WunderEconomics

WunderTeam

February 23, 2022, Berlin

Contents

1 Lösungsideen

Smart Markets for Stablecoins
  Token Engineering Research
  A Token Engineering Process

- Staken von Sub-Projects.
  - Teilprojekt wird nach **Bonding-Curves-Modell** implementiert und bekommt damit seinen eigenen Token.
  - Die Projekteinlage erfolge in WUNDER-Tokens (Staking).
  - Investoren von WUNDER hätten damit die Möglichkeit, die für sie besonders interessanten Projekte stärker zu unterstützen als lediglich das übergeordnete WunderPass-Projekt.
  - Der WUNDER bekäme damit einen intrinsischen Wert: Man braucht ihn, um sich an den Teilprojekten zu beteiligen.
  - Teilprojekte könnten outgesourcet und ausschließlich mittels einer größeren WUNDER-Einlage in den Contract des neuen Projekts incentiviert werden. Die Voraussetzung dafür wäre die Einbindung des neuen Projekts und seines Tokens in das WunderPass-Ökosystem und die Nutzung der Wunder-Identity.

2 Einbindung der Investing-Pools

- Das Pool-Projekt wird als **Curation Market** implementiert und bekommt seinen eigenen Token (IPT).
- Der IPT wird mittels **(Augmented) Bonding-Curves** implementiert, ist also gegen eine Einlage für jeden und immer mintbar.
- Die Einlage für den IPT ist in WUNDER zu erbringen (Es ist noch unklar, wie man an WUNDER kommt, wenn es vorher keinen Token-Sale gegeben hat. Ob der WUNDER ebenfalls mittels Bonding-Curves abzubilden wäre, sei hier erst einmal mehr als unklar.)
- Der erste und größere Investor für das Pool-Projekt wäre WunderPass selbst. Für die erfolgte Einlage in den Projekt-Pool bekäme WunderPass IPT, die es für Incentivierungen und Rewards für die Nutzung von Pools verwenden könnte. Dieses Invest könnte (im Gegensatz zu den Einlagen anderer Investoren) zB. auch einem Locking unterliegen, um eine gewisse Preisstabilität des IPS zu gewährleisten.

- Der Pool-Initiator müsste bei der Pool-Eröffnung IPT staken, die er unter bestimmten Umständen verlieren könnte, wenn sein Pool zB. ungenutzt bleibt. So könnte man sicherstellen, dass ernste Absichten hinter den Pools stecken und diese auch genutzt werden.
- Der Initiator wäre damit gleichzeitig auch Investor in das gesamte Pool-Projekt (da er ja für die Poolerstellung IPT kaufen muss).
- Gleichzeitig müsste der Initiator jedoch auch für sein Staken (ins Risiko gehen) belohnt werden, falls der Pool läuft und genutzt wird. Diese Belohnung würde in Form von zusätzlichen IPT (Stake-Rewards) erfolgen und z.B durch WunderPass und/oder den anderen Poolteilnehmern als eine Art Gebühr getragen werden und dabei folgenden Faktoren folgen:
  - Pool-Lifetime
  - Anzahl Teilnehmer
  - Pool-Einsatz/-Umsatz
  - etwaiger Gewinn aus Invests
  - NFT-Pass-Status
  - Upvoting durch andere IPT-Holder (als ein Art *Master Pool-Creator*)
- In jedem Fall sollte der Staker im Normalfall (falls er nicht irgendwie Scheiße baut) bei der Auflösung des Pools mindestens seinen Einsatz zurückerhalten (also keinerlei Gebühren für die Nutzung des Pool-Service zahlen). In aller Regel sollte er mit mehr als dem ursprünglich gestakten Betrag rausgehen.
- Der nötige Staking-Betrag könnte fix pro Pool sein oder aber variabel und dabei von folgenden Kriterien abhängen:
  - geplante Pool-Lifetime
  - Anzahl Teilnehmer (min/max)
  - Pool-Einsatz pro Teilnehmer (min/max)
  - etwaige abgegeben Garantien seitens Pool-Creator (*der Pool muss mindestens x, y und z erfüllen...*, bei deren Verfehlungen der Staker bestraft und im Erfolgsfall besonders entlohnt wird)
  - NFT-Pass-Status
  - Reputation in der Community (als ein Art *Master Pool-Creator*

  Die entscheidende Frage beim zu entrichtenden Stake-Betrag, ist die Klärung, ob es im Interesse des Stakers (Pool-Creator) sei, besonders viel (um größere Staking-Rewards zu erhalten) oder besonders wenig (um kein Risiko zu tragen) zu staken / staken zu müssen.

- Ein weiterer sehr essenzieller Faktor für die Größe des zu stakenden Betrags könnte der Kurs des IPTs sein. Denn laut der **Bonding-Curves**-Implementierung würde der IPT-Preis mit steigender Zirkulation steigen, was mit der Zunahme von existierende Pools geschähe. Damit wäre die Erstellung neuer Pools mit ihrer zahlenmäßigen Zunahme stets kapital-intensiver (aber nicht gleichbedeutend teurer). **Die Frage hierbei ist also, ob der zu erbringende Stake des Pool-Creators auf den *Total-Supply des IPTs* normiert werden sollte oder nicht**, die gänzlich mit der obigen Fragestellung einhergeht, ob der Pool-Creator eigentlich staken möchte oder das nur tun muss.
  - Gegen eine Normierung spricht die Annahme/Hoffnung, ein Pool-Creator sei gleichzeitig auch ein großer Supporter des gesamten Projekt und glaube daran. Wenn der IPT-Preis steigt, ist dies gleichbedeutend mit der Zunahme an genutzten Pools, an denen der Pool-Creator als Staker, Besitzer von IPT und damit Projekt-Investor auch selbst (finanziell) profitiert.
  - Für eine Normierung spricht dagegen die potenzielle Gefahr, neue oder bestehende User durch eine zu hohe finanzielle Sicherheitseinlage davon abzuschrecken neue Pools zu erstellen.

  Die Antwort auf diese Fragestellung könnte auch darin liegen, ob wir uns besonders viele oder lieber weniger aber besonders Teilnehmer-starke Pools wünschen.

- Alle anderen Pool-Teilnehmer müssen eine Gebühr für ihre Teilnahme am Pool (und die Nutzung des Service) erbringen. Auch das hat in IPT zu erfolgen. Ob die Gebühr bei Pool-Beitritt gewissermaßen als *prepaid* zu erbringen ist oder aber *on demand* für eine anfallende Aktion bleibt zunächst unklar. Die Gebühren könnten sich nach folgenden Faktoren bzw. Features richten und könnten sowohl voraussehbar sein (dann beim Pool-Beitritt zu entrichten) als auch *on demand* anfallen:
  - pro Zeiteinheit (Vorauszahlung für einen gewissen Zeitraum als prepaid; danach Zahlungsaufforderung um im Pool zu bleiben
  - abhängig vom Einsatz (multiplikativ zum ersten Punkt)
  - abhängig vom etwaigen Gewinn aus Invests (on demand)
  - abhängig vom Pool-Creator (Community-/Staking-Status als Invest-Guru; prepaid)
  - bei Aufstockung des Invests (on demand)
  - bei Vorzeitigem Ausbezahlen und Verlassen des Pools (on demand)
  - gekoppelt an Beteiligung am Staken (prozentual auf die vorigen Punkte anzurechnen)
  - abhängig vom NFT-Pass-Status (prozentual auf die vorigen Punkte anzurechnen)

- Die Teilnehmer können bei dieser Logik aber nicht wie nicht wie die Staker zusätzlich als Projekt-Investoren angesehen werden, weil sie IPTs kaufen, da die gekauften

IPTs direkt als Gebühr entrichtet werden. Für die Pool-Teilnehmer stellt der IPT also eher einen Utility- bzw. Purpose-Token dar weshalb die Höhe der zu entrichtenden Gebühr zweifelsfrei auf Basis von *Total-Supply des IPTs* normiert werden muss (die Gebühr darf keinesfalls mit Zunahme von Pools steigen).

- Die entrichteten **Gebühren gehen zu einem relevanten Teil in die Treasury des gemeinschaftlichen Investing-Pools-Contracts** und stellen damit eine gemeinschaftliche Projekt-Erwirtschaftung dar. Der verbleibende Teil der Gebühren geht an den Pool-Staker. Die Aufschlüsslung der Verteilung auf Project-Treasury und Pool-Staker könnte halbwegs komplex werden und folgende Festlegungen folgen bzw. Gegebenheiten berücksichtigen:
  - Verteilung nach einem simplen prozentualen Schlüssel (zB. 50-50)
  - Absolute Mindest- und Obergrenzen des Projekt-Pool-Anteils (mindestens Betrag x geht an den Projekt-Pool; wenn es nicht reicht, alles; ab der Mindestgrenze erfolgt eine prozentuale Verteilung bis zu einer Maximalgrenze y für den Projekt-Pool; alles darüber geht an den Staker)
  - progressive Verteilung abhängig des erbrachten Staking-Betrags (so könnte der Staker pro gestaktem IPT einen prozentualem Anteil $x \in [0;1]$ pro IPT an Gebühren für sich beanspruchen, wobei das x mit Größe des gestakten Betrags progressiv stiege)
  - Begünstigung des Stakers in Abhängigkeit seines NFT-Pass-Status.
- Folgende Auswahl sollte vermutlich bei der Pool-Erstellung angeboten werden:
  - [Pool-Creator erbringt den Stake; alle anderen Teilnehmer bezahlen die Gebühren]
  - [Alle Pool-Teilnehmer teilen sich den zu erbringenden Stake und alle anfallenden Gebühren]
- Bedingt durch den Gebühren-Mechanismus erwirtschaften das Pool-Projekt Einnahme für die gemeinschaftliche Pool-Treasury, womit auch der IPT auf natürliche Weise im Wert steigt (ohne dass neue Investoren hinzukommen müssen, die einen höheren Tokenpreis bezahlen müssen). Jeder IPT-Holder - also auch insbesondere die Pool-Staker - profitiert also an der Erstellung neuer Pools (der Staker also indirekt an seinem eigenen Pool als auch an den fremden, was additiv zu seinen direkten Stake-Rewards hinzukommt). Das fördert also Word-of-Mouth, was sowohl auf die Preissteigerung des IPTs durch neue IPT-Holder einzahlt, als auch die Pool-Treasury durch neue Pools und die dafür anfallenden Gebühren füttert, was wiederum den IPT-Kurs befeuert.
-

3 Bonding-Curves

- Gute Einführung
- Anwendungsbeispiel
- White-Paper
- Smart-Contract

Zunächst einmal eine Formalisierung einer Token-Distribution mittels Bonding-Curves:

Definition 1: Token-Distribution mittels Bonding-Curves

Angenommen man möchte einen Projekt-Token **TKN** herausgeben und dieses im Markt distribuieren. Der Mechanismus der *Bonding-Curves* stellt hierbei ein alternatives Modell zu gängigen Tokensales (z.B. ICO) dar und folgt dabei einigen wesentlich Merkmalen, die ihn teils grundlegend von herkömmlichen Tokensales abgrenzen.

- TKN wird von einem Smart-Contract verwaltet, der wesentlich mehr Logik implementiert als ein herkömmlicher ERC20-Contract.
- TKN kann jederzeit und von jedem gemintet werden. Dies geschieht gegen eine Einlage/Bezahlung in einer dafür definierten Währung (z.B. ETH oder USDT). Der Token wird quasi von dem Verwalter-Contract verkauft.
- Es existiert damit keine initiale bevorzugte Token-Ausgabe beim Contact-Launch an etwaige bevorzugte Parteien (Contract-Owner, Herausgeber, Investoren etc.). Die Ausgabe erfolgt ausschließlich gegen Einlage und kennt keine Bevorzugung entgegen der Contract-Logik.
- Die Einnahmen aus der Tokenausgabe kommen ausschließlich der Token-Contract-Treasury $\mathcal{T}$ zugute anstatt wie bei herkömmlichen Tokensales bestimmten Begünstigten (wie z.B. der Herausgeber-Company oder deren Gründern).
- TKN unterliegt keinem maximalen Gesamt-Supply. Es können stets neue Tokens ausgegeben werden, solange Interessenten existieren, die die Einlage für die Token-Ausgabe erbringen.
- Tokens können jederzeit von ihren Besitzern gegen einen - einer bestimmten Contract-Logik folgenden - Rückkaufpreis an den Token-Contract zurückgegeben werden. Zurückgegebene Tokens werden dabei sofort von dem Verwalter-Contract geburnt und somit aus der Zirkulation genommen.

- TKN kann selbstverständlich auch am Sekundärmarkt gehandelt werden (falls dieser bessere Konditionen hergibt als die Aussage bzw. Rücknahme durch den Token-Contract selbst).

Sei $i \in \mathbb{N}$ der aktuelle Gesamt-Supply von TKR (wir nehmen hier mal an, TKR sei atomar) und **$** die Tausch- bzw. Einlage-Währung (**$** ist hier abstrakt und nicht als US-Dollar zu verstehen).

Dann werden die durch die Token-Contract vorgegebenen Ausgabepreis (Kaufpreis) $\mathcal{K}$, Rücknahmepreis (Verkaufspreis) $\mathcal{V}$ und Contract-Treasury-Inhalt $\mathcal{T}$ für den zuletzt ausgegebenen Token i - jeweils in der Einheit **$** - durch die jeweils supply-abhängigen Funktionen beschrieben:

$$
\begin{aligned}
&\mathcal{K}, \mathcal{V}, \mathcal{T} : \mathbb{N} \to \mathbb{Q}^{+} \\
&\quad \mathcal{K}(i) := \text{ Letzter Token-Ausgabepreis in \$ bei einem Gesamt-Supply von i} \\
&\quad \mathcal{V}(i) := \text{ Aktueller Token-Rückkaufkurs in \$ bei einem Gesamt-Supply von i} \\
&\quad \mathcal{T}(i) := \sum_{j=1}^{i} \mathcal{K}(j)
\end{aligned}
$$

Die definierende Logik unseres Tokens lässt sich damit also formal als

$$TKR = (\mathcal{K}, \mathcal{V}, \$)$$

schreiben, wobei hierbei $\mathcal{T}$ ausgespart bleibt, da es implizit durch $\mathcal{K}$ gegeben ist.

Sicherlich können und werden bei einer konkreten Implementierung eines mittels der durch $\mathcal{K}$ und $\mathcal{V}$ gegebenen *Bonding-Curves* beschriebenen Tokens noch andere zu formalisierende Faktoren und Mechanismen eine Rolle spielen. Für die simpelste abstrakte Definition reichen die genannten Größen jedoch für den Moment aus.

Die eben - auf diskrete Weise - definierten Funktionen $\mathcal{K}(i)$ und $\mathcal{V}(i)$ erfordern insofern noch eine zusätzliche Bemerkung, als dass diese explizit nur eine Token-weise Auskunft über Ausgabe- und Rücknahmepreis geben. Möchte man mehrere Token minten oder zurückkgeben, muss der Preis für jeden der Tokens separat ausgerechnet und anschließend addiert werden. Möchte man bei einem aktuellen Supply von $i \in \mathbb{N}$ nicht einen sondern $k \in \mathbb{N}$ mit $k \leq i$ Tokens minten bzw. zurückgeben, beläuft sich der gesamte Kauf- bzw- Verkaufspreis auf

$$\mathcal{K}_k(i) := \sum_{j=i+1}^{i+k} \mathcal{K}(j)$$

$$\mathcal{V}_k(i) := \sum_{j=i-k+1}^{i} \mathcal{V}(j)\,.$$

Das besonders Hervorhebenswerte an diesem Token-Ausgabemodell ist zweifelsfrei die gemeinschaftliche aus der Token-Ausgabe gefütterte Contract-Treasury aus echten Geldeinlagen, die nicht etwa einer dritten (Ausgabe-)Partei zugute kommt, sondern de facto den Tokeninhabern gehört. Die Existenz dieser Rücklagen gibt den ausgegebenen Tokens theoretisch einen realen Wert und ermöglicht einzig und allein die Implementierung des Rückkauf-Mechanismus. Der Gebrauch von dieser Möglichkeit und die Verankerung der Rückkauffunktion $\mathcal{V}$ in der Logik des Token-Contracts realisiert den besagten realen Wert dann auch in der Praxis und nennt sich ***"market maker of last resort"***. Denn wenn ich eine definitive - in Contract-Logik verankerte - Sicherheit habe, ein Asset jederzeit verkaufen zu können, besitzt dieses Asset auch einen echten, intrinsischen Value, der nicht zwingend den marktwirtschaftlichen Mechanismen unterliegt - und somit auch keinen etwaigen Hypes um einen gut vermarkteten Tokensale ohne dahinterliegende Substanz. Vielmehr folgt der Tokenpreis der gemeinschaftlichen Projekt-Treasury $\mathcal{T}$, die ihrerseits substanziell mit dem Projekterfolg einhergeht.

Die letzte Einsicht lässt uns zu zwei wesentlichen Gedanken gelangen, die die entscheidenden Argumente für das *Bonding-Curves*-Modell liefern könnten:

- Der Rückgabepreis $\mathcal{V}(i)$ sollte eine direkte Abhängigkeit vom Treasury-Inhalt $\mathcal{T}(i)$ aufweisen.

- Nach bisheriger Definition hängt der Treasury-Inhalt $\mathcal{T}(i)$ ausschließlich vom aktuellen Supply $i \in \mathbb{N}$ (und den damit einhergehenden Ausgabepreisen $\mathcal{K}(j)$ für $j \leq i$) ab. Gepaart mit der ersten Forderung bedeutete dies implizit nichts anderes, als dass der aktuelle Rücknahmepreis ausschließlich von den Ausgabepreisen der bisherigen Tokens abhinge. Dies ist schlecht und ein sehr großes Problem der gängigen *Bonding-Curves*-Implementierungen, da Koppelung des Rücknahmepreises - also des intrinsischen Werts des Tokens - ausschließlich an den Kaufpreis voriger Tokens - und die Wertentwicklung damit an den Kaufpreis etwaiger zukünftig ausgegebener Tokens, würde mathematisch alternativlos eine monoton steigende Ausgabepreis-Funktion $\mathcal{K}(i)$ erfordern. Ohne eine sehr stark fundierte projekt-bezogene Argumentation für ein monoton steigendes $\mathcal{K}(i)$ schrie das gesamte Modell nur so nach *Pump & Dump* und *Hot Potatoe*. Und tatsächlich ist es so, dass nahezu alle *Bonding-Curves*-Implementierungen Gebrauch von einer (streng) monoton steigenden Ausgabepreis-Kurve $\mathcal{K}(i)$ machen. Sie argumentieren mit anderem generierten Projekt-Value, der nicht durch die Contract-Treasury $\mathcal{T}(i)$ gemessen werden kann und diese Argumentation muss nicht zwingend falsch oder ungenügend sein. Uns reicht dies aber nicht - zumal es mehr als gute Gründe für ein monoton steigendes $\mathcal{K}(i)$ gibt (dazu später mehr). Somit bleibt uns nichts anderes als die - zumindest teilweise - Abkoppelung von $\mathcal{T}(i)$ und $\mathcal{K}(i)$, womit wir auch unsere obige Definition von $\mathcal{T}(i) = \sum_{j=1}^{i} \mathcal{K}(j)$ wieder teils verwerfen müssen.

Wir fassen zusammen:

Conclusion 1: Contract-Treasury als wichtigster Baustein zum Erfolg

Wie sind der Überzeugung, der Contract-Treasury-Inhalt - gemessen als $\mathcal{T}(i)$ - sei der entscheidende Baustein für einen soliden *Bonding-Curves*-Token. $\mathcal{T}(i)$ beeinflusst direkt den Rücknahmepreis $\mathcal{V}(i)$, verleiht dem Token damit einen echten geldwerten Value, was wiederum als Kaufargument für neue Tokens gilt und damit implizit auch zur Beurteilung des Ausgabepreises $\mathcal{K}(i)$ seitens etwaiger neuer Investoren hinzugezogen wird.

Konkret auf den Rücknahmepreis $\mathcal{V}(i)$ bezogen sehen wir kaum sinnvollere Alternativen als der gängigen Definition

$$\mathcal{V}(i) = \frac{\mathcal{T}(i)}{i}$$

zu folgen, was gleichbedeutend damit ist, dass der Besitz am Contract-Treasury-Inhalt pro rata auf die sich in Zirkulation befindenden Token verteilt wird, was sich konsequenterweise im Rücknahmepreis $\mathcal{V}(i)$ widerspiegelt. Mit der in Definition 1 beschriebenen Treasury-Funktion $\mathcal{T}(i)$ ergibt sich damit für den Rücknahmepreis $\mathcal{V}(i)$

$$\mathcal{V}(i) = \frac{\mathcal{T}(i)}{i} = \frac{\sum_{j=1}^{i} \mathcal{K}(j)}{i}.$$

Um einen Kauf bei aktuellem Supply von $i \in \mathbb{N}$ zu dem Preis von $\mathcal{K}(i)$ für sich als Investor zu rechtfertigen, muss man argumentieren, man könne den gekauften Token irgendwann zu einem höheren Preis wieder zurückgeben:

$$\exists k > i, \text{ so dass } \mathcal{V}(k) > \mathcal{K}(i)$$

$$\Leftrightarrow \sum_{j=1}^{k} \mathcal{K}(j) > k \cdot \mathcal{K}(i)$$

Gleichzeitig sollte $\mathcal{V}(i) \leq \mathcal{K}(i)$ für alle Supplies i selbstverständlich angenommen werden können, da sonst Arbitrage entstünde, was sofort vom Markt aufgefressen werden würde.

Solche Anforderungen gehen alternativlos mit einem zwingend monoton steigenden $\mathcal{K}(i)$ einher ('monoton steigend' wäre hierbei noch zu präzisieren, da es nicht zu hundert Prozent dem mathematischen Verständnis gleicht und die Aussage wahrscheinlich noch zu beweisen; intuitiv ist es aber klar). Da eine zwingend monoton steigende Preiskurve als Investitionsmotivation - in einem abstrakt stehenden Kontext und ohne zusätzliche Argumente - schlichtweg unseriös ist, fordern wir für den *Contract-Treasury-Inhalt*

$$\mathcal{T}(i) > \sum_{j=1}^{i} \mathcal{K}(j),$$

bzw.

$$\mathcal{T}(i) = \sum_{j=1}^{i} \mathcal{K}(j) \ + f(t,i) \text{ mit } f(t,i) > 0,$$

wobei $f(t,i)$ eine nicht genau präzisierte, positive *Value-Funktion* unseres Projekts darstellt. Also so eine Art Gradmesser der (externen) Wertschöpfung/Wirtschaftlichkeit unseres Projekts, die nicht in direktem Bezug zum Projekt-Kontrakt steht. Man könnte $f(t,i)$ vielleicht ***Of-Contract-EBIT*** unseres Projekt nennen - wie auch immer dieses erwirtschaftet wird.

Wie durch das t angedeutet, bringt das $f(t,i)$ die zeitliche Dimension in unsere *Contract-Treasury*-Rechnung, die externen (wirtschaftlichen) Einflüssen unterliegt und nicht mehr ausschließlich vom Gesamtsupply i abhängt - gleichwohl der Gesamtsupply i durchaus auch die genannten externen Einflüsse und damit auch $f(t,i)$ begünstigen kann.

Der *Of-Contract-EBIT* muss zwar nicht, kann aber durchaus auch aus anderen Smart-Contracts fließen. Solche Inter-Contract-Geldflüsse sind natürlich - falls möglich - eine stets bevorzugte Variante.

Ist dies nicht möglich - und etwaige finanzielle Projekteinnahmen tatsächlich gänzlich *off-chain*, bedarf es eines definierten und vertrauensvollen Mechanismus, der dafür sorge, dass die erzielten Projekterträge in die gemeinschaftliche Projekt-Treasury eingezahlt werden. Dies könnte entweder durch eine gesonderte Contract-Function dargestellt werden, oder aber durch den allgemeingültigen Weg mittels Tokenkäufen. Im zweiten Fall würden die gegen die extern erwirtschaftete Einlage ausgegebenen Tokens pro rata auf alle aktuellen Tokenhalter verteilt werden.

Mit einer nachweislich existenten *externen projektbezogenen Profit-Funktion* $f(t,i)$ bekäme ein einem Projekt zugrunde liegendes *Bonding-Curves-Token-Modell* das ihm noch fehlende - und aus unserer Sicht unverzichtbare - Merkmal: Nämlich eine gewisse Abkoppelung des realen Tokenwerts - gemessen durch $\mathcal{V}(i)$ - von der oft - zurecht als scheeball-artig kritisierten - Ausgabepreis-Kurve $\mathcal{K}(i)$.

Damit liefern wir aus unserer Sicht den bisher bei dem meisten *Bonding-Curves-*

Implementierungen fehlenden Baustein für eine solide und fundierte Token-Distribution mittels eines *Bonding-Curves-Modells* und entgegnen damit - zumindest auf abstrakt Weise - dem bestehenden Hauptproblem der *Bonding-Curves*: Nämlich *Ponzi, Pump & Dump oder Hot Potatoe* zu sein.

Wir behaupten hierbei keinesfalls, den heiligen Gral für das Funktionieren von *Bonding-Curves-gestützten Token-Modellen* gefunden zu haben. Denn schließlich ist die Existenz des von uns eingeführten $f(t, i)$ alles andere als gegeben, äußerst projekt-abhängig und zudem in der Regel vermutlich nicht leicht zu formalisieren - geschweige denn ohne optimistische Annahmen zu beweisen. Denn nicht zuletzt argumentieren viele auf *Bonding-Curves-Token-Modelle* gestützte Projekte genau wie wir hier an dieser Stelle: *Es existiere ein externer Projekt-Value, von welchem die Tokeninhaber profitieren!* Nur geben diese Argumentationen diesem Value nicht den Namen $f(t, i)$ und verpassen damit eine formal abstrakte Verallgemeinerung.

Wir fassen zusammen:

Conclusion 2: Token-externer Projekt-Value

Wir reduzieren das bestehende Problem von *Bonding-Curves-Token-Modellen* hinsichtlich *'Ponzi' und 'Pump & Dump'* auf den Nachweis der Existenz einer ***Of-Contract-EBIT-Funktion*** $f(t, i) > 0$ und deren Formalisierung anstatt von undefiniertem *externen Projekt-Value* zu sprechen.

Idealerweise wird $f(t, i) > 0$ durch unbestreitbare Logik eines Smart-Contracts begründet, der in wertschöpfender Interaktion mit unserem Token-Contract steht (Profite in seine Treasury einzahlt). Andernfalls erschwert sich die Argumentation und muss solide begründet und formalisiert werden.

Um das $f(t, i)$ nicht ganz als abstraktes Mysterium dastehen zu lassen und Zweifel an dessen Existenz zu zerstreuen:

Beispiel 1: DeFi-Projekte besitzen stets ein $f(t, i) > 0$

Jedes DeFi-Projekt besitzt ein $f(t, i) > 0$! Ob

- DEX-Provider à la *Balancer*,
- Market-Places à la *OpenSea*,
- Lending-Platforms

oder viele andere agieren wirtschaftlich, indem sie in der Regel Provisionen auf ihre Dienstleistung veranschlagen. Diese Gebühren sind unmissverständlich in ihrer Contract-Logik verankert und gänzlich transparent.

Würden solche Projekte einen *Bonding-Curves-gestützten* Utility-Token herausgeben und einen gewissen Abfluss ihrer Provisions-Profite in die Contract-Treasury dieses Tokens implementieren, würde solch ein Mechanismus auf ganz natürlich Weise das von uns geforderte $f(t,i) > 0$ definieren. Jeder Tokeninhaber würde damit jeder gebühren-pflichtigen Transaktion mit partizipieren.

Wie nun bereits mehrfach betont, ist und bleibt das von uns eingeführte $f(t,i)$ projektbezogen. Wir wollen an dieser Stelle dagegen weiterhin möglichst abstrakt und allgemein bleiben und uns im folgenden der Ausgabepreis-Kurve $\mathcal{K}(i)$ widmen - insbesondere auch mit der Zielsetzung die Anforderungen an das $f(t,i)$ so gering zu gestalten, wie nur möglich.

Wie ebenfalls bereits herausgearbeitet, ist die verwendete Implementierung des $\mathcal{K}(i)$ ohne nachweisbare Existenz eines $f(t,i) > 0$ in vielen *Bonding-Curves-Projekten* als ein teils unseriöser Preistreiber zu sehen. Dies resultierte aus der bereits oben formalisierten Kaufentscheidung eines jeden potenziellen Tokenkäufers:

$$\text{Ich sollte kaufen } \Leftrightarrow \exists k > i, \text{ so dass } \mathcal{V}(k) > \mathcal{K}(i)$$

Und zwar **Preistreiber** deswegen, weil die Kaufentscheidung eines Tokens bei aktuellem Supply $i \in \mathbb{N}$ ohne fundiertes $f(t,i)$ von Kaufentscheidungen Anderer bei größerem Supply $i, i+1, ..., k$ abhängt. Man sollte also genau dann kaufen, wenn man davon ausgeht, das andere später auch kaufen - und das noch zu einem höheren Preis. Diese müssten dann davon ausgehen, dass wiederum andere noch später zu einem noch höheren Kurs einsteigen und so weiter.

An bier WIP

Und obwohl wir die Existenz eines $f(t,i) > 0$ nicht allgemein sicherstellen und es erst recht nicht konkret benennen können, so können wir zumindest eine Mindestanforderung herleiten und diese dabei zusätzlich ins Verhältnis zum Risiko eines potenziellen Investors setzen.

Dazu wollen wir das $\mathcal{V}(i)$ von etwaigen künftigen Käufen abkoppeln und seine Abhängigkeit von $\mathcal{K}(j)$ auf ausschließlich vergangene Käufe $\mathcal{K}(j)$ mit $j <= i$ reduzieren.

Prämisse 1: Risiko eines Tokenkaufs

Wir definieren eine zusätzliche Abhängigkeit zwischen Ausgabepreis-Kurve $\mathcal{K}(i)$ und Rücknahmepreis-Kurve $\mathcal{V}(i)$:

$$\mathcal{K}(i) = (1+\rho) \cdot \mathcal{V}(i) = (1+\rho) \cdot \frac{\mathcal{T}(i)}{i} = (1+\rho) \cdot \frac{\sum_{j=1}^{i} \mathcal{K}(j)}{i} \text{ mit } \rho > 0$$

Neu an dieser Forderung ist hierbei lediglich die erste Gleichheit. Die anderen sind

Resultat unserer bereits weiter oben definierten Anforderungen an die Rücknahmepreis-Kurve $\mathcal{V}(i)$.

Das $\rho > 0$ beschreibt hierbei das Invest-Risiko eines Tokenkaufs bei Supply von $i \in \mathbb{N}$. Unsere Forderung ist also wie folgt zu interpretieren: ρ beziffert den prozentualen Höchstverlust, den ein potenzieller Investor bei einem Kauf eines Tokens zum Preis von $\mathcal{K}(i)$ bei einem Supply von $i \in \mathbb{N}$ im schlimmsten Fall zu tragen hätte. Denn er könnte den gekauften Token jederzeit zum Preis von $\mathcal{V}(i) = \frac{\mathcal{K}(i)}{1+\rho}$ wieder an den Contract zurückgeben und sich dafür auszahlen lassen.

Hinsichtlich dieser Interpretation wird das $\rho > 0$ in der Praxis also vermutlich tendenziell sehr klein zu wählen sein: $0 < \rho \ll 1$.

Die konkrete Wahl von ρ wird hierbei in starker Wechselwirkung zum projektbezogenen $f(t,i) > 0$ stehen. Je vielversprechender der durch $f(t,i)$ beschriebe *Of-Contract-EBIT* des Projekts ausfällt, desto größeres Risiko und damit ρ ist einem Tokenkäufer zuzumuten und umgekehrt.

Am Ende gilt wahrscheinlich sogar

$$\text{Es existiert kein } f(t,i) > 0 \;\Leftrightarrow\; \rho = 0 \;\Leftrightarrow\; \mathcal{V}(i) = \mathcal{K}(i) \;\; \forall i \in \mathbb{N}$$

Das Risiko ist mit der gemachten Vorgabe an die Rücknahmepreis-Kurve ist insofern mit gegebener Sicherheit gedeckelt als das $\mathcal{V}(i)$ für $\rho > 0$ stark monoton steigend ist

Zudem kann man bei gegebenem $\rho > 0$ seine durch

$$\exists k > i, \text{ so dass } \mathcal{V}(k) > \mathcal{K}(i)$$

gechallengte Kaufentscheidung validieren und nicht nur die Existenz eines solchen $k > i$ beweisen, sondern dieses k auch konkret in Abhängigkeit des ρ berechnen.

WIP

Begünstigte formalisieren (mit zusätzlicher Funktion). Begünstigte erhalten einen Teil der Projekt-Treasury zu ihrer freien Verfügung.