A Mathematical Review of the Saga Cryptocurrency

Adam T Smith, SUMWARE LLP (UK)
asmith.multiply@gmail.com
www.linkedin.com/in/adam-smith-9525b1136/

30 March 2020

1 Introduction

This review examines the financial mathematics of the Saga cryptocurrency, as set out in the Saga Monetary Model Paper, November 2018[1]. It was commissioned by Saga Monetary Technologies.

Mathematical issues appear as boxed remarks, a summary of which is given in the table below - **no significant problems were identified**. Sections (3) and (4) are discussions for which this is inapplicable.

Remark	Description	Severity
1	Conditions preventing manipulation	**Harmless**
2	Price sensitivity for variable reserve ratio	**Harmless**
3	Interpolation used in the shrinking economy	**Harmless**
4	Errors in Appendix C simulation results	**Low**

These **terms** are used throughout:

- **SGA**, Saga cryptocurrency coins, denominated in SDR.
- **SDR**, Special Drawing Rights, a currency unit based on a basket of five key international currencies defined by the International Monetary Fund: U.S. dollar 41.73%, euro 30.93%, renminbi 10.92%, Japanese yen 8.33%, British pound 8.09%. It is not currency as such, for example there are no SDR bank accounts, but is used as a reserve asset by nations through the IMF. (1 SDR = 1.38 US Dollar, 30 March 2020.)

[1] See www.saga.org/resources/

- **ETH**, Ether, the native Ethereum currency.
- **Smart contract**, the Saga (Ethereum) smart contract that buys and sells SGA from users.
- **Target Points, TP1 to TP7**, the 7 points in market capitalisation where SGA is given a designated reserve ratio.
- **SGN**, Saga Genesis cryptotokens, used to reward the Saga originators and provide ongoing funding.
- **GMP**, the 94 Genesis Minting Point where additional SGA are created for SGN holders.
- **Conversion ratio**, the number of SGA currently allocated to each SGN.
- **Vesting Point**s, 30% of SGN, owned by Saga Monetary Technologies Limited, receive their SGA later than other SGN at these 3 points.
- **Saga Monetary Technologies Limited (SMT)**, the English company limited by guarantee that develops and maintains Saga.
- **M,B,T**, million, billion (10^9), trillion (10^{12}).
- **SP**, my abbreviation for the Saga Monetary Model Paper, November 2018.

Review Coverage

Since a smart contract sets SGA prices they acquire blockchain immutability and are "transparent, predictable and impartial" (SP p4). Section (2) covers the mathematical specification of this. A governance mechanism enables changes to be made but this is outside the scope of this review. The smart contract and Ethereum platform are assumed to work perfectly, with the mathematics and finance being our only consideration.

ETH reserves are acquired from SGA sales since the smart contract can only deal with cryptocurrencies, but are held mainly in bank accounts in the SDR currencies to negate currency risk. Reserves therefore need management and coordination with the smart contract, including currency exchange transactions between ETH and the SDR currencies. This topic is discussed in section (3).

Since Saga has a fractional reserve inevitably the question of whether a run on the currency is possible arises. Saga is designed to curb this possibility as discussed in the final section (4).

The following simplifications are often made and it's convenient to refer to them as the **simplified model**:

- The smart contract gives a single price for both SGA sales and purchases, whereas it really has a bid/ offer spread. See (2.4).
- Interest and costs associated with reserves are ignored. See (2.1) **O2**.
- In reality SGA undergoes an inflation (increase in number) of SGA at each GMP, and the deflating (decrease in number) model is not the same as the increasing one. See (2.3).

2 The Saga Monetary Model

This section verifies and expands upon the mathematical construction of Saga, though not always in the same sequence as the SP. It was written so that the reader does not need to continually refer to the SP, but references are always given.

The relevant variables (SP p14) are:

- N, the number of SGA coins in circulation.
- P, the price per SGA in SDR given by the smart contract.
- R, the value of the reserve in SDR.
- r, the reserve ratio as a fraction of SGA market cap.

2.1 SP p8-9 - Objectives for Saga's Monetary Model

To meet its four fundamental objectives a design choice is made that the model price (mid price in the full model) be a function solely of number of SGA outstanding, i.e. $P = P(N)$. Moreover $P(N)$ is made a (non-strictly) increasing function that is constant at $P = 1$ SDR for $N \leq 20$M, and then gradually increases as N grows using a specified schedule. Therefore there is only one free variable, which can be chosen to be N, R, or market capitalisation NP. P and r are unsuitable since they are constant for part of the range.

How does this meet the objectives?

O1 - To prevent the possibility of malicious users manipulating the system and gaming the Reserve for unfair profit.

The SP rightly points out that using another possible input to P, trading volume (say in the secondary market on crypto exchanges), allows gaming through artificial trading between collaborators, however I see difficulties with this paragraph:

> **Moreover, an effective way of ensuring the model is not susceptible to unfair gaming by participants is to make it path-independent. The behaviour of the model in a particular state should depend on that state alone, not how we got there. It is not possible to add more than one free variable to a pricing function and at the same time have a model which is both path-independent and robust.**

Remark 1. **Conditions preventing manipulation**

First, using a path-independent input for P does not necessarily prevent gaming, for example the number of SGA holders allows gaming by collaborators opening accounts in between buying and then selling SGA.

Further any set of variables could in principle be used safely as long as users have no control over any of them. This rules out functions of the path of N, and in fact N appears to be the only non-manipulable free variable.

Going beyond the simplified model Saga is path dependent in some respects. R is dependent on the history of N when bid/ offer spread is considered, and shrinking economy prices depend on the highest N previously reached, though this are not useful for manipulation.

Since P is a function of N only these points are irrelevant in practice and users have no ability to control P beyond ordinary SGA purchases and sales which obviously does not admit gaming, meeting **O1**.

Severity level: Harmless.

O2 - To ensure the pricing model is 'robust': if all SGA holders decide to sell their tokens back to the Contract, there must be enough money in the Reserve to pay them back at the model's prices.

This is clearly satisfied in the simplified model since SGA currency inflation and deflation mirror each other exactly. For the real monetary model bid/ offer spread is no problem since the reserves gain spread income and interest also benefit reserves, but costs (and any deposit loses) reduce reserves. ETH currency exchange also generates some financial risk to the reserves.

At this point it's useful to point out that the prices the smart contract gives to users are rescaled to adjust for difference between actual reserves and their model value at the current N (SP p30-31)

$$P_{\text{actual}} = \frac{R_{\text{actual}}}{R_{\text{model}}} P_{\text{model}} \tag{1}$$

All costs and benefits are incorporated through the factor $R_{\text{actual}}/R_{\text{model}}$, which rescales price and reserves so that the actual reserves available are

distributed in proportion all the way down to $N = 0$, meeting the objective. Since it varies its value must be periodically reset in the smart contract by SMT.

GMPs and the shrinking economy are a part of model prices and **O2** is reconsidered for these in (2.3) **Shrinking Economy**.

P always refers to model price in the rest of this review.

O3 - The price of SGA should reflect the strength of the Saga currency. This could be measured by metrics such as: i) the amount of SGA in circulation; ii) the number of unique SGA holders; iii) the volume of SGA transactions.

Option (i) was chosen. Moreover since P is an increasing function of N, P also increases with market capitalisation (and R). Market cap is arguably the best single measure of currency strength since it represents the total demand for the currency.

O4 - The monetary model should aim to regulate volatility of SGA price, while also balancing the need for sufficient price appreciation.

Price appreciation occurs through progressively lower reserve backing as will shortly be described, but this also increases volatility. This is dealt with first in (2.2) **Reserve Ratio and Volatility**.

2.2 Saga's Pricing Model

SP p14 - Deriving Price from Reserve Ratio

The first equation here is just the definition of the reserve ratio r, since NP is the SGA market capitalisation (SP eq 1)

$$R = rNP \tag{2}$$

The next equation expresses reserve amount in the simplified model another way[2], as the cumulative value of all sales of SGA (SP eq 2)

$$R(N) = \int_0^N dP = \int_0^N P(n)dn \tag{3}$$

The path from 0 to N is irrelevant in the simplified model, since purchases (i.e. buying SGA back from users) cancel sales between the same values of N.

[2]Almost too trivial to mention is that a typo in the SP excludes the d in $\int_0^N dP$.

Substituting (2) into (1) and differentiating with respect to N leads to a differential equation

$$\frac{1}{P}\frac{dP}{dN} = \frac{1}{rN}\left(1 - r - N\frac{dr}{dN}\right) \tag{4}$$

using $r = r(N)$ since there is only one independent variable, and also $\frac{d}{dN}\int_0^N P(n)dn = P(N)$.

Next r is specialised to a continuous piecewise linear function of N,

$$r_i(N) = \alpha_i - \beta_i N \tag{5}$$

where index i labels the pieces. As the SP points out any desired continuous function can be accurately approximated with many small sections, but in practice wide linear pieces meet all needs. The pieces are defined by seven Target Points chosen using the designers judgment with a specific reserve ratio at milestones in market cap, reproduced here (SP Table p42):

TP	**1**	**2**	**3**	**4**	**5**	**6**	**7**
R	20M	100M	200M	500M	10B	75B	300B
r	100%	95%	85%	65%	30%	20%	10%
Market cap	20M	105M	230M	770M	33B	375B	3T

These join up the linear sections. Up to TP1 SGA is fully reserved ($r = 1$), and above TP7 market cap is always ten times reserves ($r = 0.1$). Continuity in $r(N)$ is needed to ensure continuity in $P(N)$, and $dr(N)/dN \leq 0 \Rightarrow dP(N)/dN \geq 0$ as needed for **O3**.

Comment

The SP points out that eq (3) considers SGA to be bought in infinitesimal portions, which is quite accurate since transactions are priced using the simple expression produced by evaluating integral (3) rather than an approximate discretisation[3]. See Appendix A.

SP p15 - Saga's Reserve Ratio Function

The solution to differential equation (4) on a linear section is stated to be

$$P = \frac{\omega_i}{Nr_i}\left(\frac{N}{r_i}\right)^{1/\alpha_i} \tag{6}$$

[3]This was confirmed with the Saga team. Also the smart contract imposes no minimum transaction size, though of course SGA does have a minimum quantity, set at 10^{-18}, below economic transaction size.

with ω_i a constant. Note that when $r = 1$ this simplifies to constant P.

Comment

Since this solution is a cornerstone of Saga I verified it using Sagemath[4] as shown in Appendix B. This may seem excessive for a straightforward problem but I wanted to provide a formal verification.

SP p15-16 - Reserve Ratio & Volatility

This subsection aims to show that price volatility is restrained in accordance with **O4**, using the differential equation for constant r relating P and R

$$\frac{dP}{P} = (1-r)\frac{dR}{R} \quad \Rightarrow \quad P \sim R^{1-r} \tag{7}$$

with $\sim$ meaning proportional. The constant factor $(1-r)$ is the sensitivity of price growth to reserve growth, or equivalently how volatility in cash flows in and out of the system is transmitted to volatility in SGA price. It's better to use R as the independent variable here since it represents a real cash amount whereas N is more arbitrary.

Comments

The SP gives a couple of numerical examples illustrating the relation, but also asserts:

> **For simplicity in our calculations ... we consider a constant reserve ratio, though similar principles apply when working with a variable reserve ratio.**

Remark 2. **Price sensitivity for variable reserve ratio**

Since $(1-r) \leq 0.9$ price volatility will always apparently be constrained and we need to check whether variable r significantly increases it. The corresponding differential equation for $r(N) = \alpha - \beta N$ is

$$\frac{dP}{P} = (1 - r + \beta N)\,\frac{dR}{R} \tag{8}$$

This is derived in Appendix C. If the new βN term is sufficiently high price sensitivity can become large.

[4] See www.sagemath.org. Sagemath is a large open source CAS (Computer Algebra System), software that can perform symbolic mathematical calculations.

The following table quantifies the effect of this in the simplified model:

TP	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**higher**
mcap	20M	105M	230M	770M	33B	375B	3T	-
r	1	0.95	0.85	0.65	0.3	0.2	0.1	0.1
N	20M	98.7M	193M	453M	2.48B	4.80B	6.16B	-
$\beta = -\frac{\triangle r}{\triangle N}$	0	6.35E-4	1.06E-3	7.69E-4	1.73E-4	4.31E-5	7.35E-5	0
βN	0	0.0627	0.204	0.348	0.428	0.207	0.453 N	0
$1 - r$	**0**	**0.05**	**0.15**	**0.35**	**0.7**	**0.8**	**0.9**	**0.9**
$1 - r + \beta N$	**0**	**0.113**	**0.355**	**0.698**	**1.128**	**1.01**	**1.35**	**0.9**

Market cap and r are from the simplified model Target Points Table while N is from SP Appendix D for the full model, which is a little inconsistent but fine for the accuracy needed here. Calculations are for points at the high N end of each linear segment where sensitivity $(1 - r + \beta N)$ is largest. β is per million. The differential equation is approximate for finite differences $\triangle R$ and $\triangle P$, but this is fine since using the largest local sensitivity overstates sensitivity for any finite difference which is conservative.

Comparing the last two rows sensitivity increases but only reaches a maximum of 1.35 just before TP7, and has much lower values when the currency is smaller. We are still well within the same order of magnitude as the constant r numbers, and price volatility remains well constrained meeting **O4**. This picture changes somewhat when GMPs are taken into account, but subsection (2.3) shows that that **O4** is not compromised.

Severity level: Harmless.

Another approach is to calculate exact differences and this is done for selected points in SP Table 2 p25. Sensitivity numbers can be obtained from

this using

$$\frac{\triangle P/P}{\triangle R/R} \simeq \frac{1\% \text{ change in } P}{\text{corresponding } \% \text{ change in } R}$$

and these are given in the following table.

mcap	100M	500M	1B	5B	10B	50B	100B	500B	1T
sensitivity	0.097	0.45	0.5	0.71	0.76	0.83	0.909	1.27	1.32

These numbers are consistent with the $(1 - r + \beta N)$ row in the table in Remark 2, though lower because that method is conservative. Again this confirms that volatility is restrained. Monte Carlo simulations provide a further check, see subsection (2.5).

At this point I'd like to look at this from a wider hopefully illuminating viewpoint. Using eq (2) to change variables in the $P - N$ solution eq (6) to $P - R$ and also $N - R$, and obtaining differential equations for these variable pairs (see Appendix C) and their implied growth relationships, we have

$$P = \frac{\omega^\alpha}{r^2} R^{1-\alpha}, \quad \frac{dP}{P} = (1 - r + \beta N)\frac{dR}{R}, \quad P \sim R^{1-r+\beta N} \tag{9}$$

$$N = \frac{r}{\omega^\alpha} R^\alpha, \qquad \frac{dN}{N} = r\frac{dR}{R}, \qquad N \sim R^r \tag{10}$$

The differential equations and growth relationships are approximate here if using finite differences ($\triangle R$ etc) because r and N are variable.

Specialising now to constant r (so that $r = \alpha$, $\beta = 0$) produces

$$\mathrm{P}{=}\frac{\omega^r}{r^2} R^{1-r}, \quad \frac{dP}{P} = (1 - r)\frac{dR}{R}, \quad P \sim R^{1-r} \tag{11}$$

$$N = \frac{r}{\omega^r} R^r, \qquad \frac{dN}{N} = r\frac{dR}{R}, \qquad N \sim R^r \tag{12}$$

This time using finite differences is exact. The second two $P - R$ relations verify the SP, but more interesting is the joint behaviour of P and N.

Market cap varies as $NP \sim R^1$ or has growth rate 1 (unsurprising for constant r), and cash flow into the system produces price inflation and coin number inflation, with r deciding how the total growth and volatility is split between the two. For small currency size up to TP1, $r = 1$ and inflation goes entirely to number, while above TP7 $r = 0.1$ and price inflation is maximised at 0.9 and number growth minimised at 0.1. The same goes for cash flow out of the system and deflation.

This also means that P increases with R for any constant $r < 1$, such as above TP7. Intuitively the reserves receive the full price of sold SGA but only a fraction r of this is needed to support that price so there is then room to increase P further. In practice a hard limit is set for N preventing expansion above market cap 5T SDR, though the smart contract will still buy back SGA and allow deflation to occur (SP p40).

Returning to the variable r version the difference is that the total growth rate of market cap increases (for a small change in N) to $1 + \beta N$, and the extra βN goes to price inflation. This extra growth comes from the increase in factor $1/r$ within $NP = R/r$.

2.3 Saga Genesis and the Shrinking Economy

SP p17-19, p26-31 - Shrinking Economy

There must be a method to reward Saga's investors and provide ongoing funding. Saga has rejected initial coin allocations in favour of a method that provides rewards at set stages in the growth of the SGA, in order to align interests much better with the success of the currency. This is provided by the SGN cryptotoken. Whenever given levels of N called the Genesis Minting Points (GMPs) are first reached new SGA are created (minted) for SGN holders.

P is held constant over a GMP and R is obviously constant too, so (2) implies rN is constant over a jump, or

$$N_{\text{after}} = N_{\text{before}} + \triangle N, \quad r_{\text{after}} = \frac{N_{\text{before}}}{N_{\text{before}} + \triangle N}\, r_{\text{before}} \tag{13}$$

where $\triangle N$ is the quantity of SGA minted. Also, market cap jumps up by $P \triangle N$.

This interferes with the Target Points schedule for r of the simplified model, so the rule is that after a jump the growing curve continues to aim for the next Target Point, requiring a new linear section of $r(N)$ with new α, β. For example this produces three linear sections of decreasing slope between TP1 and TP2 'pointing' to TP2, and similarly between TP2 and TP3 as seen in the blue plot in Fig (1). If r dips below the next target value it's kept constant (SP p42), as happens for the last sections before TP2 and TP3.

After a jump $r(N)$ cannot follow the same path back down for falling N as it did on the way up, and another path must be specified. All shrinking curves must intersect two points at the low and high N boundaries:

(i) $r = 1$ at $N = 20M$ (like Target Point 1).

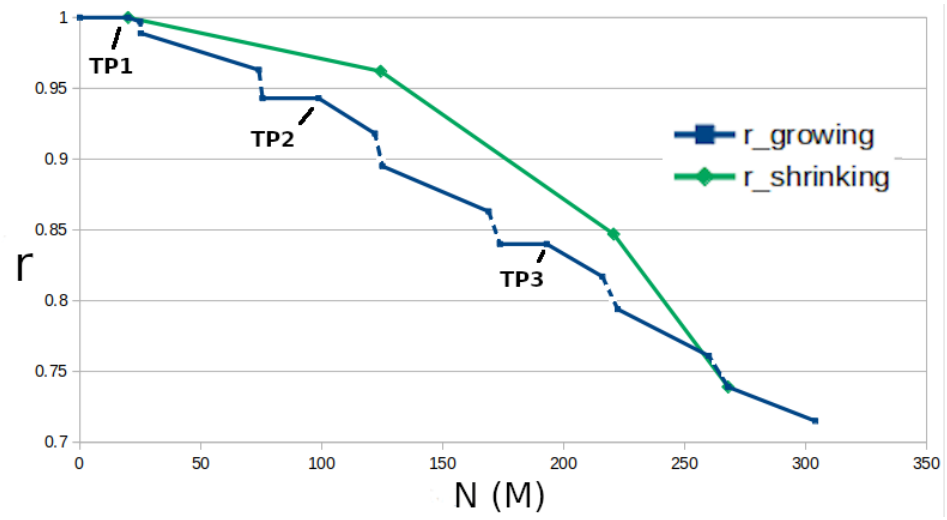

Figure 1: The growing economy in blue and the shrinking economy after the minting at $N = 260M$ in green. The dotted lines are GMPs.

(ii) The point after the jump $(N_{\text{after}},\ r_{\text{after}})$, which connects to the growing curve for higher N, ensuring P is continuous.

In between these two points each shrinking curve is specified by the formula (SP, p27)

$$r_{\text{shrinking}} = r_{\text{base}} + (1 - r_{\text{base}})\,\frac{r_{\text{base}} - r_{\text{min}}}{1 - r_{\text{min}}} \tag{14}$$

where r_{base} is taken from the growing economy curve and $r_{\text{min}} = r_{\text{after}}$. The second term is included to increase $r_{\text{shrinking}}$, as "a higher reserve backing provides extra support to Saga's shrinking economy" (SP p26), but the SP does not quite give the full mathematical details here as an interpolation described in the following remark based on discussion with the Saga team is used.

Remark 3. **Interpolation used in the shrinking economy**
Let's chose the GMP at $N = 260M$ where $8M$ SGA is minted as an example to illustrate the method, see Fig (1) which also complements the SP by providing a plot in the pair (N, r). First take the low and high N points (i) and (ii) and insert between them the round 10% values

of r on the growing economy curve, producing the list of (N, r) points

$$\textbf{base} = \{(20M, 1), (124.4M, 0.9), (220.7M, 0.8), (268M, 0.739)\}$$

Previous GMPs jump over the r =90% and 80% points so linear interpolation using their before and after (N, r) points is used to obtain the N. This happens all the way down to 20%. Also, if a round 10% value occurs within the last jump to $r_{\min}$ it's excluded.

Add the increment term to the r value of each, which is zero for the first and last entry, giving the new points

$$\textbf{shrink}=\{(20M, 1), (124.4M, 0.962), (220.7M, 0.847), (268M, 0.739)\}$$

and $r_{\text{shrinking}}(N)$ is the linear interpolation between these points.

Comments:

- The linear interpolation is essential so that $P - N$ formula (6) can also be used for $P_{\text{shrinking}}(N)$. Using round 10% values of r gives nicely separated interpolating points. (The joins between sections can be seen in SP Fig 10, p30.)

- While a shrinking curve is mostly above the growing one due to the interpolation there can be a small region on the right where $r_{\text{shrinking}} < r_{\text{growing}}$, as is just visible in Fig 1. In fact the first three GMPs do not reach low enough r to acquire the 90% point, so their shrinking curves are just straight lines that are also lower for parts of their ranges.

- We need to recheck **O4** that volatility is constrained since the GMPs change the growing curve and there is a new shrinking curve. Price sensitivity to R is the quantity $(1 - r + \beta N)$.

  GMPs cause the growing curve β to be lower (less slope) than the simple model at any N. r is lower too but never lower than the value at the next Target Point, except by a small amount in the last segments when β is zero. Therefore growing curve sensitivities cannot be much larger than for the simple model in Remark (2) and present no problem.

  Shrinking curves are a little more complex. r_{base} points are at roughly the same r as the simple model, but the second term

in eq (14) changes things. Slope β is lower and r higher in the low$N$ range, lowering sensitivity there compared to the simple model. For the higher N region slope is increased, and in fact nearly doubles for the highest N for nearly the same r (this factor will be explained shortly below), so that sensitivity is less than $(1 - r + 2\beta N)$. From the table in Remark (2) sensivity therefore rises from 1.35 to 1.8 at TP7 with smaller increases for the other points, again giving no problem. (The first three GMPs do not have interpolating points and therefore produce shrinking curves very similar to the simple model growing curve.)

- A minor point is that contrary to SP Note 2 p27 the second increment term is not proportional to the shrinkage since the high water mark (since it's zero at point (i)).

Severity level: Harmless.

Further comments

Now let's look closer at the second term in eq (14): It's quadratic in r_{base}, zero at the boundary points and positive between them, and scaled by the total r range in the denominator. Since it has a humped shape we should check that $r_{\text{shrinking}}$ never rises with increasing N which would contradict[5] **O3,** by examining the derivative of eq (14) without the interpolation

$$\begin{aligned} \frac{dr_{\text{shrinking}}}{dr_{\text{base}}} &= 2\frac{1 - r_{\text{base}}}{1 - r_{\text{min}}} \\ &= \begin{cases} 0 & \text{at point (i) } r_{\text{base}} = 1, \ (N = 20M) \\ 2 & \text{at point (ii) } r_{\text{base}} = r_{\text{min}} \end{cases} \end{aligned}$$

So, taking the interpolation into account the shrinking curve always slopes downward from $N = 20M$, and then the following linear sections slope downward more and more and there's no problem for any shrinking curve. Fig 2 should help to visualise this.

The chain rule gives

$$\frac{dr_{\text{shrinking}}}{dN} = \frac{dr_{\text{shrinking}}}{dr_{\text{base}}} \frac{dr_{base}}{dN}$$

[5] Technically from eq (4) this is a stricter condition than the rising P required by **O3**, but it's clear we also want reserve ratio to fall with N.

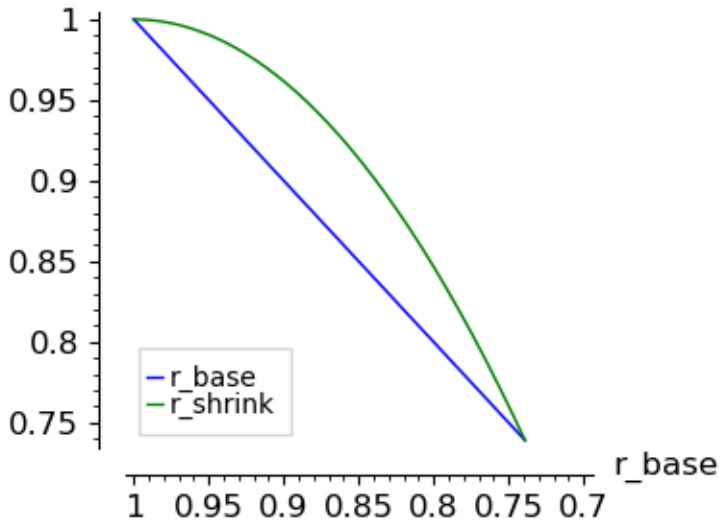

Figure 2: The base and shrinking curves without the interpolation.

though this only applies where $r_{\text{base}}(N)$, which we take to be the growing curve, is defined, i.e. not inside GMP jumps. It can be seen from the zero derivative at $N = 20M$ that this clever choice of increment raises up $r_{\text{shrinking}}$ the greatest amount possible for a quadratic without giving it a hump. There's always a GMP jump to r_{min}, so $r_{\text{base}}(N)$ is undefined there where a doubling of the growing curve slope would be, but there is a comparable steepening in the high N area.

Due to the mintings the reserves integral for the growing curve (3) has a gap in N for each GMP, so that for example

$$R = \int_0^{N_{\text{before}}} P(n)dn + \int_{N_{\text{after}}}^{N} P(n)dn \tag{15}$$

when N is above the first GMP and below the second.

Regarding objective **O2** (reserves being sufficient) $r = 1$ ensures this applies for N from $20M$ down to 0, but also reserves must not already be all paid out before reaching this on moving down a shrinking curve. A good way to look at this is to use eq (12) $dR/R = dN/rN$ combined with the fact that r is larger on shrinking curves, to see that less reserves are paid out when shrinking than are taken in when growing, through lower prices. However for shrinking the reserve integral (3) has no gaps in N where the reserves don't change, and must make up for the the growing economy gaps so this

is not a proof of reserve sufficiency. (This is the requirement $\int_0^N P(m)dm = \int_0^{N+n} P'(m)dm$ in SP p26, where prime indicates the shrinking curve and n is the jump in number due to a single GMP.)

We can also see that the constant price below $N = 20M$ after shrinking is inevitably not 1 as it is for the growing economy, due to this dilution effect of GMPs (the same reserves are shared among larger N) and the different shrinking curve. From SP Fig 8 we can see that it's value is about 0.8 to 0.85 SDR for the shrinking curves of GMPs in the range of market caps 1B to 100B SDR.

SP p 43-44 - Location of minting points and quantity of SGA minted

GMPs are located using a recurrence relation in reserve amount

$$\begin{aligned} R_{i+1} &= u + vR_i \\ R_1 &= \text{25M SDR} \end{aligned} \tag{16}$$

where u and v are absolute and relative step size constants. The amount of SGA minted is

$$\begin{aligned} \triangle N &= Mf \\ \text{where } M &= N - (\text{number of SGA previously minted}) \end{aligned} \tag{17}$$

with constant 'minting factor' f and M the number of SGA bought by users.

The constants are fixed according to ranges of amount of SGA minted so far for each SGN, the 'conversion ratio' given in SP p45 and reproduced here.

conversion ratio	u	v	f
up to 1 at TP4	50M SDR	1%	-
then up to 4	50M SDR	1.5%	1%
then up to 10	150M SDR	5%	1%
then up to 15	250M SDR	12%	1%

Note that the minting factor is not used in the first section and instead minting amount depends on distance from the target of conversion ratio 1 at $R = 500$M SDR, i.e. Target Point 4.

There are 107M SGN tokens and the parameters are chosen so that a maximum of 15 SGA per SGN are minted, at which point they form less than 30% of all SGA.

As a precaution against manipulation by SGN the SGA price must remain above the minting point for seven days before the minting occurs. This discourages from buying SGA in order to trigger a minting and then selling the SGA immediately afterwards for more valuable SGN.

Comment

The method ensures that GMPs are spaced at geometrically increasing intervals of R, and there is not a disproportionately high number of SGA minted relative to current N and size of the currency, or compounding amounts minted based on SGA already allocated to SGN. There are 94 GMPs in order to avoid large minting amounts at any point. All GMPs lie within the varying r range between Target Points 1 and 7.

SP p17 - SGN Conversion

SGN can be exchanged for their current allocation of SGA at any time using the smart contract, but converted SGN are burned extinguishing their rights to later mintings (SP p17). When future GMPs are reached SGA are still minted for the burned SGN in order for the monetary model to remain deterministic and predictable, but these SGA are always unallocated. Consequently N can never fall below this and some reserves will be trapped, however SGA has the advantage of the support of those reserves.

Comments

There's a good reason for this design. Conversion must not trigger a change in SGA price, as this would allow SGN a manipulation method by taking a trading position in SGA, converting, and then closing out the position for a profit. For example the obvious idea of burning any ownerless SGA and reducing N would affect SGA price, moving it up or down[6] .

SGN value consists of the current SGA allocation plus potential future SGA from future mintings. Since converting gives up the second component SGN should always be more valuable unconverted and realise more in the secondary market than by converting (as pointed in SP p19), until the final GMP when they become financially equivalent to 15 SGA. Nevertheless some conversion may occur as a route for SGN to cash out if the secondary market for SGN has not yet formed or otherwise cannot oblige.

An alternative design that does avoid changing the SGA price is to distribute any ownerless SGA allocation to the remaining SGN, but instead the chosen design is selected for being straightforward while also allowing SGA to benefit from any trapped reserves (as confirmed by the Saga team).

[6]For this scenario eqs (1), (4) and (10) lead to $dP_{\text{actual}}/P_{\text{actual}} = (-r + \beta N)/r\, dN/N$, which from the table in Remark (2) is positive for some ranges of N and negative for others. Also SGN would be further away from the next minting.

SP p20,45 - Vesting

Saga Monetary Technologies own 36% of the SGN, and 30% are given a stricter treatment than normal SGN. These SGN are minted in three batches of 10% when SGA market cap reaches the three Vesting Points of 600M, 0.25B, and 2B SDR. The appropriate number of SGA are simultaneously minted and allocated to them so that they immediately become equivalent to normal SGN. This also preserves the SGN-SGA ratio. The purpose of this is to prevent the sale of SGN in earlier stages of currency growth when this might have a damaging impact.

Comment

This feature presents no problems, and will hardly be noticeable to SGA holders.

2.4 SP p31-36 - Bid/ Offer spread

The smart contract SGA bid and offer prices are given by $(1 \pm w)P$ using the scheme

$$w = \begin{cases} 0.15\%, & \text{market cap} \leq 1\text{B} \\ c_1 + c_2/r, & 1\text{B} \leq \text{market cap} \leq 1\text{T} \\ 15\%, & 1\text{T} \leq \text{market cap} \end{cases} \tag{18}$$

where P is the model price and also mid-price. Constants c_1 and c_2 are fixed by requiring continuity at the joining points between ranges. The currency will only grow when the smart contract offer is more competitive than the secondary market, and only contract when the smart contract bid is more competitive. Prices can move within the range without N changing.

The small value 0.15% is chosen to match typical spreads on crypto trading exchanges so that when the currency is small the smart contract controls price and serves as market maker before any secondary market has developed. It also provides an income to pay for ongoing costs. At market cap of 1B when experience with other cryptocurrencies conservatively suggests a secondary market for SGA will have developed, the spread starts to widen, though this can be delayed. Now the secondary market gradually plays a larger role as the currency grows. The maximum value of $w = 15\%$ is chosen to match the required currency band for admission in to the Eurozone and to encompass the observed normal fluctuations over one year of major currencies of 30%.

Four benefits for this are given.

- It prevents N changing with every fluctuation in the market.

- Operating costs are reduced as trading is progressively handed over to the secondary market.
- Spread provides an income for the reserves.
- Spread forms a protection against front running.

Front running is a common blockchain issue (as mentioned in the SP) arising from the public visibility of blockchains and awaiting transactions (mempool). The mempool varies between different mining nodes somewhat depending on how transactions got passed around the network, but an attacker can monitor for a large SGA order that will significantly changes P and place a trade hoping to get filled by the smart contract first.

Spread offers protection against this since the change in P due to the large order must be large enough for the attacker to beat the bid/ offer spread: SP Table 4 p39 shows breakeven order sizes for this at various SGA market caps.

Comments on the table:

- Breakeven order size increases with market cap except for the change from first row at 100M SDR to second row at 300M SDR. This exception is explained by the variation of P with R being higher in the second case so that a smaller trade size creates a larger shift in P, while spread remains the same at $w = 0.15\%$.
- I verified the first row by setting the percentage change in P equal to the bid offer spread, and using eq 4 to give

$$2w = \frac{\triangle P}{P} = \triangle N \frac{1 - r + \beta N}{rN} \tag{19}$$

  This assumes that the trade does not make r exit its linear segment, and that using finite differences is accurate. The trade size in SDR is therefore

$$P \triangle N = \frac{2wrNP}{(1 - r + \beta N)} \tag{20}$$

  also assuming that the P integral for trade cost can be approximated by $P \triangle N$. Both the initial and final N lie in the constant r segment before Target Point 3, as seen in Fig 1, and the right hand side evaluates to $2 * 0.015\% * 0.943 * 100M/(1 - 0.943) = 4.96M$ SDR, which is only 1.2% away from the SP result of $4.9M$.

2.5 Monte-Carlo Simulations

The SP provides further analysis of the monetary model in the form of numerical simulations that take into account its full complexity, with growing and shrinking curves, minting points and price spread.

2.5.1 SP Appendix B - Price volatility

The methodology here is to simulate 20,000 random market cap time series, each of 365 days with constant standard deviation of return (volatility or vol) σ each day and mean zero. For each sample time series the standard deviation divided by mean is calculated, for market cap itself and also for the implied SGA prices using the monetary model. These are averaged over the 20,000 samples to produce the converged relative volatility results of SP table p51, for $\sigma = 0.5\%, 1\%$ and a range of six initial market caps. They are called 'relative' because of the division by the mean which gives equal weighting to sample series with high mean and low mean.

Comments on the method and results:

- Normally distributed return (geometric Brownian motion or lognormal process) is a good standard base assumption. The method investigates volatilities over time series rather than at a fixed time horizon, but the ratio between market cap vol and price vol will be roughly similar for both pictures.

- Market cap relative volatility results are 3.61% for $\sigma = 0.5\%$ and 7.24% for $\sigma = 1\%$ regardless of the starting market cap because they are simply the mean of (standard deviation / mean) of each time series, which removes any dependence. Since these results don't require the Saga monetary model, I verified them using NumPy in a Jupyter workbook (not shown here) to the three significant figures of the SP using only 80,000 samples.

- Relative volatility of price is 0.14% at the lowest market cap 10M SDR for both σ values because almost all price paths lie within the $r = 1$, $P = 1$ initial section of the economy. P mostly bumps up and down between the bid and offer price each day, half the time staying put and half the time moving to the other, giving relative vol of 0.3% /2, or slightly less since sometimes a price falls inside the price band.

- Relative price volatility results increase with starting market cap for each σ, reflecting the decrease in r and higher price sensitivity. A

further rough check can be done using yet another differential equation, this time for the $P-C$ pair where C is market cap, obtained from eqs (9) and (10)

$$\frac{dP}{P} = \frac{1-r+\beta N}{1+\beta N}\frac{dC}{C} \tag{21}$$

Choosing the highest market cap of 1T SDR where it's largest, linear interpolation (of the denominator and numerator separately) between TP6 and TP7 for the simple model in the table in the Remark 2 gives sensitivity $\frac{1-r+\beta N}{1+\beta N} = 0.86$. If we multiply the relative market cap vol results by this we get 4.2% and 6.2% which are fairly close to the relative price vol results of 3.51% and 6.72%, for $\sigma = 0.5\%, 1\%$ respectively.

- SP Fig B1, b2-7 p47-50 show ten example market cap sample time series for $\sigma = 1\%$ and their resulting price paths at the six different starting market caps from 10M to 1T. Price changes show no variation at 10M SDR through to nearly the same variation as market cap at 1T SDR in line with eq (21).

- The previous four points corroborate the simulation results and again confirm that price volatility is constrained. The six initial market caps give comprehensive coverage.

- It was argued earlier that R should be the independent variable since it represents real cash flow in and out of the economy, but price sensitivity to market cap is only a little lower than to R due to the extra $(1+\beta N)$ factor in the denominator of eq (21), about 1.26 at market cap 1T SDR, so the two are similar.

2.5.2 SP Appendix C - Spread income

In this Appendix a similar method is used, but with prices rather than market cap driving the simulation. 20,000 sample price time series with mean zero and constant daily vols of $\sigma = 0.5\%, 1\%, 5\%$ are produced, and used with the same initial market caps except for 20M SDR which being at Target Point 1 prohibits any lower prices. When a new price in a time series moves outside the current bid or offer price a trade of appropriate size with the smart contract is simulated to change price to the new price. This creates gross income for the reserves, and a cost of 0.15% equal to half the minimum spread is applied to also give a net income. Averages for both income types and relative price volatility over the 20,000 samples are produced.

Comments on the method and results:

- Setting cost to a notional 0.15% is not completely realistic but is a good basis for illuminating how income varies with the inputs.
- Price has low sensitivity to market cap at low market cap as seen in the other simulation, which boosts trade sizes and gross income there compared to simulating market cap.
- Net income results are zero for low volatility and lowest initial market cap 100M SDR because very few time series go above the market cap 1B SDR level where the spread starts to rise from it's minimum size and all gross profits are taken by costs. $\sigma = 5\%$ must be sufficient to put some time series above this.

Remark 4. **Errors in simulation results**

The price volatility results for market cap $100M$ should be the same as the Appendix B market cap volatility results which are defined identically, i.e. 3.61% for $\sigma = 0.5\%$ and 7.24% for σ =1%. Small differences for the higher market caps seem due to rounding.

I also produced a table of the ratio of net-income to gross income results:

market cap		**100M**	**1B**	**10B**	**100B**	**1T**
σ	**0.5%**	0%	27%	94%	97%	98%
	1%	0%	39%	94%	* 9.7% *	98%
	5%	59%	* 7.8% *	94%	97%	99%

The two starred results are rather far from the trend in both directions and may indicate miscalculations.

Any errors are confined to these simulation results, do not damage the monetary model, and are therefore not serious.

Severity level: Low.

2.6 SP Appendix D - Saga Model Points

This Appendix lists the 7 Target Points, 3 Vesting Points and 94 Genesis Minting Points (GMPs) of Saga and key data at each point.

Comment and checks:

- Target Points 2 to 6 have r unchanged from the previous point and slightly below their target values because the GMP at the previous point takes r slightly below the target value. Target point 7 is exactly on target at $r = 0.1$ and market cap 3T as it needs to be to produce the maximum price multiple of 10 times reserves.
- The following consistency checks were confirmed to the significant figures given in the table:
  - The Target Points and Vesting Points do not change the SGN-SGA conversion ratio from the previous row.
  - The Target Points do not change r from the previous row.
  - The given minting amount produces the given inflation percentage.
  - The given minting amount and number N produces the given reserve ratio.
  - The cumulative SGA minted produces the given conversion ratio.

3 Ether as the operating currency

As mentioned in the introduction smart contract SGA trades are conducted in ETH, which must be exchanged to and from the SDR basket currencies of the reserve. The SP p37-39 describes this as follows:

- **ETH float:** A float of ETH is maintained to reduce the frequency and costs of currency exchange transactions. It's slower, especially outside of normal banking hours, and more costly to perform bank transfers and currency exchanges compared to having the smart contract simply use the float, but this generates some currency risk since the float is not in SDR. There's a trade off between liquidity and currency risk and the amount of float is intended to be sufficient for 'normal markets'.
- **Order queue:** It's possible to run out of ETH float when SGA is selling off. (Conversely the float may become large and currency risk

increase when SGA is being bought.) Some ETH can be acquired out of hours using Saga's currency exchange providers but when the float is depleted a FIFO (First In First Out, i.e. first come first served) queue of transactions is formed. ETH is paid out according to the ETH/ SDR rate prevailing at trade settlement, not at trade time. Clearly queuing frustrates liquidity, but this is considered the best possible solution.

Further important information is given in the webpage, *Reserve Attestation — What You Need to Know* [7] which describes how reserves are declared, and a reserve management plan that includes progressively moving to a higher proportion of reserves in bank accounts and lower ETH float as market cap increases.

Comments:

- The choice of SDR should broaden demand for SGA while being untied to any specific national currency. The SDR proportions change at the IMFs five yearly review which will then require a rebalancing of reserves. Sometimes the constituent currencies change too - for example the November 2015 review decided to include the Chinese yuan from 1 October 2016.

- The ETH/ SDR rate is needed by the smart contract, and is input by SMT every time it changes by more than a small amount (confirmed with the Saga team).

- The order queue inflicts no ETH currency risk on the user, who receives the ETH equivalent of their SDR when settlement occurs. Similarly there is no corresponding risk to the reserves, though in practice any difference between realised exchange rates and the smart contract rate will have an effect. The main issue is the user not getting paid immediately.

- On the other hand the ETH float represents some currency risk to reserves. Clearly it's good to see reserve management plans set out, and the potential to utilise future developments such as in hedging instruments and stablecoins.

[7] www.saga.org/blog/blogPost/Xe84wBIAAB8AaStp/ , 9 December 2019. Retrieved 12 February 2020.

4 Discussion of the Possibility of Currency Run

Now that the Saga design has been fully covered the issue of possible runs on the SGA currency can finally be discussed, or one viewpoint provided at any rate. In general a run can occur whenever early sellers receive more than later ones, giving all an incentive to sell first. The classic case of course is a bank run where depositors want to withdraw their deposits before fractional reserves run out, and without intervention the bank fails leaving latecomers with nothing. Positive feedback creates a stable equilibrium of escalating withdrawals.

The SGA monetary model has a price that becomes higher as the currency grows and lower as it contracts which potentially gives an incentive for selling that can snowball. The Monte-Carlo simulations give no insight into this since they have price changes independent of earlier prices (the Markov property) and lack the essential feedback. However Saga's design has important features to mitigate or interrupt the feedback mechanism of a runaway sell off as follows:

1. **Rising reserve ratio:** A primary measure must surely be that the reserve ratio r increases in a sell off, ultimately to full reserving at $N \leq 20M$ where price becomes constant. Reserves never run out and all sellers can be paid complying with objective **O2** in stark contrast to bank runs.

   Recalling subsection (2.2) higher r produces smaller price changes for the same percentage change in reserves or cash flow, so that not only does higher r help confidence in itself it also slows down the rate of price fall. There is a countercyclical effect whereby the greater the selling pressure the larger r becomes to slow it down.

2. **Shrinking path:** Shrinking curves have a concave shape compared to the growing one, so that when moving down a shrinking curve in a sell off higher r is reached quicker, with the benefits just given. This give an undesirable faster price decreases initially to some degree that then slows down, but it seems preferable to reach higher r quicker.

3. **Maximum price gearing 10x:** SGA price never exceeds ten times their reserve backing ($r = 0.1$), the same ratio that the US Federal Reserve requires on banks' Net Transaction Account (SP p13). Bank reserving is a complex topic not directly comparable to the Saga monetary model but this seems a fairly modest limit, and it isn't reached

until Target Point 7 when market cap is at the huge amount of 3T SDR and the currency should be much more robust.

4. **Spread:** Another important countercyclical feature is that Saga's reserves gain spread income whenever the currency is shrinking. (Since the model price is at mid price half the spread gets reflected in buys and half for sales.) A further small nudge is that spread is slightly larger for SGA sales than buys, with the effect being bigger for larger trade size as might occur in a sell off scenario (see Appendix A).

   Spread cost is also a market friction[8] dampening volatility and discouraging users from selling SGA back to the smart contract. Naturally it's a friction for buying too, but it seems better to grow more slowly and carefully than to facilitate a sudden currency expansion that may be prone to fall back again. Spread size is made larger for lower r when it's most useful.

5. **Blockchain guarantee:** Putting SGA pricing on a blockchain means the algorithm can be trusted and that accurate information about the current state is available. (Trust is required in the off chain reserve management parts of the system too and is addressed by reserve attestations. Also the ETH float is liable to run out in a sell off, delaying trade settlement for users, but it's hard to see this having an impact, except possibly initially if the market doesn't appreciate that this is an operational issue of liquidating reserves.)

6. **SGN and minting point design:** Some value is transferred to SGN tokens through the minting of SGA, but these are triggered only when the currency reaches set sizes of market cap which are geometrically separated in N, and the amounts are never a large fraction of the current N. Along with the disincentive to convert SGN this should help prevent the newly minted supply of SGA depressing the price, though some conversion and SGA sale might occur in a sell off. Other than this SGN does not interact with SGA and can generate no harmful feedback loop. Unallocated SGA and trapped reserves will probably only be small but nonetheless they put a floor on N, and P too should more than 20M SGA become trapped.

Clearly these measures must defeat a run on the currency sooner or later, though it's hard to say how far r would fall before this happens - or if they

[8] See en.wikipedia.org/wiki/Frictionless_market.

might prevent it occurring in the first place. Overall the Target Points schedule for r is a plan to evolve the SGA currency from low to very high market cap. Due to its novelty there's nothing to compare this specific plan to, but it appears conservative with a slow and gentle decrease in r.

A Calculation of trade price

Substituting the $P-N$ solution (6) in equation (3) gives a simple closed form expression for the smart contract purchase cost (or sale proceeds) in SDR taking number from N_1 to N_2

$$\begin{aligned}
\text{cost} &= \int_{N_1}^{N_2} P(n)dn \\
&= \int_{N_1}^{N_2} \omega \frac{n^{1/\alpha-1}}{(\alpha-\beta n)^{1/\alpha+1}} dn \\
&= \omega \left[\left(\frac{n}{\alpha-\beta n} \right)^{1/\alpha} \right]_{N_1}^{N_2} \\
&= \omega \left[(\alpha/N_2-\beta)^{-1/\alpha} - (\alpha/N_1-\beta)^{-1/\alpha} \right] \qquad (22)
\end{aligned}$$

where subscript i is dropped. If the range N_1 to N_2 extends over more than one linear section of r on a growing or shrinking curve then cost is a sum of such expressions.

Bid/ offer spread is applied after this integration using the initial quantity N_1 in eq (18) (confirmed with the Saga team). This creates a slightly lower offer spread (user buys from N_1 to N_2) than bid spread (user sells from N_2 to N_1) within the range where spread varies, the effect being bigger for larger $\triangle N$.

This amount is then rescaled by the reserve adjustment factor in eq (1) to produce the actual cost in SDR, which is finally translated to ETH using the ETH/ SDR rate. The smart contract uses data updated by SMT for both these steps.

B Solution to the main differential equation

The following Sagemath Jupyter notebook shows a series of Python input and outputs cells that form a linked sequence of calculations that confirms solution (6) in the last cell.

Sagemath - Solving the key DE

In [1]:
```
print version();      # Sagemath version
!jupyter --version    # Jupyter client version
```

```
SageMath version 8.9, Release Date: 2019-09-29
4.4.0
```

In [2]:
```
var('a,b,N')  # Declare variables for r(N) = a + b*N
# Note: using the opposite sign for beta.

p = function('p')(N)   # Declare p to be a function of N
```

In [3]:
```
# DE solver (uses Maxima). First argument is DE, substituting for r.
# Other args are dependent and independent vars. (_C is constant)

sol1 = desolve( diff(p,N)/p - (1-2*b*N-a)/((a+b*N)*N) , p, ivar=N );
print(sol1)
```

```
_C*e^(-(a + 1)*log(N*b + a)/a - (a - 1)*log(N)/a)
```

In [4]:
```
# Apply identity exp(log(x)) = x, and factor.

sol2 = sol1.canonicalize_radical(); print(sol2);
sol3 = sol2.factor(); print(sol3)
```

```
N^(1/a)*_C/((N^2*b + N*a)*(N*b + a)^(1/a))
(N*b + a)^(-1/a - 1)*N^(1/a - 1)*_C
```

Subtract given solution for $P(N)$, again substituting for r.

In [5]:
```
var('_C')
should_be_zero = sol3 - _C / (N*(a + b*N)) * (N / (a + b*N))^(1/a);
should_be_zero.canonicalize_radical()   # Simplify powers.
```

Out[5]:
```
0
```

C Further differential equations for variable r

Rearrange differential equation (4) and use linear $r(N) = \alpha - \beta N$ so that $dr/dN = -\beta$

$$\frac{dP}{P} = \frac{dN}{N}\frac{1-r+\beta N}{r}$$

Eq (2) implies $dR/R = dr/r + dN/N + dP/P$, allowing elimination of dN/N

$$\frac{dP}{P} = \left(\frac{dR}{R} - \frac{dr}{r} - \frac{dP}{P}\right)\frac{1-r+\beta N}{r}$$

Now eliminate dr/r using

$$\begin{aligned} r &= \alpha - \beta\frac{R}{rP} \\ 0 &= r^2 - \alpha r + \beta\frac{R}{P} \\ \frac{dr}{r} &= \frac{-\beta N}{r-\beta N}\left(\frac{dR}{R} - \frac{dP}{P}\right) \end{aligned}$$

giving

$$\begin{aligned} \frac{dP}{P} &= \left(\frac{dR}{R} + \frac{\beta N}{r-\beta N}\left(\frac{dR}{R} - \frac{dP}{P}\right) - \frac{dP}{P}\right)\frac{1-r+\beta N}{r} \\ &= \left(\frac{dR}{R} - \frac{dP}{P}\right)\left(1 + \frac{\beta N}{r-\beta N}\right)\frac{1-r+\beta N}{r} \\ &= \left(\frac{dR}{R} - \frac{dP}{P}\right)\frac{1-r+\beta N}{r-\beta N} \end{aligned}$$

finally giving

$$\frac{dP}{P} = (1-r+\beta N)\frac{dR}{R}$$

Alternatively differentiate $P = \frac{\omega^\alpha}{r^2}R^{1-\alpha}$. Deriving the differential equation for the $N-R$ pair is similar.