-term liquidity providers. That means for liquidity that has been locked in an AMM sufficiently long the liquidity providers get the HODL returns on their asset when they withdraw.

We now want to value the Impermanent Loss option. In other words, we want to know how much the pool will, in expectation, hand over to the arbitrageurs.

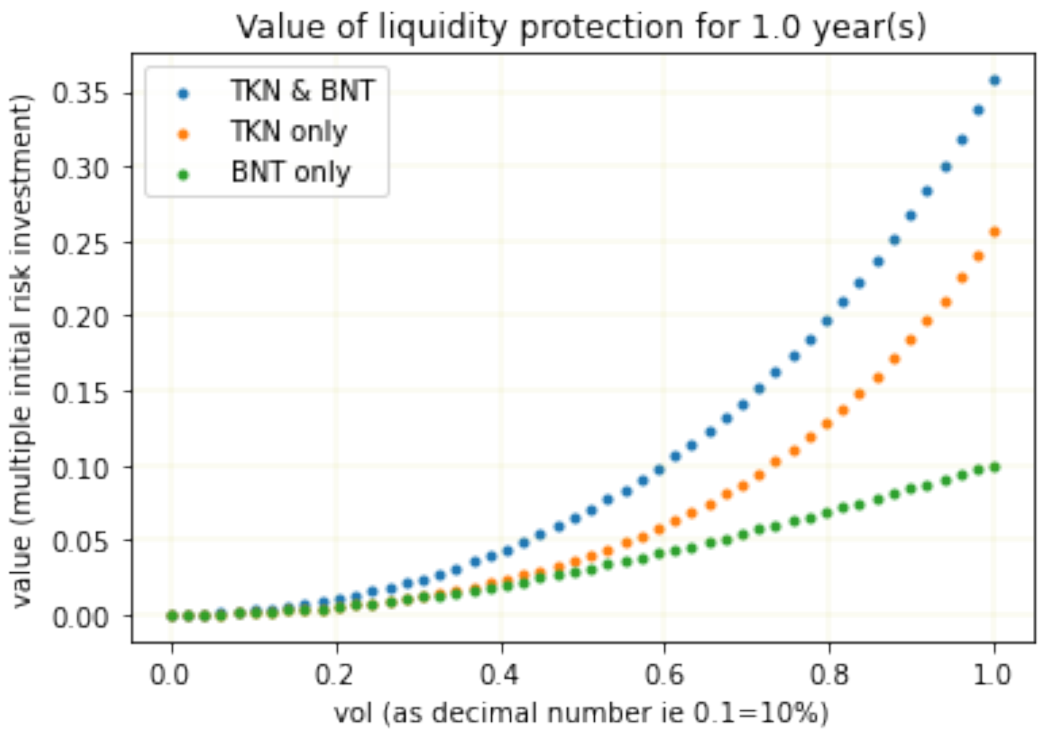
As we have seen, the overall Impermanent Loss follows this very easy formula

$$IL(x) = 1 + x - 2\sqrt{x}$$

The first thing to notice is the IL is not bounded for large x; in fact, it grows linearly. For $x = 0$ the portfolio IL is 1, and IL_{LP} allocated to the liquidity provider entirely disappears. The latter is simply because when the TKN price is at zero then the HODL value of the portfolio is zero, and the AMM portfolio cannot underperform this, so the entire Impermanent Loss in this case is allocated to the provider of BNT liquidity.

Using quantitative finance lingo liquidity providers are offered a perpetual American option with the above payment profile. “American option” means that it can be exercised at any point before maturity, “perpetual option” means that there is no maturity, so “perpetual American option” means is can be exercised once at any point in the future.

Ignoring subtleties around what drift to apply to assets in the crypto world, and whether delta hedging is actually possible, this option can be priced in a standard Black-Scholes framework, using a lognormal distribution for x. In order to be able to do this we need to make a number of observations and assumptions. Firstly, we assume that early exercise of the American option will not be optimal which is most likely true. Even if it is not true the corresponding European option will be a lower limit for the option price. Secondly, we need to restrict our maturity. For larger maturities T the option value will grow in $\sqrt{T}$ which is unbounded. In other words, the option granted has infinite value unless it is exercised at some date in the not indefinite future. The assumption here is that governance will at one point introduce some appropriate limit.



Value of liquidity protections split by TKN and BNT

Above we have drawn the value of the liquidity protection under the assumption that it is a one-year European option, meaning that it can only be exercised after exactly one year. What is ignored here is that this option premium is balanced by fees, which we will discuss in the next section. To adjust this chart for different time horizons one needs to take into account that volatility scales like the square root of maturity, meaning that a quadrupling of the maturity period leads to a doubling of volatility.

We have also split up the value of the liquidity protection option between TKN holders and BNT holders. They are close for smaller volatilities, but they diverge for bigger ones. According to other analysis' that we have done this is driven in particular by scenarios where TKN goes up very strongly against BNT.

Valuing fees

The purpose of Liquidity Protection is to attract liquidity providers into Bancor's pools; liquidity providers are necessary for the Bancor pools to be able to "do business", and liquidity providers have a choice where to place their liquidity. Therefore, the cost of Liquidity Protection is the cost the pools pay for doing business.

One might argue that initially the cost of doing business is too high, ie that liquidity providers are getting too good a deal. At this stage this is hard to decide, the proof of this is in the pudding: if the Bancor protocol does not offer sufficiently attractive terms liquidity providers won't come, if the Bancor protocol offers too attractive terms they will come but they will take the lion's share of the profits. Ultimately, like with any business, key here is to have a robust cost and risk control framework in place that allows the Bancor protocol to fine tune the offer to market conditions, and to find a spot that is attractive enough to generate sales and to still maintain a healthy profit margin.

Currently fees are 0.2% of the trading volume going through a pool, and they can be adjusted per pool to be competitive in the marketplace. In line with what has been said in the previous paragraph, fine tuning the fees will ultimately maximize profits by setting them in a way that both volume and profit margin are sufficiently high. In particular the BNT holders who contribute to the on-going business by providing Liquidity Protection must be adequately rewarded for the services they render to the protocol.

Note that customers who use the Bancor system are by and large expected to use it to exchange non-BNT tokens into each other, meaning that BNT is only an intermediate leg in that trade. On that basis the effective fee doubles, so as it stands it would be 0.4% for trades between say ETH and WBTC. Trading customers not only pay fees, but they also pay slippage. This slippage however does not benefit the pool but is picked up by the arbitrageurs who will ultimately balance the pool so in our analysis here it is not relevant.

The *allocation* of fees is somewhat unusual in that if follows the value of the collateral. So if $x = p/p_0$ is the relative price change between TKN and BNT between when the liquidity has been contributed to the pool and when it has been withdrawn then the fees are not allocated 50/50 between TKN or BNT but are distributed according in the ratio $1{:}\,x$. In other words: if BNT rallies, BNT holders get the lion's share of the fees and vice versa. Whilst this can cause pleasant or unpleasant surprises in individual cases over time, in a non-trending market the allocation will be 50:50, which is what we assume going forwards.

The key quantity we need to estimate for the revenues for liquidity providers is what we want to call the *collateral turnover*, ie the number of days it takes for the trading volume to equal the collateral amount. To give an example: if the pool contains 1,000,000 TKN and trades 100,000 TKN per day then the collateral turnover would be 10 days. We were looking through a number of Uniswap pools to get an idea of possible turnovers and, excluding the incentivized pools we found that many pools turn over 1x per day, some even 2x per day, and that the slower pools seem to be around the 5 days turnover mark.

On the basis that fees are distributed 50/50 for every turn each of the two liquidity providers earns 0.1% on their value staked. Turning the pool over twice per day would therefore give a fee income of about 75% of the pool volume on an annualized, non-compounding basis for the BNT liquidity provided, and the same figure for TKN liquidity. The equivalent figures for 1-day turnover and 5-day turnover are 35% and 7.5% respectively.

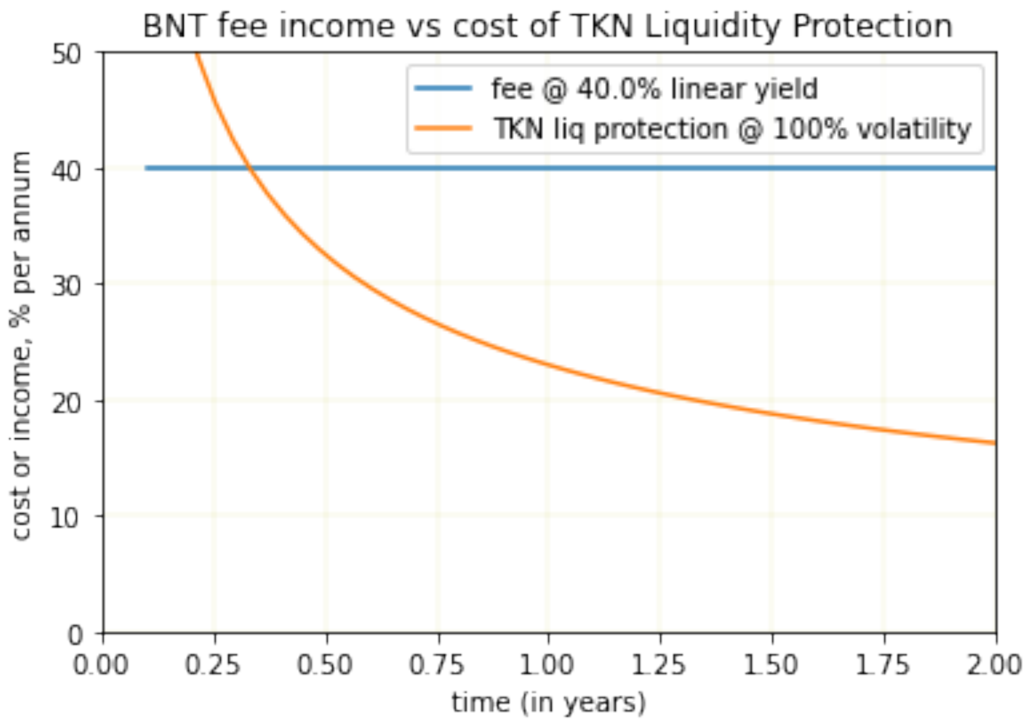
Annualized fee vs cost of TKN liquidity protection

The key here is that as fees grow over time in T while the option value only grows in $\sqrt{T}$ so over a sufficiently long-time horizon, the fees are expected to dominate the option value. In the above chart we are looking at fees vs the value of liquidity protection as a function of this horizon T, and we have linearly annualised those figures, ie we have divided by T. The two fee scenarios are an, in our view, optimistic scenario of 40% annual linear growth and an, in our view, pessimistic view 7.5% annual linear growth. For volatilities we use an annualized 50% and 100% as a reference. In our view those volatility numbers are not unreasonable, but they are very hard to predict. None of those numbers should be relied upon without further analysis.

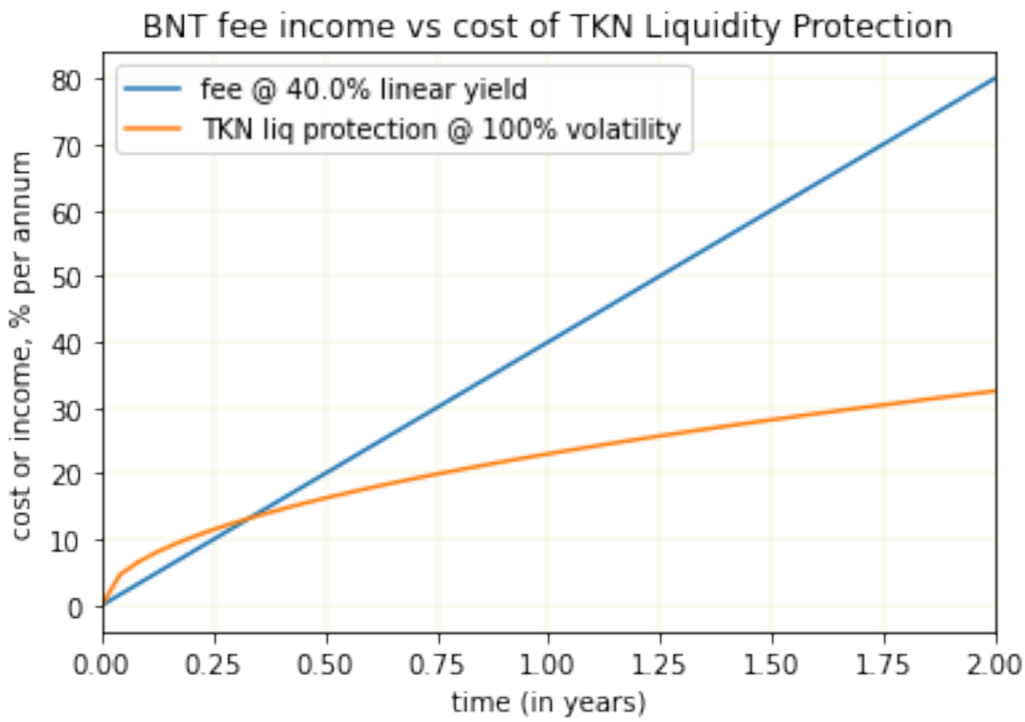
We are using linear growth, meaning that we have ignored the compound growth on the pool due to the fees because in this case we would have had to adjust the option value in a non-trivial manner. So effectively this analysis looks at the scenario “profits are withdrawn when they arise” which is a valid economic scenario.

Those fees will in particular be earned by the entirety of BNT investors. The revenues will differ for different BNT holders however – for example BNT staked in a pool will earn the stakes of that pool. Also, BNT holders can “earn” additional fees via the burning of fees paid to the network on the BNT it minted into the pools. If the liquidity provided into BNT pools is a multiple of the BNT owned by BNT holders this can be a sizeable additional revenue stream. On the other hand, this stream is not entirely without risk because the Liquidity Protection is effectively a cost charged to all BNT holders via dilution.

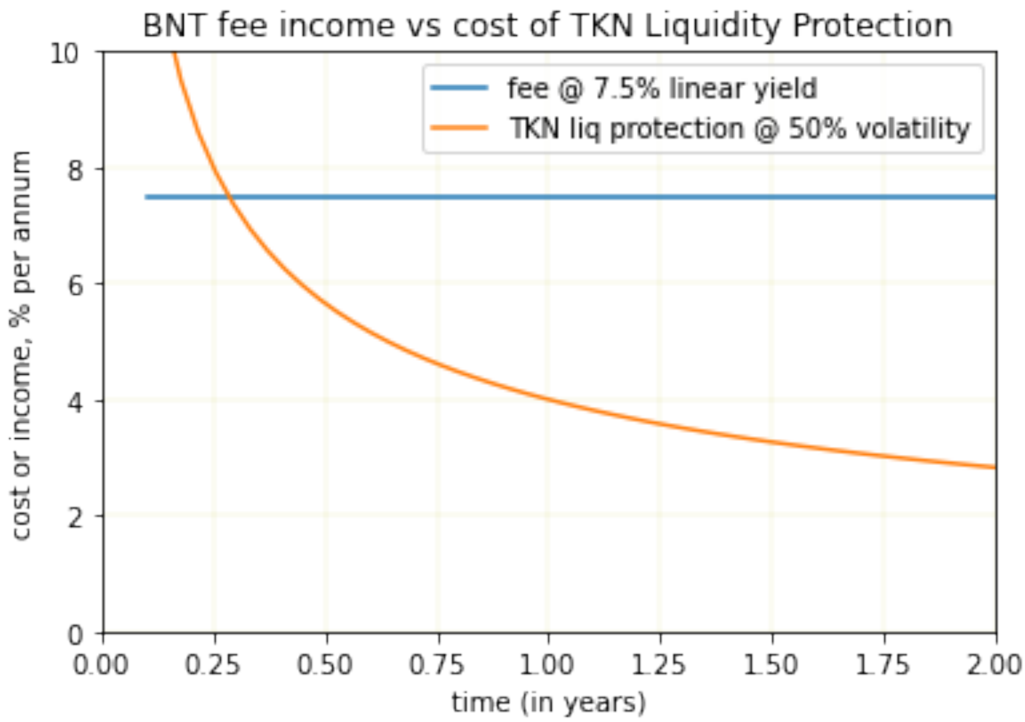
Below we show two fee-versus-option-price scenarios. The scenarios are the ones described above, ie 50% volatility and 7.5% fees and 100% volatility and 40% fees respectively. We show each charts in two representations, one being normalized “per year” and the other one accruing. In the normalized charts fees are flat and option value decreases with the time horizon, in the accrual charts the fees grow linearly and the option value increases as square root of time. In both scenarios we considered here the break-even point (where the fees earned outweigh the option value) is after about 3 months. This of course strongly depends on the scenarios considered, and different scenarios can have very different break-event points.



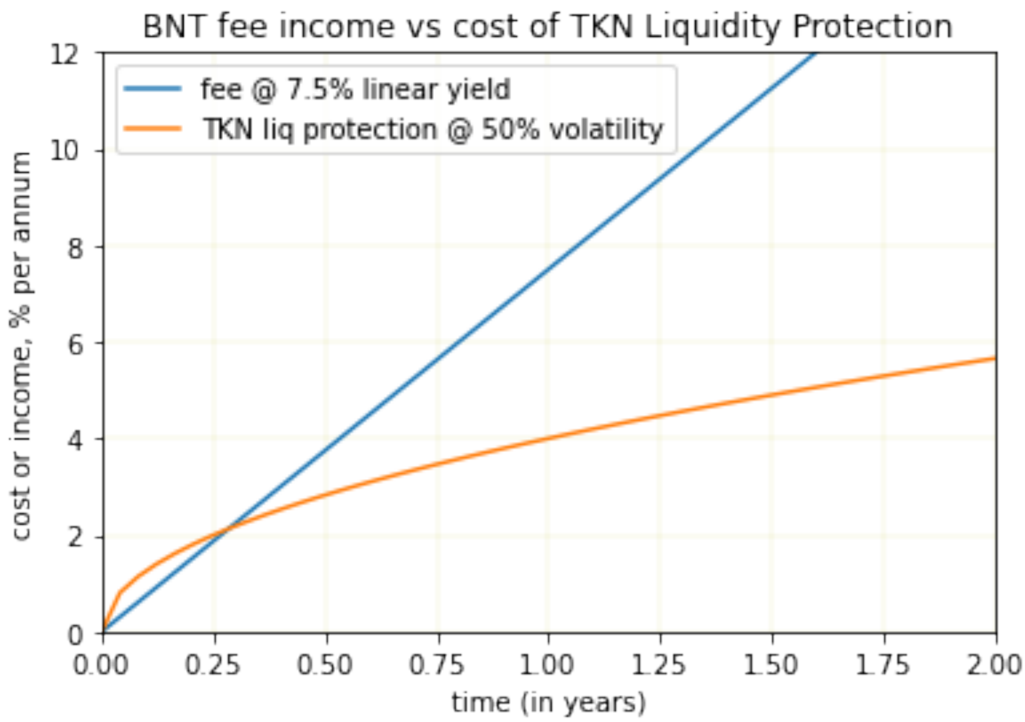
BNT fee income vs cost of TKN Liquidity Protection (scenario1, normalized)



BNT fee income vs cost of TKN Liquidity Protection (scenario1)



BNT fee income vs cost of TKN Liquidity Protection (scenario2, normalized)



BNT fee income vs cost of TKN Liquidity Protection (scenario2)

BNT inflation risk

We have already discussed that the network does not have a treasury, but instead pays its debts via “monetization”, ie via minting of new BNT. We have also seen that this has a number of advantages, in particular with respect to rewarding BNT holders for their services rendered to the protocol.

Momentum-driven assets like BNT can be subject to different dynamics when it comes to the impact on dilution, in that prices can be driven more by current demand and supply considerations than by fundamental measures, including market capitalization.

Based on this line of argument minting – even potentially unlimited minting – into liquidity pools for the purpose of matching single asset contributions is not an inflationary event per se as the BNT in the pools only interacts weakly with the supply and demand of BNT outside of the pool. Here however we are considering a different situation, notably when a liquidity provider who is withdrawing from a liquidity pool is exercising their liquidity protection option, and part of the payout is in newly minted BNT. Chances are that this liquidity provider does not want to keep their money in BNT but exchange it to another token of their choice, possibly the TKN they have withdrawn, or any other token if the withdrawal is due to a desire to liquidate TKN holdings at this point.

So, the situation where we find ourselves is that the network, in order to fulfill its obligations, has to print potentially substantial amounts of BNT in order to compensate liquidity providers. As a reminder, the pool Impermanent Loss is $1+x-2\sqrt{x}$ and for unbounded token prices x, the Impermanent Loss is unbounded and grows asymptotically like x. Single asset contribution slightly changes this formula, but it turns out that the biggest part of the option value goes to single asset contributors on the TKN upside, ie large x, so this does not make much of a difference.

Note that the increase in x can either be caused by an increase in the TKN price, or a decrease in the BNT price. If it is the latter then this will happen, in average, across all Bancor pools, so they will experience, in average, Impermanent Loss all at the same time. On the face of it this constitutes a downwards spiral risk. For example, assume that one TKN in a major pool has risen substantially against BNT, and a large liquidity provider liquidates, making use of their liquidity protection option. Further assume that they get a significant portion of their payout in BNT that they subsequently sell in the market, lowering the BNT price. The lowering of BNT increases the Impermanent Loss across *all* Bancor pools. If this in turn leads others to make use of their liquidity protection option, then this can lead to a downward spiral in BNT.

There are three natural counterbalances to this. Firstly, the secondary impact is not *automatic*. Just because the Impermanent Loss increases in all Bancor pools does not mean the liquidity providers withdraw their assets at once, especially given that there are some circuit breakers in place that make panic withdrawal a bad and potentially more risky option. If liquidity providers do not withdraw, the downward pressure on BNT is not amplified.

Secondly, as we have already discussed previously, the pool system is a natural stabilizer for the BNT price, in both ways. If BNT goes down, then the pools will be bidding in the market to buy BNT by selling some of their TKN holdings. The opposite happens on the upside, and to the extent that a significant amount of the total BNT money supply is inside the pools this dampening effect on extreme volatility can be be powerful.

Thirdly, and arguably most importantly, there are fees. Every dollar of liquidity attracted brings down the pool slippage. Assuming trading volume is optimally routed, and everything else being equal, decreased pool slippage means that more trading volume will end up in this pool, which in turn means increased fee levels. As we have argued above, (paying for) Liquidity Protection is to some extent the cost of doing business, ie the cost for BNT holders to be able to earn fees. The fundamental economic assumption of the protocol design is that the additional fees generated outweigh the cost of Liquidity Protection. If this is indeed the case then the downward spiral should be avoided.

Having said all this - the risk of a downward spiral might be remote but it is real and the governance process will need to ensure that there are appropriate limits in place until it can be asserted whether or not the *cost* of doing business can be justified by the revenues.

Risk limits and other governance implications

To summarize where we stand: we have seen that the Bancor v2.1 protocol is designed to be attractive in particular to liquidity providers, on the basis that those are the key protocol "customers" that need to be convinced to choose this protocol over alternatives. We have also seen that the subsidy of the protocol to long term liquidity providers under certain scenarios can be substantial. The protocol's expectation is that the cost of this subsidy is covered by the fees the protocol earns on that liquidity.

Key here is that the subsidy is not a fixed amount but instead un unhedged option, notably the Liquidity Protection option that insures long term liquidity providers against Impermanent Loss. The protocol's current choice is to not spend funds on hedging this option. Instead the ex-post cost when an option is exercised is socialized across the network, first by liquidating network assets and in case those are not sufficient by minting BNT.

The expectation is that, similar to how a traditional market maker takes a positional risk, over time the cost of providing this protection will be lower than the fees that can be earned from it. In this context, it is important to understand that the decision whether to provide Liquidity Protection, and ultimately under what terms if future protocol changes are taken into account, is a per-pool governance decision. It stands to reason that governance will over time ensure that the terms are economically beneficial for BNT holders. This does not preclude an initial loss-making period where the business is grown. This initial period allows everyone to learn how the system behaves "within its natural habitat", especially what is needed to attract liquidity providers into the system.

1. ``

The 3rd point above is not a specific phase-in - it simply relies on the design feature that Liquidity Protection is only available to long-term providers. There is not currently a specific limit in place but there is the possibility to introduce one during the build-up phase.

This is a new system, and whether those limits are sufficient is only that can be ascertained with certainty after the fact. However, they certainly improve the risk position compared to an unrestricted system in an important way.

Conclusion

In this paper we described our understanding of Bancor's v2.1 protocol and presented analysis that in our view is important to understand it.

The context of the protocol is that the space of Automated Market Makers ("AMMs") of which Bancor was one of the first is a highly competitive multi-sided marketplace. The critical participants of the ecosystem are the liquidity providers, and the competition for them is fierce between the competing protocols. Bancor has come up with an, in our view, innovative solution in this space by providing what they call Liquidity Protection to long-term liquidity providers, ie they insure them against Impermanent Loss.

We have shown that Impermanent Loss can be a major impediment for potential liquidity providers to stake their asset in the system, especially if they believe that their assets will outperform the market. Even worse, we have shown that in the case where one token moons whilst the other goes to zero, liquidity provider who contributed their assets to AMMs may lose everything whilst HODLing investors might make substantial returns. Therefore, in our view, Bancor v2.1's value proposition to potential liquidity providers can be very interesting. The fee-earning-potential that this liquidity generates might well exceed the cost of providing such protection, especially in a later stage when the liquidity providers are acquainted with the system and their remuneration might be made less generous. Also, contrary to the *"we pay you tokens to provide liquidity on our platform"* business model so often seen in the AMM market currently, the Bancor protocol seems to have a defensible moat. Even someone copying the entire code of the protocol will not have the risk-taking Bancor protocol in the background, and this risk taking is, in our view, the core of Bancor's unique value proposition.

All the above is a hypothesis yet to be validated. This is a very common situation startups launching a new product. Ultimately, once the protocol is launched there must be a careful analysis of whether the cost to the protocol of providing their services to their multiple customer groups is justified by the fee earnings potential, and/or how it should be tweaked.

If the protocol succeeds, then the potential for growth is substantial. It has been said that stocks may all become tokenized. The entities currently trading those earn billions of dollars in fees, so if this market is up for grabs then some of it may be captured by the successful AMM protocols and the token holders who provide value to the protocols like it is the case for BNT. Moreover, if and when markets for fractionalized investments and other tokens truly take off, then those fractionalized investment tokens need to be traded somewhere, and the leading AMM protocols may well capture a significant portion of this new fee wallet as well.

Appendix 1: AMMs and quantitative finance

Traditional quantitative finance

Brokers, dealers, market makers and exchanges

Before we go into the details let us make a detour to traditional finance to fix some ideas and to define some terminology. For secondary market trading — ie the trading of securities already issued to the market — there are two fundamental intermediation models: *brokers* and *dealers*. The difference between the two is that a broker does not take a proprietary position in the asset traded — they just match buyers and sellers. Dealers on the other hand (also referred to as *market makers*) are willing to trade with the market directly. For illiquid assets this means that dealers need to have a trading inventory because they can only sell what they have. For more liquid assets they have a chance to sell assets first and then hope that they'll find the opposite side before they have to settle the trade two or so days later, so they might be able to do without an inventory.

The largest trading venues in traditional markets are the *exchanges* who organize trading in the high-volume securities, typically using an order book. They are matching buyers and sellers directly and do not run their own book. Using our definition above they are brokers. As an aside, this is one of the areas where traditional finance and DeFi lingo diverges: the term DEX, aka decentralized exchange, can refer to an entity that trades directly with the market, hence would be a dealer or a market maker in traditional lingo, and not a broker or an exchange.

Futures and options

An AMM is a dealer in the traditional lingo, ie an entity that is taking a proprietary position in the assets in which it makes markets because they need a trading inventory. An AMM's position is dynamic, ie it changes subject to market prices even without end-customer trades. As we will see below, the work of Black, Scholes and Merton links options and dynamic trading strategies, so we need to briefly talk about futures and options before we can come back to AMMs and trading strategies.

A *forward contract* is the obligation to exchange two assets at a specific time in the future at a specific "forward" price. So, for example to buy 2 TKN against 1 BNT in a year's time would be a forward contract. A *futures contract* is similar to a forward contract, except that it is traded on an organized exchange and hence it is subject to daily mark-to-market and margining.

A call option contract is the right, but not the obligation, to buy a specific asset at a specific date in the future at a pre-determined "strike" price. A put option contract is the same, but for the right to sell. When drawing the price of a call or a put against the final spot price we get the well-known hockey stick chart. By combining multiple calls or puts — possibly some or all of them short — we can replicate any piecewise linear payoff profile. When using an infinite number of calls and puts we can replicate any smooth payoff function.

One important relationship is the *call put parity* which states that a call minus a put is a forward. As formula:

$$C_K(S) - P_K(S) = F_K(S)$$

where S is the spot price, and K is the strike price of the call, the put, and the forward. The important corollary here is that calls and puts are not different from an option point of view because they only differ by a linear component.

The names that are nowadays most closely linked to option pricing are those of Black, Scholes and Merton. It is a common misconception that they were the first to price options using probability theory and expected payoffs. However, this method had been around for centuries. Their contribution is that they showed that an option can be *hedged*, meaning that its payoff can be replicated, without risk, by buying and selling the underlying asset. This was a game changer as it moved the bar from "I make money on average…" to "I make money every time when I sell an option above its fair value". In practice this is not entirely true because the uncertainty moved into the model parameters, notably the volatility.

The key learning here is the following

> Every final option payoff profile can be replicated using a dynamic trading strategy in the underlying assets, so there is a connection between the option profiles and dynamic strategies. A priori this relationship is one way, but we see that a log of the trading strategies that we are interested in – notably the AMM strategy – can be linked to final profiles.

Greeks and the Black Scholes equation

When we are talking about trading strategies above, we are talking about what is known as *self-financing trading strategies*. In short this means that the value of the strategy only changes because of market moves, but not because of contribution or withdrawal of assets. A self-financing trading strategy can in principle start at any initial value. However, it is often convenient to start at zero and borrow all funds needed. Generally, the assumption here is that both numeraire and risk asset can be borrowed at no frictional cost, and that trades happen at market price without bid/offer spread. We also assume zero interest rates for ease of presentation. This latter assumption might however not be appropriate for all use cases and it needs to be reviewed.

In Black Scholes Merton lingo, the hedge of an option is determined by its *Delta* (or Δ) which corresponds to the amount of risk asset held, denoted in units of the risk asset. It is, in the mathematical sense, the derivative of the option value with respect to the spot price. In other words, it is the best linear approximation of the value we can get. In our case the Delta corresponds to the amount of TKN held, measured in native TKN units. Because the strategy is self-financing, we can track how much numeraire (ie BNT in our case) the strategy holds - it is effectively whatever is in the "current account" after all trades executed. This can be a negative number. The *Cash Delta* is the Delta measure not in units of the risk asset but in units of numeraire, ie it is the Delta multiplied by the spot price. Note that Delta can only change because of trading, not because of market moves. Cash Delta however will change as spot price moves.

The *Gamma* (or Γ) of an option is the change in Delta — ie the change in hedge — with respect to small moves in the spot price. The *Cash Gamma* is the Gamma multiplied with the square of the spot price. Gamma as a number is often really hard to interpret. The interpretation of *Cash Gamma* on the other hand is very intuitive:

> The Cash Gamma is the required adjustment to the hedge portfolio, in terms of the numeraire, for a given percentage move in the spot. For example, a Cash Gamma of 100 BNT means that for every 1% move on the underlying price the hedge needs to be adjusted by buying or selling 100*1% = 1 BNT worth of the asset.

Importantly, the Cash Gamma is also the term that appears in the Black Scholes equation. If we focus on the option term only (or assume zero interest rates and dividends) this equation reads

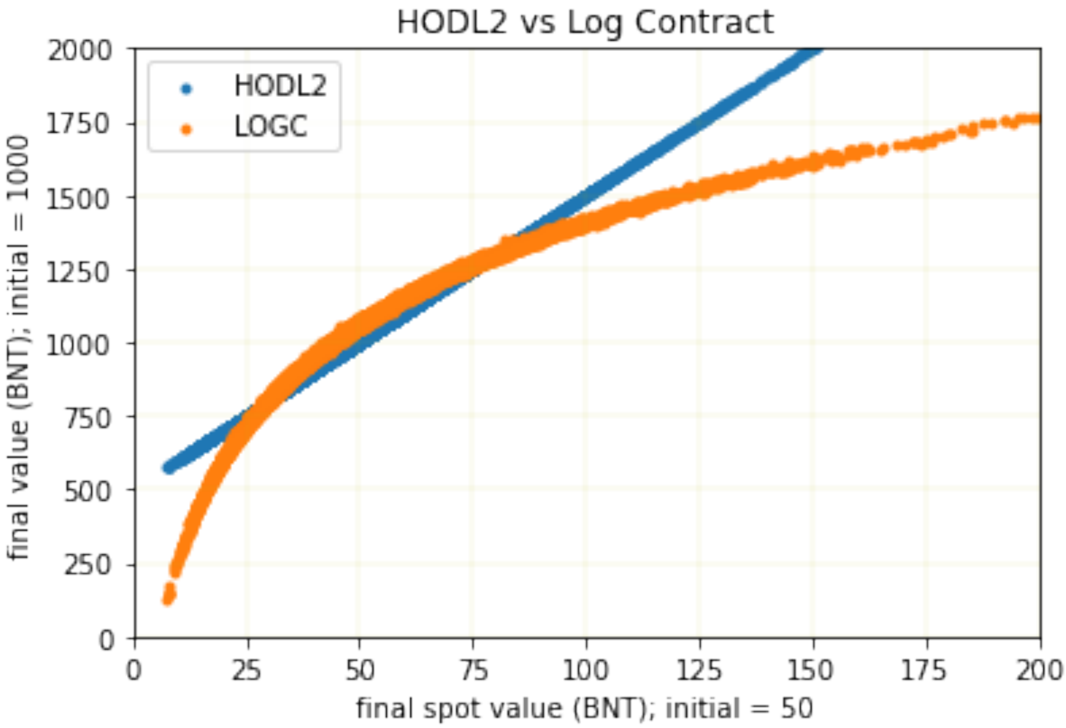
$$\Theta = -\frac{1}{2}\sigma^2 \Gamma_{cash} dt$$

Here Theta (Θ) is the cost (or gain) of running the strategy, or in other words, its fair value. Sigma (σ) is the lognormal volatility of the Brownian motion driving the spot process, and Gamma Cash is the Gamma of the strategy, ie how the risk investment changes with respect to spot moves. The cost (or gain) is entirely related to buying high, selling low or vice-versa whenever the market moves. As Gamma is related to the *convexity* of the option profile (linear profiles like forwards don't have Gamma) the "time decay" Theta is also known as *"convexity gain / loss"*.

The "log contract" trading strategy

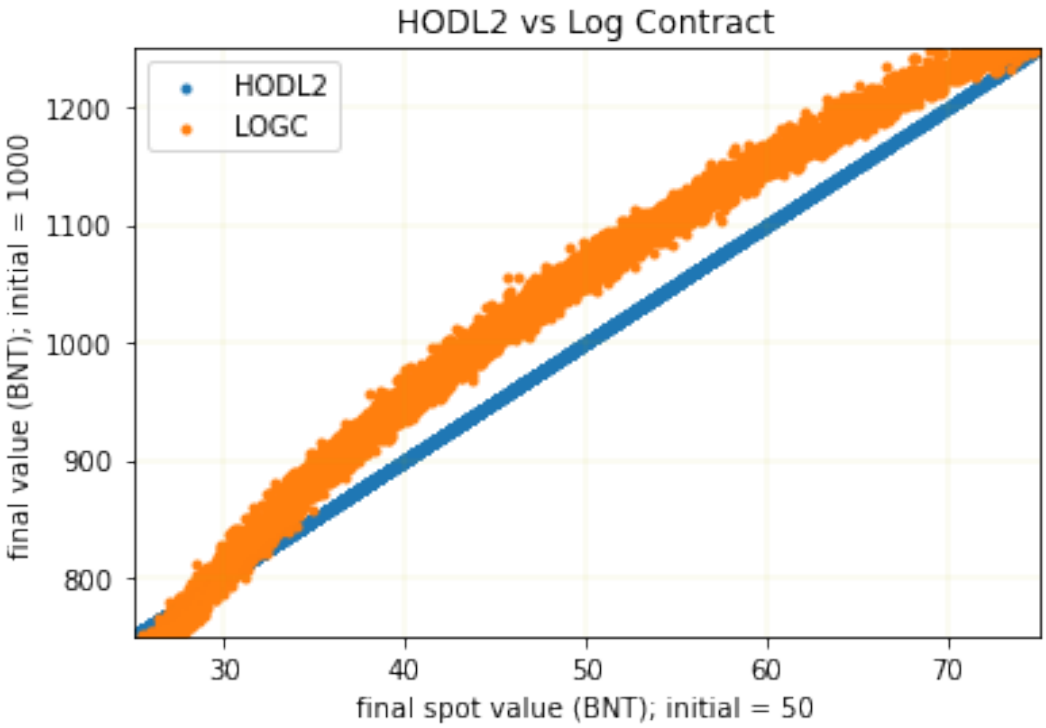
Before we move on to the trading strategy implemented by AMMs we want to briefly discuss the "log contract" trading strategy which is well studied in the quantitative finance world. It ties the important concepts together in way that makes it easier to understand them in the context of AMMs.

The log contract is an option whose final payoff is $\ln S/S_0$ where S_0 is some arbitrary chosen reference spot value, for example the initial value of the spot. The Delta is the derivative of the value with respect to the spot price, which in this case is $1/S$. This is measured in number of TKN, so if we translate it to our numeraire BNT we find that the Cash Delta is $S * 1/S = 1$ BNT. In other words, the dynamic hedging strategy that is replicating the log contract is keeping always the same amount of BNT invested in the risk asset.



Log Contract vs HODL

In the chart above we see a simulated log contract strategy with an initial spot price of 50 BNT and an initial investment of 1000 BNT (500 in BNT and 500 in the risk asset). The x-axis is the final spot price, and the y-axis is the final value of the strategy. The reference strategy is HODL2 which is simply "holding on to the initial investment". Here we see nicely the log shape of the final value, and we also see the log contract outperforms HODL2 in the middle area because of the convexity gains due to its Gamma that allows for buying low and selling high in range trading markets.



Log Contract vs HODL (zoomed)

Here we see the same chart zoomed in to show that whilst the gains on the HODL strategy are deterministic once the final spot price is known, the gains on the log contract strategy are stochastic. This is because different paths ending up at the same spot value can experience different levels of realized volatility and therefore the convexity gains on the Gamma will be different.

Automated market makers as trading strategies

At this stage we have provided the context and framework in which we can analyze AMMs, and in particular the Bancor AMM. In a first step we will focus on the investment-vehicle aspect of AMMs as this is where the Impermanent Loss ultimately stems from. Once we have analyzed this, we will consider the impact of fees in the following section.

AMMs as investment vehicles

As we have laid out above, AMMs are not brokers or exchanges, but they are dealers, ie they are taking a proprietary position vis-a-vis the market. In order to be able to do that they need to hold a trading inventory. In traditional markets the risk associated with a trading inventory can sometimes be mitigated. For example, using risk diversification and derivatives the trading inventory may be hedged, at least on a macro level. Also, in traditional markets with T+2 settlement dealers can often act somewhat like brokers in that they sell assets they don’t own on the assumption that by the time they need to deliver they can buy it in the market. The latter route is not available in a crypto setting where instantaneous settlement is the norm. However, risk diversification and insurance are already possible today — and part of Bancor’s protocol, as we see below - and derivatives markets to hedge macros risk might develop over time.

Having said that, let's ignore this for the time being and let's focus on the fact that to be able to make markets an AMM needs a trading inventory, and this trading inventory is de facto an investment strategy. Bancor v1 was one of the first protocols to implement an invariant-based "$k = x * y$" AMM, and Bancor's v2.1 release still follows this general pattern. The details of those market makers have been described in detail elsewhere, so here we'll only give the most important results.

In a $k = x * y$ pool, the pool smart contract is willing to engage into any trade that keeps the invariant k "invariant", ie the product of the number of tokens it holds remains constant. To give a practical example, a pool holding 100 BNT and 200 TKN (both measured in their own native units) would have a k of $100 * 200 = 20{,}000$. The pool is indifferent between this token composition and any other token composition that yields the same invariant, say 200 BNT and 100 TKN. This means the pool is willing to buy 100 BNT in exchange for 100 TKN which would bring it there. Note however the pool would not trade the other way on the same terms. If the pool has to *buy* 100 TKN then it will have 300 TKN. To keep the invariant constant in this case it must have 66.6 BNT. So, the pool would *sell* 33.3 BNT in exchange for 100 TKN. Different buying and selling prices are a common feature of traditional market making — that's their profit.

In this case we have a price bracket of 0.33/1.00 BNT per TKN which in traditional market maker terms is wide, but this is because the spread depends on size the size of the trade compared to the size of the pool. Trading 100 TKN when the pool only contains 200 TKN is a big trade. For smaller trades the pool's bid/ask spread tightens. Eg for buying/selling 10 TKN the spread is a much more reasonable 0.48/0.53 BNT per TKN.

We note that the initial pool is 100 BNT and 200 TKN and that the bid/ask for very small trades converges towards the pool-implied price, which in this case would be 0.5 BNT for 1 TKN. So, for small trades, the pool always offers the pool implied price, regardless of market conditions. In presence of a market where arbitrageurs can trade at the prevailing price in each direction, they can make a risk-free profit by trading with the market on the one side, and the pool on the other side. The only circumstances where this is not the case is if the pool-implied price and the market price coincide. As a consequence, arbitrageurs will always trade with a pool until the pool-implied price equals the market price.

In our example the initial pool contained 100 BNT and 200 TKN, leading to a pool implied price of 0.5 BNT per 1 TKN. If we express the value of those TKN in BNT we find that their value is 100 BNT. This is not a coincidence, but a simple consequence of the definition of the pool-implied price. In short,

> An AMM pool that is arbitraged against an external market will always contain an equal value in both assets. This is true regardless of the numeraire chosen.

The CRI investment strategy

To summarize what we have found above, a k=x*y AMM pool that is arbitraged against a sufficiently liquid market will at every point in time contain the same value in tokens of either kind. This is true in any numeraire, and in particular in the BNT numeraire, so in particular we find that for every BNT the pool contains $1/p$ TKN where p is the number of BNT for 1 TKN.

We have above discussed the constant-BNT-value “log contract” investment strategy where at every point in time the investor had a fixed amount of BNT invested in TKN. This is similar, except that the strategy is not “invest a fixed amount of BNT” but “split the investment equally between BNT and TKN”. This strategy - which we want to denote as “Constant Relative Investment” or “CRI” - is somewhat softer than the log contract strategy. It keeps a more balanced portfolio between the two assets and therefore shifts less risk around, both on the upside and the downside. It is easy to see that the worst-case downside of the CRI strategy is 0, which is not great, but which is much better than the log-contracts minus infinity.

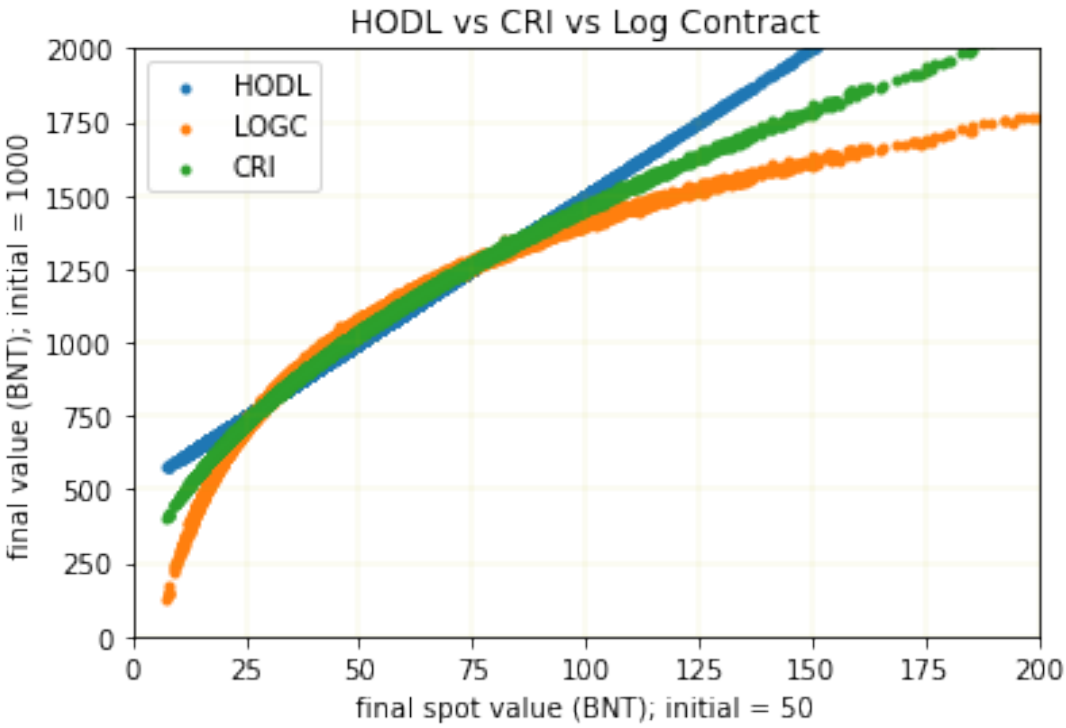
Note that the HODL reference strategy here is not our previous HODL (which we want to call HODL1 now) and which was “invest 1 BNT into TKN at the start and hodl” but it is HODL2 which is “invest 1 BNT into TKN and keep 1 BNT in the current account and hodl”. The maximum downside of HODL2, when looked at it from the BNT numeraire, is 1, and therefore CRI’s 0 is still worse than HODL2. On the upside - and we’ll give this well-known fact without a proof - the portfolio value does not grow like $\log(p/p_0)$ but instead like $\sqrt{p/p_0}$. Square root is better than log, but it is still (much) worse than the linear growth of $1+x$ shown by HODL2.

The CRI investment strategy, like the log contract strategy, generates buy-low-sell-high convexity gains in scenarios where the two assets are range trading. At the same volatility those gains are smaller than that of the log contract strategy, because it has a lower Gamma.

So, to summarize,

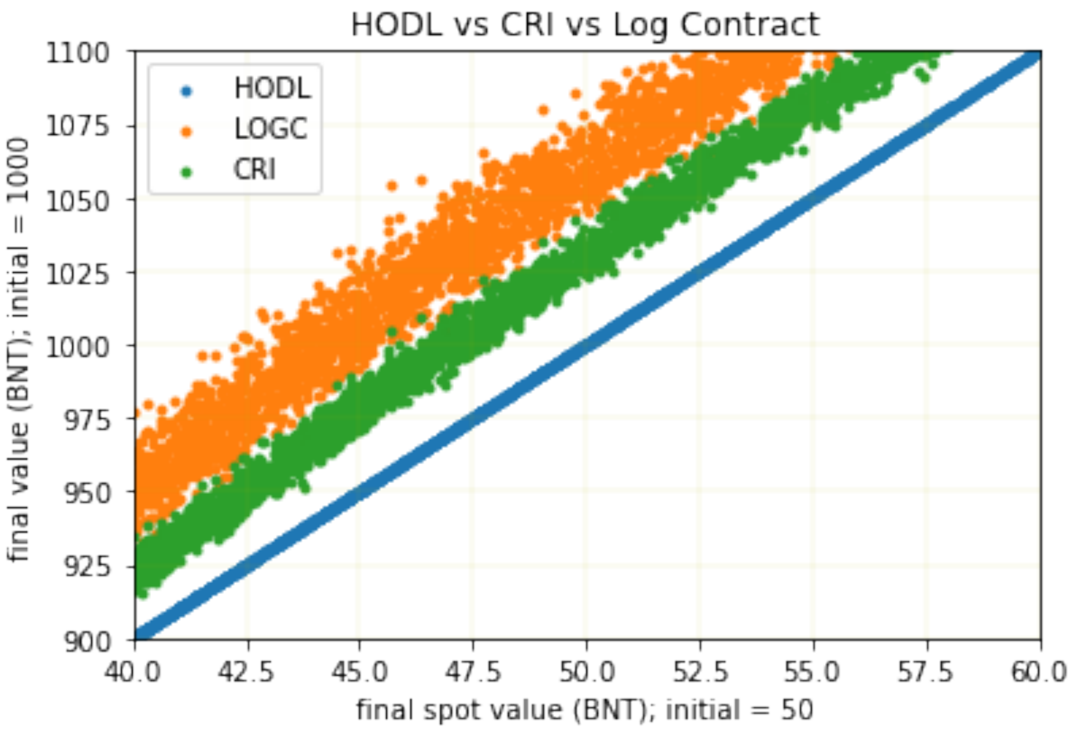
> CGI is like a log contract, except that it trades in less risk in the wings for less gains when range trading. Just like the log contract is tied to the final profile of $\log(p/p_0)$ the CGI strategy is tied to the final profile $2\sqrt{p/p_0}$.

We have redrawn here the log contract charts from above adding the CRI strategy:



HODL vs CRI cs Log Contract

In the view above we see that the CRI result is between the log contract result and the HODL2 result: it loses less at the wings, it gains less in the center.



HODL vs CRI vs Log Contract zoomed

In the zoomed-in view above we see that the CRI strategy like the log contract strategy yields stochastic results due to the stochastic convexity gains.

Arbitrageurs and the AMM investment strategy

We have discussed the CGI strategy as an active investment strategy where trades are executed at the new market price after every move. This is not an adequate description for what happens in an AMM, as the AMM is not actively trading but relies on arbitrageurs to adjust it. Still ignoring fees, an easy but tedious calculation shows that a pool that is arbitraged at a price of p_0 and that is now in an environment where the price is p_1 allows arbitrageurs to trade at the better price $\sqrt{p_0 p_1}$. This is by design to encourage arbitrageurs to trade.

We see that the if the price moves from p_0 to p_1 and back to $p_2 = p_0$ then the pool will trade at the same price upwards and downwards. This is the origin of the term "Impermanent Loss": whenever markets move, the pool suffers a loss as compared to the HODL strategy. However, if ever markets move back to where they started from this loss will be reversed.

The Impermanent Loss is impermanent only against the HODL2 strategy. However the real reference strategy is CRI, and the loss of the AMM pool against the CRI strategy is permanent: the latter makes convexity gains on every roundtrip in the market, but the former pays those convexity gains to arbitrageurs and therefore only takes part in the "impermanent" convexity losses in both wings.

The final value of the AMM strategy is path independent, ie it only depends on the final value of the spot price. If we define $x = p/p_0$ where p_0 is the price of TKN in expressed in BNT at time $t = 0$ and $p = p(t)$ is the same at time t, then our initial portfolio of 1 BNT and 1 BNT worth of TKN will have the following final value

$$AMM(x) = 2\sqrt{x}$$

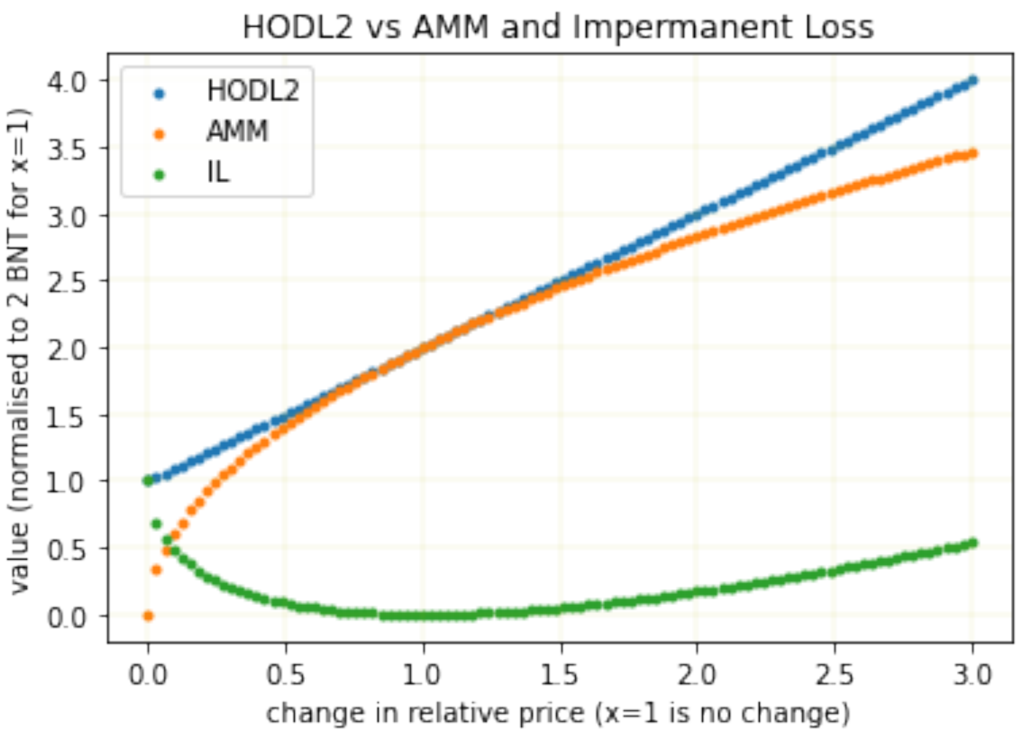
Note that this compares to the value of the HODL2 strategy of

$$HODL2(x) = 1 + x$$

and we see that $AMM(1) = HODL(1) = 2$ and that $AMM(x) < HODL2(x)$ for $x \neq 1$. We define the difference between HODL2 and AMM as the Impermanent Loss

$$IL(x) = HODL2(x) - AMM(x) = 1 + x - 2\sqrt{x}$$

We have drawn the relationship in the chart below:



HODL vs AMM and Impermanent Loss

On the x-axis is the relative price change $x = p/p_0$ and on the y-axis is the value of the HODL2 portfolio, of the AMM porfolio, and the Impermanent Loss, which is the difference between the two, all three in BNT. The normalization of the chart is for an initial portfolio of 1 BNT and 1 BNT worth of TKN, so both strategies' value at $x = 1$ is 2.

To summarize our finding so far

> The AMM investment strategy is similar to the CRI investment strategy, except that (a) the convexity gains when range trading is paid away to arbitrageurs, whilst (b) the losses in the wings (when comparing it against HODL2) are maintained. The value of an AMM pool not charging fees is path-independent and depends only on the final value of the normalized price ratio x where the dependency is in $\sqrt{x}$.

AMMs as fee-earning market makers

So far, we have looked at AMMs purely from an investment point of view, but this is not their primary purpose: their primary purpose is to generate fees for their investors by allowing other market participants to trade. As it is common in this area, we will refer to those investors as "liquidity providers" in what follows.

There are three types of "fees" in the wider sense of the term that a pool's trading customers are paying

- Ethereum gaz fees to get the transaction executed
- Slippage aka implied bid/ask spread
- Fees specifically charged by the contract

Ethereum gaz fees they are currently very high, but economically they are insubstantial from a big picture point of view. The reason is that Ethereum fees do not depend on the transaction size so for large transactions they become irrelevant.

We have already introduced slippage above, and we have found that it can be substantial when the size of the trade gets to the same order of magnitude as the number of tokens available in the pool. One might think that this advantages larger pools, but it turns out that this is not the case: a customer who wants to minimize slippage - and whose trades are big enough that they don't have to care about per-transaction gaz fees - will split their order into smaller pieces and route those pieces to multiple AMMs. But for gaz costs, a set of small but otherwise identical pools performs exactly like one bigger pool aggregating all of them. So, slippage is what it is, and it mostly depends on the amount of tokens that liquidity providers contribute to the various pools that are trading either the cross in question, or at least one leg of the cross that can be combined with another leg to the desired trade.

The last cost is "fees specifically charged by the contract". They can either be fixed or percentage or both, but with the same argument as with gaz fees it is only the percentage fees that matter in the big picture. The question of those fees is also who gets them – notably the liquidity providers or the protocol – which we will discuss in the section the competitive situation just below.

Dilution and fundamentally-valued vs momentum assets

A lot of the Bancor v2.1 protocol hinge on the ability by the network to mint and burn BNT in the process of managing the liquidity pools. We will look at this what this means from an economics point of view, and especially for the token economics of BNT.

If a token like BNT is backed by fixed pool of assets – along the lines of an asset backed stable coin – the economics is very easy: the overall market capitalization of the token should be that of the "collateral" asset backing it. If it is not immediately exchangeable there can be a discount or even a premium, for example because of concerns about safety, or because of convenience considerations, but by and large the market capitalization should match that of the backing. In particular the impact of dilution should be straight forward: if there are an additional say 10% of tokens issues without increasing the pool, then their value should drop to $1/1.1 \sim 91\%$.

Popular assets in finance are "company shares" which are securities which receive certain discretionary cash flows called "dividends", have some governance rights, and that in the wind-up of the company have the residual claim on its assets. For an established company shares are by and large in the "asset backed" category, except that the asset in this case is not "gold in a safe", but the company's ability to generate cash. In this case the dilution rule should still apply, and by and large this is the case. For start-up companies however that can be different, one famous episode being the recent Tesla stock split where the split significantly increased the company's market capitalization because the price did not adjust as it was expected to adjust.

Tesla is what is known as a "momentum" stock, ie a stock that is less valued on its ability to generate future cash flows, but more on the ability to find someone else to sell it to at a higher price. The most famous of all momentum assets is gold which trades largely detached from its valuation as an industrial commodity. Another important momentum asset is Bitcoin, as are many other crypto assets including Ethereum.

Having said this, Ethereum might be turning itself into a fundamentally value asset at one point, just as Tesla might. The reason in Ethereum's case is Ethereum 2.0's staking mechanism which is something that can generate cash and therefore can be valued from a fundamental point of view. BNT is like Ethereum in the twilight zone between being an asset that is currently valued mostly on a momentum basis, but that because of the staking and governance attached to it might be susceptible to a fundamental valuation at one point.

The key learning from this discussion is the following:

> If a fundamentally asset suffers dilution, then its price will adjust so that overall market capitalization remains the same. For momentum assets this is not necessarily the case. For them dilution – especially dilution that does not impact current market – might result in smaller price moves, or no price moves at all.

Appendix 2

Formulas

In our framework we have two assets, a risk asset we denote as *TKN*, and a numeraire asset we denote as *BNT*. The choice of risk and numeraire asset is arbitrary and whilst it effects how we express the results it does not affect the substantive results.

In this world, all prices are expressed in terms of the numeraire asset *BNT*. In particular p is the price of the risk asset *TKN* expressed in units of *BNT*, ie it costs p *BTN* to purchase 1 *TKN*.

The normalized price ratio $x = x(t)$ is

$$x = p/p_0$$

where $p = p(t)$ is the price at an arbitrary time $t > 0$ and $p_0 = p(0)$ is the price at time $t = 0$.

When we are now looking at investment strategies, we normalize not only the prices, but also the initial investment portfolio. More specifically, we normalize the value of the initial investment portfolio to 2. The two main trading strategies we considered in relation to AMMs were *HODL* (also referred to as *HODL2* because it hodls 2 assets) and *CRI*. In HODL2 the initial investment is 1 unit of BNT and 1 BNT worth of TKN and there is not further trading. In *CRI* ("Constant Relative Investment") the initial portfolio investment is the same, 1 unit of BNT and 1 BNT worth of TKN. However, whenever the market moves the portfolio is adjusted so that the BNT-value of the BNT position equals the BNT value of the TKN position. Note that this condition is numeraire-invariant: if the BNT value of the two positions is the same then it is the same in any other numeraire, say the USD.

The value of the *HODL* strategy is

$$HODL(x) \equiv HODL2(x) = 1 + x$$

The value of the *CRI* strategy is

$$CRI(x) = 2\sqrt{x} + CG$$

where CG are the convexity gains of that strategy, ie the money that is being made on buying low and selling high whenever the market is range trading. In the *AMM* strategy the convexity gains are paid away to the arbitrageurs, and we find

$$AMM(x) = 2\sqrt{x}$$

Note that $AMM(x)$ is equal to $HODL(x)$ at $x = 1$. This is not as trivial as it sounds as $x = 1$ does not necessarily mean $t = 0$. This is where the notion of *Impermanent Loss* comes from: whenever prices go back to their initial ratio then the value of the *AMM* portfolio is the same as the one of the *HODL2* portfolio. For other values than $x = 1$ we find that $AMM(x)$ is strictly inferior to $HODL2(x)$. This leads us to formally define the Impermanent Loss IL as

$$IL(x) = HODL2(x) - AMM(x) = 1 + x - 2\sqrt{x}$$

where we chose a throughout positive sign for IL.

We define the *Impermanent Loss Attributions* to the numeraire BNT and to the risk asset TKN respectively as

$$IL_B(x) = \frac{1}{1+x} IL(x) = \frac{1 - 2\sqrt{x}}{1+x}$$

and

$$IL_T(x) = \frac{x}{1+x} IL(x) = x\frac{1 - 2\sqrt{x}}{1+x}$$

Evidently, we have

$$IL_B(x) + IL_T(x) = IL(x)$$

We also define the positive and negative branches of the Impermanent Loss as

$$IL^+(x) = \Theta(x-1) * IL(x)$$

for the positive branch, and

$$IL^-(x) = \Theta(1-x) * IL(x)$$

where Θ is the Heaviside step function that is 0 for $x < 0$ and 1 for $x \geq 0$. By construction the support of IL^+ is the positive numbers, that of IL^- is the negative numbers, and they add up to IL.

We define the four possible combinations of $IL_{B/T}^{+/-}$ in the natural manner and note that again they add up to IL.

Invariants

AMMs work by way of an "invariant"

$$k = x * y$$

What this means is that here x, y are the respective amounts of the two tokens in the pool, measured in their own native units. Note that x is not the same x that is denoting the price.

This is unfortunate, but we want to stick to the usual notations in this paper. We will rarely use x in the pool invariant meaning, and if we do, we will be very clear about this. The number k is the *invariant* that the pool maintains when trading. In other words, ignoring fees the pool is willing to engage into any trade with the token it holds provided that

$$x_1 * y_1 = x_0 * y_0 \equiv k$$

where the indices 0,1 indicate the respective values pre and post trading respectively.

If $k = x * y$ is an invariant, so is any function $f(k) = f(x * y)$. A useful invariant in this context is

$$\bar{k} = \frac{\sqrt{x * y}}{N}$$

The quantity N tracks the number of tokens contributed to the pool and it is chosen such that $\bar{k}$ remains constant after pool contributions and withdrawals. The square root here makes for nicer scaling properties which allow in particular to allow to obtain the following identity

$$\frac{\bar{k}_1}{\bar{k}_0} = 1 + \phi$$

where $\bar{k}_1$ and $\bar{k}_0$ are the values of $\bar{k}$ at times $t = 0$ and $t = 1$ respectively, and ϕ is the percentage fee the pool earned during that period (more precisely, ϕ is the variation of pool value that can not be explained by contributions and withdrawals).

Alternative liquidity protection

Below is an alternative liquidity protection mechanism. It differs in that whilst the investors' liquidity is protected, the first layer of protection is the fees. Mathematically, if the investor chooses to withdraw then as single asset provider, they get

$$AMS_{LP}^{P} = \left(x + \max\left(x \frac{2\sqrt{x}}{1+x}(1+\phi) - x, 0 \right) \right) \cdot N$$

where ϕ is the fee accrued to the pool tokens as a percentage of their notional value. The corresponding formula for BNT-only contributions is

$$AMS_{LP}^{P} = \left(1 + \max\left(\frac{2\sqrt{x}}{1+x}(1+\phi) - 1,0 \right) \right) \cdot N$$