ARTONOMOUS MECHANISMS DEFINITIONS

MICHAEL ZARGHAM

Formal definitions of the Artonomous economy and component mechanisms for consideration and Review by Architect and Principle Engineer, Simon De La Rouviere.

1. System State Variable Definitions

As simple preliminaries define the Ethereum network block height to be indexed by k, the set of all Ethereum addresses to be denoted $\mathcal{A}$, the address of the Artonomous contract to by $\alpha \in \mathcal{A}$ and that all other Ethereum addresses may be references as some $a \in \mathcal{A}$.

Definition 1. *Define the* ***Gallery*** *to the set of unique Artworks owned by the Artonomous Contract. The set will be denoted $\mathcal{G}$ for Gallery and each unique artwork in $w \in \mathcal{G}$ is a non-fungible token whose state is stored by the Artonomous contract. The set of all works is given by $\mathcal{W}$.*

For any work $w \in \mathcal{W}$, there is mapping

$$\text{Owner} : \mathcal{W} \to \mathcal{A} \tag{1}$$

that is to say, that for any $w \in \mathcal{W}$ there is an

$$a(w) := \text{Owner}(w) \in \mathcal{A} \tag{2}$$

is the address that owns the artwork w. Furthermore, the Gallery is formally the set

$$\mathcal{G} = \{w \in \mathcal{W} | a(w) = \alpha\} \subseteq \mathcal{W}. \tag{3}$$

Definition 2. *The data containing the* ***Blueprint*** *for each artwork w must also be contained in the non-fungible token. For the purpose of this system level analysis that data is defined abstractly as a mapping.*

For any work $w \in \mathcal{W}$, there is mapping

$$\text{Data} : \mathcal{W} \to \mathcal{D} \tag{4}$$

where $\mathcal{D}$ is the domain of the artwork blueprints. This can be thought of as the custom data type which which be defined by some struct within the NFT definition. It suffices to to say, that for any $w \in \mathcal{W}$ there is an

$$d(w) := \text{Data}(w) \in \mathcal{D}. \tag{5}$$

It is assumed that there is some logic component that case decode any $d \in \mathcal{D}$ to render the artwork as a result of simply querying the data $d(w)$ from token w. Note, an interesting feature might be to allow the owner $a(w)$ to determine permissions for querying the blueprint $d(w)$ from contract α. Further note that while the Blueprint for any given artwork is unchanging in k, the owner account can be expected to change. All artwork w has owner $a(w) = \alpha$ in the block $k_0(w)$ which is the block when that artwork was created.

Definition 3. *The Ethereum Balance of the Artonomous Control called the* ***Pool*** *is an explicit state of the contract α in the Ethereum network. Denote the value of the Pool $E_\alpha(k)$ at block height k.*

Further, establish the notation that E_a is the balance in Ethereum of any account $a \in \mathcal{A}$. The Balance of the Pool is the central state variable of the Artonomous Artist Economy; this value serves as the central coupling variable interrelating the component mechanisms presented in the following section.

Definition 4. *The Artonomous Contract may issue a fungible token called a* ***Soul*** *Token in exchange for Ethereum. The balance of Soul owned by any address a is given by $S_a(k)$ The total Soul floating in the Ethereum network is*

$$S(k) = \sum_{a \in \mathcal{A}} S_a(k)$$

which is a state variable immediately observable from Artonomous contract.

The Artonomous Artist may have a balance of Souls S_α. It is proposed that this balance be created in accordance with the initial Ether balance of the deployed main-net contract α in a quantity consistent with the Bonding Curve equations as defined by the Bonding mechanism in the following section. An important consequence of the Artonomous Contract owning Soul is that all other Patrons can only collectively extract

$$\Delta E(k) = \frac{S(k) - S_\alpha(k)}{S(k)} E_\alpha(k) \tag{6}$$

at anytime k, providing us a means of demonstrating that a particular set of designed mechanisms allow the Autonomous Artist resilience to failure by running out of funds. Note that (6) assumes a proportional withdrawal mechanism as described in the Artononous Readme.

2. System Component Definitions

In this section each of the four mechanisms which interact as part of the Artonomous economy are defined. Those mechanisms are

(1) Art Generation and NFT Minting
(2) Art Sale - Auction Mechanism
(3) Patron Bonding mechanism - Soul Minting
(4) Patron Withdrawal mechanism - Soul Burning

Definition 5. *The Art Generation Mechanism is a private method of the Artonomous contract only to be used by the Bot responsible for triggering the art generation event each day. Note that due to the passivity of smart contracts, some off-chain actor must broadcast this transaction. It is however necessary to define the cost of this action. Define the* *generation event of artwork w to be $g(w)$ and the block height of $g(w)$ to be $k_0(w)$. The cost of generating artwork w denoted in Ether is $c(w)$.*

It is out of scope for this analysis to specific the extent to which the art generation code lives in the off-chain bot or in the on-chain method. What is in scope is accounting for the impact of an artwork generation event on the Pool.

$$E_\alpha^+ = E_\alpha - c(w) \tag{7}$$

where this update occurs during block $k_0(w)$. It is insufficient to represent this as

$$E_\alpha(k_0+1) = E_\alpha(k_o) - c(w)$$

because other transactions effecting the balance E_α may occur during block k_0. The $^+$ notation is used for discrete event state updates that occur with the ordered list of transactions that make up block k_0. For more details see [1].

Definition 6. *The **Auction** Mechanism is the mathematical inner workings of the public purchase method which allows any user to buy a piece of artwork in the Gallery. Denote the price of purchases artwork $w \in \mathcal{G}$ as $p_w(\kappa)$ where $\kappa = k - k_0(w)$ represents the period of time that w has been in the Gallery.*

Any acceptable Auction Mechanism must have the form

$$\text{Price} : \mathcal{W} \times \mathbb{W} \rightarrow \mathbb{R}_+ \tag{8}$$

where $\mathbb{W} = \{0, 1, 2, ...\}$ is the set of whole numbers and $\mathbb{R}_+$ is nonnegative real numbers. Modeling the output as a nonnegative real is sufficient for modeling purposed but the implementation with in fact require an Integer data type consistent with the Ether cryptocurrency.

The author proposes the following construction:

- Define a global parameter $\gamma \in (0, 1)$ to be the exponential discounting rate
- Set a local variable p_0 to be equal to the largest purchase price that occurred in the last week (approximated by block range)
- At the generation event define
$$p_w(0) = p_0$$
- For each subsequent block decrement
$$p_w(\kappa) = \gamma \cdot p_w(\kappa - 1)$$

Note that this method is consistent with the inexact backtracking line search, a common tool in convex optimization. Implementation notes: the value γ must be stored as two integers η and β such that $\gamma = \frac{\eta}{\beta}$ and $\eta < \beta$ each decrement is subject to rounding errors caused by rounding errors in approximating floating point math with integers.

The event where an artwork w is purchased occurs at block $k_1(w)$, and therefore yields revenue according to

$$E_\alpha^+ = E_\alpha + p_w\left(k_1(w) - k_0(w)\right) \tag{9}$$

for artwork w, where $p_w\left(k_1(w) - k_0(w)\right)$ is computed at the time transaction itself is computed.

The goal of this mechanism is to provide collectors a good opportunity to purchase the artwork at their bid price without requiring extensive transactions. The value p_0 is created at the generation event and the Artonomous can always compute the price associated with a purchase event as part of resolving the transaction. Cite the Cryptokitties auction contract which uses a linear declining price auction with similar mechanics.

Definition 7. *The **Bonding** Mechanism is the mathematic inner workings of the public method which mints Soul in exchange for Ether. The mechanism is defined as a bonding curve which is a special case of a value function as defined in* [1]. *Define the bonding function as* $B(E_\alpha, S)$.

A simple separable construction would be

$$B(E_\alpha, S) = \frac{g(E_\alpha)}{f(S)}. \tag{10}$$

Interpreting $B(E_\alpha, S) = c$ as invariant the Bonding Mechanism must attempt to enforce,

$$f(S) = c \cdot g(E_\alpha), \tag{11}$$

it suffices to set $c = 1$ as any desired constants can be encoded in $f(\cdot)$ and $g(\cdot)$. A bonding curve is generally expressed with $f(S) = S$ so that it can be interpreted as

$$S = g(E_\alpha) \tag{12}$$

which implies an instantaneous price

$$\frac{\partial B(e,S)}{\partial e} = \frac{\partial g(e)}{\partial e}. \tag{13}$$

The author defers on proposing a bonding curve but will demonstrate the concept by discussing the quadratic bonding curve where $f(x) = x$ and $g(y) = y^2/2$, applied as

$$\begin{aligned} f(S) &= S && (14)\\ h(E_\alpha) &= \frac{E_\alpha^2}{2} && (15)\\ B(E_\alpha, S) &= \frac{E_\alpha^2}{2S}. && (16) \end{aligned}$$

This construct implies an instantaneous of the value of Soul in Ether as

$$\frac{\partial B(e,S)}{\partial e}\Big|_{e=E_\alpha} = \frac{E_\alpha}{S} \tag{17}$$

Ether per Soul, a value directly queriable from the Artonomous Conrtact. However, bonding Ether to the Artononmous contract is not determined by this spot price. The Bonding curve, being a special case of an invariant allows direct computation of the minted Soul for any Ether bonding transaction via invariant conservation. In the general case, the spot price computed by manipulating the invariant equation

Suppose, the current state of the Bonding curve is $B(E_\alpha, S)$ and a user engages with the Artonomous contract by making a bonding transaction that sends an amount of Ether e. Then the amount of Soul minted to the message sender is given by the requirement that

$$B(E_\alpha + e, S + s) = B(E_\alpha, S). \tag{18}$$

In the quadratic case,

$$\frac{(E_\alpha + e)^2}{2(S+s)} = \frac{E_\alpha^2}{2S} \tag{19}$$

and it suffices to solve for s,

$$s = s(e, E_\alpha, S) = \left(2\frac{e}{E_\alpha} + e^2\right) \cdot S \tag{20}$$

Such an invariant based derivation means that the designer may choose any bonding curve with $f(S) = S$ and can reasonably expect to have a simply computable mechanism. More complex mechanisms may be designed for general $f(S)$ but the calculus becomes more difficult and in many cases impractical for derivation or computation.

Having defined the Bonding mechanism as state dependent, it can be viewed as state update

$$\begin{align} E_\alpha^+ &= E_\alpha + e \tag{21}\\ S^+ &= S + s(e, E_\alpha, S) \tag{22}\\ &= \left(1 + 2\frac{e}{E_\alpha} + e^2\right) \cdot S \tag{23}\end{align}$$

for each user action characterized by Bonding an amount of Ether e and receiving an amount of soul $s(e, E_\alpha, S)$.

Definition 8. *The **Withdraw** Mechanism is the mathematical inner workings of the public method by which users sends s Soul to the Artonomous contract in exchange for $e = e(s, E_\alpha, S)$ Ether.*

As noted above the mechanism for withdrawals is stated in the existing Artonomous Documentation as a proportional share of the Pool. The associated equation for the mechanism is

$$e = e(s, E_\alpha, S) = \frac{s}{S} E_\alpha \tag{24}$$

resulting in state change equations

$$\begin{align} S^+ &= S - s \tag{25}\\ E_\alpha^+ &= E_\alpha - e(s, E_\alpha, S) \tag{26}\\ &= \left(1 - \frac{s}{S}\right) E_\alpha. \tag{27}\end{align}$$

Note that by observing that $s \leq S - S_\alpha$, the result in equation (6) for $\Delta E = E_\alpha^+ - E_\alpha$ is easily recovered algebraically

3. Behavior Model

In order to create an entire system model, it is not sufficient characterize how the mechanisms work, it is also required that behavioral models are defined for each of the user roles which will interact with these mechanisms. Two user types are considered, Patrons and Collectors, an account a may at any time be acting as an combination of these rules as determined by which mechanisms engaged with.

Definition 9. *The* ***Collector*** *role is characterized by buying, holding, selling, or trading artworks w. A collector a is assumed to have some private valuation $v_a(w)$ denominated in Ether for all artworks w. The Collector will decide to buy, sell, or trade artwork when a opportunity presents itself.*

For the purposes of this analysis, we need only consider the decision to buy from the Gallery. An opportunity to buy an artwork will be accepted if $v_a(w) > p_w(\kappa)$. Due to the backtracking nature of the auction presented, the Collector with the largest $v_a(w)$ is the most likely to purchase any particular work, but in the case that p_0 is too low, any agent with $v_a(w) > p_0$ may be the first to claim the work.

For the purpose of economy design testing an exogenous stochastic process will randomly generate a value $v(w)$ which represents the maximum any active Collector is willing to pay $\max_a v_a(w)$ for each work when it is generated. Note that this value accounts only for active Collectors and not Collectors who might wish to Purchase the artwork but are not monitoring the Gallery and thus cannot take the action. Modeling the period of attention of Collectors is out of scope at this time. The purchase of that artwork will be accounted for in the system precisely when $p_w(\kappa)$ falls below v_a.

The state update equations associated with the Collectors purchase action resolve according to equation (9) and $k_1(w) = k_0 + \kappa$ is blockheight when $p_w(\kappa) < v_a$. This is a *rational* model with respect to the private valuation of the artwork, however, that valuation can be based on anything, including random noise, so it is possible to model arbitrary irrational behavior using the simple $v_a(w)$ model.

At this time, trading behavior does not influence the Artonomous Economy state. If in the future, fees for trades were imposed, then additional revenue streams could only be accounted for by enhancing the behavioral model of collectors to include both attention and distributions of value functions in order to estimate the rates of artwork circulation and account for the related revenues.

Definition 10. *The* ***Patron*** *role is characterized by bonding, holding, trading or burning Soul. A Patron a is assumed to have some private perceived valuation of Soul V_a denominated in Ether and some quantity of Soul S_a.*

The private signals V_a maybe be rational or irrational or a mixture. Rational estimates are general derived from the spot prices, effective payout of liquidating ones entire balance and/or a project future value of these quantities. By starting with these quantities and adding noise to create value distributions, the the model effectively accounts for a mixture of rational and irrational behavior as encoded by the choice of stochastic process. Under the assumption that there is at any block k a distribution of private valuations of Soul it is possible model the system by assuming that Patron Agents will mint and burn their Soul for Ether at prices and in quantities equivalent to arbitraging against their private belief of the Soul value. The effect of decomposing the behavior model in this manner is that agents are always mathematically rational with respect to their signal but that private signal itself is capable of encoding irrational beliefs, which are in turn captured via stochastic process models used in creating the value distribution.

In order to implement a system level model of user behavior, construct a balance weight distribution, which one can think of as a histogram of prices weighted by quantities of Soul tokens. This mathematical object may sound exotic, but an order book is essentially the same data object. Define our histogram bins as as the ordered list of values $r \in \mathbb{R}_+^{n+1}$ such that

$$r_i = i \cdot \frac{r_{max}}{n} \tag{28}$$

for $i \in \{0, 1, 2, \ldots, n\}$. There are n bins and bin i covers range $[r_i, r_{i+1})$ and the final element, $r_n = r_{max}$. Our order book like histogram, can then be defined as $H \in \mathbb{R}_+^n$ where

$$H_i = \sum_{a \in \{a | r_i \leq V_a < r_{i+1}\}} V_a \cdot S_a. \tag{29}$$

This histogram view allows us to consider the Patrons as state dependent actors with out needing to handle all the dimensional complexities that arise from a Linear Time Expanding (LTE) system as outlined in [1].

At any block k, the spot price estimate of Soul Tokens in Ether is computed according to equation (17),

$$P = \frac{E_\alpha}{S}. \tag{30}$$

The value P must fall in some bin j, $P \in [r_j, r_{j+1})$. Let us assume that agents in bin j have insufficient incentive to act. For the purpose of deriving actions, consider each bin to act as an aggregate agent i with Soul value belief

$$\bar{V_i} = \frac{r_{j+1} - r_j}{2} \tag{31}$$

with total balance H_i.

For all bins $i < j$ the Soul tokens the Patrons possess are valued by the Artonomous contract higher than by the agents, that is $\bar{V_i} \geq P$. Therefore arbitrage actions involve burning Soul Tokens in exchange for Ether to the extent that Artonomous contracts estimate P can be expected to move to $\bar{V_i}$, which these agents may compute using the Bonding curve and spot price equations. Consider an action s_i respecting mechanism (24) such that the following constraint remains true:

$$\frac{E_\alpha - e_i(s_i, E_\alpha, S)}{S - s_i} \leq \bar{V_i}. \tag{32}$$

However, the ratio $P^+ = \frac{E_\alpha + e_i}{S + s_i}$ is conserved over all pairs (s_i, e_i) respecting equation (24), so the rational response is to sell up to H_i. In order to provide additional control in the simulation, add a parameter $\phi \in (0,1]$ representing the percentage of the Soul to be burned, resulting the state update equation

$$\begin{aligned} H_i^+ &= \phi H_i \ \forall\, i < j \qquad (33)\\ S^+ &= S - \phi \sum_{i<j} H_i \qquad (34)\\ E_\alpha^+ &= E_\alpha - \sum_{i<j} e_i(s_i, E_\alpha, S) \qquad (35)\\ &= E_\alpha \left(1 - \frac{\phi \sum_{i<j} H_i}{S}\right) \qquad (36) \end{aligned}$$

Now let us consider, the bins bins $i > j$ the Soul tokens the Patrons posses are valued by the Artonomous contract lower than by the agents, that is $\bar{V}_i \leq P$. Therefore therefore arbitrage actions involve bonding Ether in order to Mint Soul tokens to the extent that the Artonomous contracts estimate P can be expected to move to $\bar{V}_i$, which these agents may compute using the Bonding curve equation. Consider an action e_i respecting mechanism (20) such that the following constraint remains true:

$$\frac{E_\alpha + e_i}{S + s_i(e_i, E_\alpha, S)} \geq \bar{V}_i. \qquad (37)$$

The maximal arbitrage action would be to choose $\hat{e}_i$ such that the constraint above is met with equality. The action is to be defined as a fixed fraction θ of the maximal action, $e_i = \max\{0, \theta\hat{e}_i\}$. Computing that action $\hat{e}_i$ satisfies the equation

$$E_\alpha + \hat{e}_i = \bar{V}_i \cdot S \cdot \left(1 + 2\frac{\hat{e}_i}{E_\alpha} + \hat{e}_i^2\right) \qquad (38)$$

which may be reorganized as

$$\hat{e}_i^2 + \frac{1}{E_\alpha}\left(2 - \frac{E_\alpha}{V_i \cdot S}\right)\hat{e}_i + \left(1 - \frac{E_\alpha}{V_i \cdot S}\right) = 0, \qquad (39)$$

and solved via the quadratic equation, at taking the root further right on the real line

$$\hat{e}_i = \mathrm{Re}\left[\frac{1}{2V_i \cdot S} - \frac{1}{E_\alpha} + \sqrt{\frac{E_\alpha}{V_i \cdot S} + \frac{1}{4V_i^2 \cdot S^2} + \frac{1}{E_\alpha^2} - \frac{1}{V_i \cdot S} - 1}\right]. \qquad (40)$$

The resulting state update equations are left in implicitly in terms of

$$\begin{aligned} &e_i(V_i, E_\alpha, S) = \qquad (41)\\ &\qquad \theta \cdot \max\left\{0, \mathrm{Re}\left[\frac{1}{2V_i \cdot S} - \frac{1}{E_\alpha} + \sqrt{\frac{E_\alpha}{V_i \cdot S} + \frac{1}{4V_i^2 \cdot S^2} + \frac{1}{E_\alpha^2} - \frac{1}{V_i \cdot S} - 1}\right]\right\} \end{aligned}$$

with the amount of Soul being minted calculated as

$$\begin{aligned}
s_i(V_i, E_\alpha, S) &= s_i(e_i, E_\alpha, S) && (42)\\
&= \left(2\frac{e_i(V_i, E_\alpha, S)}{E_\alpha} + e_i^2(V_i, E_\alpha, S)\right)\cdot S && (43)\\
&= \left(2\frac{e_i}{E_\alpha} + e_i^2\right) S. && (44)
\end{aligned}$$

As inelegant as this equation is, it is directly computable from the state and thus can be implemented as part of the simulated behavior. Note that the complexity arises for the function $g(x)$ in definition of the bonding curve, indicating that the designer should have care when considering nonlinear bonding curve functions. **With luck upon careful review by others, we'll find a bug in the derivations and this can get cleaned up.**

The system wide state update as a result of the minting process is defined as

$$\begin{aligned}
H_i^+ &= H_i + \theta\cdot[\hat{e}_i]_+ \;\forall\, i > j && (45)\\
E_\alpha^+ &= E_\alpha + \sum_{i>j}\theta\cdot[\hat{e}_i]_+ && (46)\\
S^+ &= S + \theta\sum_{i>j}\left(2\frac{[\hat{e}_i]_+}{E_\alpha} + \theta\cdot[\hat{e}_i]_+^2\right) S && (47)
\end{aligned}$$

implicitly defined in terms of $[\hat{e}_i]_+$ where $[\cdot]_+$ denotes the positive projection and $\hat{e}_i$ is computed from the previous state according to equation (40).

4. Economic System Discrete Differential Equations

All of the definitions and derivations in the preceding sections exist for the purpose of having a well defined discrete dynamical system model characterized by state feedback mechanisms and well defined driving stochastic processes.

$$\begin{aligned}
\mathcal{G}(k+1) &= (\mathcal{G}(k)\setminus\{w : k_1(w) = k\}) \cup \{w : k_0(w) = k\} && (48)\\
E_\alpha(k+1) &= E_\alpha(k)\cdot\left(1 - \frac{\phi\sum_{i<j} H_i}{S}\right) + \sum_{i>j}\theta\cdot[\hat{e}_i]_+ && (49)\\
&\quad + \sum_{w\in\{w:k_1(w)=k\}} p_w\left(k - k_0(w)\right) \quad - \sum_{w\in\{w:k_0(w)=k\}} c(w) && (50)\\
S(k+1) &= S\cdot\left(1 + \theta\sum_{i>j}\left(2\frac{[\hat{e}_i]_+}{E_\alpha} + \theta\cdot[\hat{e}_i]_+^2\right)\right) - \phi\sum_{i<j} H_i && (51)\\
H_i(k+1) &= \phi H_i(k)\;\forall\, i < j && (52)\\
H_i(k+1) &= H_i(k) + \theta\cdot[\hat{e}_i]_+ \;\forall\, i > j. && (53)
\end{aligned}$$

Under this model the implied price of Soul token in Ether is given by

$$P(k) = \frac{E_\alpha(k)}{S(k)} \tag{54}$$

at every block k.

To iterate a simulation using this differential equation it is necessary to choose a distribution for the artwork values v_w and to select from that distribution a value for each artwork w generated. It is also necessary to draw belief distribution V_i for all bins i.

It would be possible to further drive the system with evolving private beliefs of V_i by defining a state dependent linear transformation

$$V(k+1) = \lambda \cdot TV(k) + (1-\lambda) \cdot P(k)\vec{\mathbf{1}} + \delta(k) \tag{55}$$

where T is stochastic matrix representing mixing of opinions and $P(k)\vec{\mathbf{1}}$ represents the influence of the observed price. The $\vec{\mathbf{1}}$ notation is the vector of all ones. The relative weight of the opinion mixing process and the observed value are capture by a convex combination weighted by $\lambda \in (0,1)$. The additional term $\delta(k) \in \mathbb{R}$ is a noise model.

A final note on this addition driving stochastic process: the result of updating the vector V is an update to the vector H. This can be handled between iterations. It is effectively a coordinate transformation. Fortunately this is a relatively straight-forward process thanks to linearity.

5. Future Work

Write simulations in python. Profit! (a.k.a. iterate mechanism design and testing until desired economy level properties emerge).

References

[1] Michael Zargham, Zixuan Zhang, Victor Preciado *A State-Space Modeling Framework for Engineering Blockchain-Enabled Economic Systems*, `https://github.com/BlockScience/artonomous/blob/master/token_engineering/Reference/ICCS2018.pdf` 2018.