From Curved Bonding to Configuration Spaces

Michael Zargham*, Jamsheed Shorish† and Krzysztof Paruch‡
Research Institute for Cryptoeconomics
Vienna University of Economics and Business
Vienna, Austria
e-mail: *Michael.Zargham@wu.ac.at, †Jamsheed.Shorish@wu.ac.at, ‡Krzysztof.Paruch@wu.ac.at

***Abstract*—Bonding curves are continuous liquidity mechanisms which are used in market design for cryptographically-supported token economies. Tokens are atomic units of state information which are cryptographically verifiable in peer-to-peer networks. Bonding curves are an example of an enforceable mechanism through which participating agents influence this state. By designing such mechanisms, an engineer may establish the topological structure of a token economy without presupposing the utilities or associated actions of the agents within that economy. This is accomplished by introducing configuration spaces, which are proper subsets of the global state space representing all achievable states under the designed mechanisms. Any global properties true for all points in the configuration space are true for all possible sequences of actions on the part of agents. This paper generalizes the notion of a bonding curve to formalize the relationship between cryptographically enforced mechanisms and their associated configuration spaces, using invariant properties of conservation functions. We then proceed to apply this framework to analyze the augmented bonding curve design, which is currently under development by a project in the non-profit funding sector.**

***Index Terms*—Economics, Blockchain, Dynamic Games**

I. Introduction

Cryptoeconomic systems [1] are digital data-driven economies facilitated by distributed ledger technology (DLT), such as blockchain, and making use of cryptographic tokens acting as information carriers within the system [2]. The properties of this technology permit the maintenance of a tamper-proof state layer (see e.g. [3]) describing economic activities within the system in real time. These economies are dynamic, adaptive and multiscale systems [4] and comprise micro-foundational agent behaviors, meso-institutional policy restrictions and macro-systemic effects that emerge on a global level. The state layer preserves properties, acting as a link between actions, events and results.

Multiscale systems often possess complicated, nonlinear dynamics and feedback effects, leading to emergent properties [5] that cannot be discerned from an isolated examination at each scale. Complexity is compounded when multiple mechanisms are available concurrently, [6]. Structure can be added by introducing restrictions that shape the reachable system states, while at the same time imposing minimal behavioral assumptions upon system participants. Desirable macro-system properties are taken as invariant and upheld through conservation equations as part of the derivations of the systems mechanisms. Implementing these property-preserving mechanisms thus crucially influences the system's evolution.

One important mechanism is the token bonding curve, which has gained attention in the cryptoeconomics community [7], [8] as an alternative means of funding (replacing ICOs) and as a financial instrument [9], [10] for tokens. Serving simultaneously as means of funding, liquidity provider and market maker, bonding curves are powerful tools because the tokens they issue can represent access or voting rights. In the case in continuous organizations [11], the tokens are rights to future revenues of a startup. In the augmented bonding curve [12], they are rights to steer funds in a not-for-profit organization.

This work generalizes bonding curves to configuration spaces which may be described as manifolds characterized by the enforced conservation of one or more desired global properties. In a computationally mediated economic system properties are asserted using potential functions [13] and may be further enforced as *conservation functions* (cf. Section III-A), which simplifies the possible system trajectories. This dimensionality reduction causes the reachable state space, known as the *configuration space* [14], to guarantee desired properties that are not guaranteed in the *ex ante* state space. There is thus a mapping that can associate to (each set of) conservation functions a configuration space that is itself a proper subset of the global state space.

The paper is structured as follows: Section II introduces the state space representation of a shared data environment, such as a DLT or blockchain cryptoeconomic system. Section III introduces conservation functions, and demonstrates theoretically how the invariance (and hence enforcement) of global properties defines the configuration space as a subset of achievable system states. Section IV then presents an augmented bonding curve as an example of an enforceable mechanism and defines the resulting configuration space. The connection between the invariant properties of the bonding curves and the space space constraints is demonstrated, and numerical simulation results are provided in support of the connection between micro-level mechanisms and their associated global properties. Finally, Section V outlines future work.

II. State Space Representation[1]

To build the framework incorporating the micro, meso and macro level activities requires a harmonized state space model,

[1]This section parallels extant work of [15] and [16] but does not require the formal ledger or block structure to define the state space representation.

so that both system requirements and participating agent actions spaces can be defined. The resulting dynamical system defines state transitions that rely upon individual and collective decision-making, but do not require centralized coordination to aggregate micro elements into a macro scale evolutionary process.

Time $t = 1, 2, \ldots$ is assumed to be discrete—this allows for agent actions to be realistically modeled and for state transitions to be indexed according to a clock cycle of the required fidelity. Provided that the proper mapping of events to time steps is observed, passage to the continuous limit (affording the use of e.g. differential equation modeling if preferred) is always possible, resulting in a formulation comparable to population games [17] with a focus on energy conservation and passivity, [18].

The state space $\mathbf{X}$ may be interpreted as that collection of variables which serve to define the system at any point in time. In what follows we shall focus upon $\mathbf{X} \subseteq \mathbb{R}^n$ for some $n < \infty$, but in general different components of $\mathbf{X}$ may belong to different spaces.

Definition 1. *The **state** $x \in \mathbf{X}$ summarizes the system at a given point in time, in the sense that a state-dependent action or outcome mapping to the immediate future state need only condition upon x.*

The state model's micro foundations are defined over how participating agents interact in a peer-to-peer environment. Agents are assumed to interact by accessing part of a shared state (defined momentarily), with access rights secured in some fashion (e.g. public-key encryption, trusted tokens etc.). That part of the shared state accessible by the agent is indexed by an *address*, which acts as an identifier of one or more agents.[2]

Definition 2. *An **address** a is an index of a shared state that facilitates actions taken by an agent. The set of addresses for a given realization of agents is denoted by $\mathbf{A}$.*

Definition 3. *The **shared** or **local state space** is a subset $X_a \subseteq \mathbf{X}$, $a \in \mathbf{A}$, indicating that part of the global state $\mathbf{X}$ that the agent(s) with access to address a can directly influence. A **local state** $x_a \in X_a$ is a projection of the global state $x \in \mathbf{X}$ onto X_a.*

Agents may condition upon information in their shared state, taking an *action* that, in conjunction with a global state $x \in \mathbf{X}$, leads to a new global state x'. Note that the set of feasible actions taken by an agent is dependent upon the state x, which is assumed to incorporate those restrictions (legal or otherwise) which affect an action.

Definition 4. *An **action** $u_a \in U(X_a; x)$ for an agent with address a is any activity under the control of the agent that may influence the state of the system. The set $U(X_a; x)$ represents the set of feasible actions, given agent a's local state space X_a, and the global state x (which may be hidden from the agent). Denote the set of all possible sets of feasible actions, over all agents, local states and global states, by $\mathcal{U}$, and a generic element of $\mathcal{U}$ by $\mathbf{U}$.*

[2]An address may index more than one agent if a subset of agents is required to perform an action, as is the case in multi-signature encryption.

Armed with this definition, we may now define how an agent incorporates state information and their action to influence the future state:

Definition 5. *A **mechanism** is a mapping $f : \mathbf{X} \times \mathbf{U} \to \mathbf{X}$ taking the current state $x \in \mathbf{X}$ and an action $u \in \mathbf{U}$ and returning a future state x':*

$$x' := f(x, u).$$

Denote the set of all mechanisms by $\mathbf{F}$.

Note that it is possible for mechanisms to not support actions, i.e. it can be that, for a given selection $\hat{u} \in \mathbf{U}$,

$$f(x, \hat{u}) = x \quad \forall x \in \mathbf{X}.$$

This reflects the fact that certain mechanisms may not allow certain actions to influence the state, e.g. if those actions are invalid for the selected mechanism.[3] Generally we assume that, in response to the local state x_a and the (possibly hidden from the agent) global state x, an agent indexed by a will be able to select among a set of alternative mechanisms (so that the state and agent restrict the mechanism, rather than the mechanism restricting the action). An agent will thus select from a subset $F(a; x) \subseteq \mathbf{F}$.

Definition 6. *A **transaction** is a tuple $(a, u, f) \in \mathbf{A} \times \mathbf{U} \times \mathbf{F}$. A transaction is said to be **valid** if, given global state x,*

1) $u \in U(X_a; x)$,
2) $f \in F(a; x)$.

When a transaction occurs at time t we shall have occasion to emphasize this by subscripting, so that $f_t \equiv f$, $u_t \equiv u$ for transaction (a, u, f).

In what follows we assume that, although there are many agents in the system (indexed by $a \in \mathbf{A}$), there are no *collisions* between agents, i.e. agents do not simultaneously select a mechanism and associated action to update the state from x to x'. Rather, updates are indexed by arrival time t and such an update is referred to as *atomic*. With this specification, it is now possible to define the transitions between states as a sequence of transactions:

Definition 7. *A **state transition** at time t is the selection of a future state x' in response to a valid transaction (a, u_t, f_t),*

$$x' = f_t(u_t, x),\ u_t \in U(X_a; x),\ f_t \in F(a; x). \qquad (1)$$

This exposition is sufficient to identify transitions in the state of the system with selections by agents of 1) mechanisms and 2) actions, relying upon local information, but influenced by (and depending upon) the global state.

[3]Other methods, such as restricting the action set by mechanism, can also be used to exclude the impact of certain actions upon the state. Our selection is parsimonious and is made without loss of generality.

At first, the resulting dynamical system summarized by (1) may appear to live in a potentially high-dimensional space, with representative graph $(x, x') \in \mathbf{X} \times \mathbf{X}$. However, the structure of the system can be extended by placing internally consistent restrictions upon the dynamics, lowering the dimension of the resulting induced state space, called the *configuration space*.

III. Configuration Space

The configuration space serves the role of enforcing desirable macro-economic properties, while retaining sufficient degrees of freedom for the agents at the micro level to act according to their own private preferences. It is these preferences that induce the selection of an action, u, from possible actions $U(X_a; x)$, but these preferences need not be 'known' by any other participant of the system. Through the selected mechanism f, the system incorporates agent decisions and selects a new state from the enforced set of alternatives, which is the configuration space. Table I illustrates this passage of scale from micro (agent) to macro (system) levels.

TABLE I: Relating Agent Behavior to System State

Scale	Level of Abstraction	
	Possible	***Actual***
Agent	Action Set $U(X_a; x)$	Actions $u \in U(X_a; x)$
System	Configuration Space $\mathbf{X_C}$	realization $x' = f(u, x) \in \mathbf{X_C}$

A. Conservation Functions and Invariance

The enforcement of desired properties of the system is accomplished through the use of *conservation functions*. Conservation functions are output functions engineered to encode desired global properties. By limiting their values to be scalars, additional mathematical equipment can be brought to bear regarding convergence properties.

Definition 8. *A* ***conservation function*** *is a scalar function of the state of the economic network*

$$V : \mathbf{X} \to \mathbb{R}$$

encoding a desired property.

A conservation function is a representation or measure of a property, and must be constructed specifically for each particular property under scrutiny. Consider as one such property the imposition of an equality constraint upon the system. Such a constraint might be relevant, for example, in the Bitcoin network, where the equality constraint enforces the no-double-spending rule.

An *unchanging* property can be represented by a real-valued conservation function V provided that, for all state trajectories $x_0, x_1, \ldots$, $V(x_t) = c \in \mathbb{R}$. In other words, regardless of the state x_t achieved by the system, the conservation function $V(x_t)$ is *invariant*:

Definition 9. *A conservation function V is* ***invariant*** *if, given the sequence of states $x_0, x_1, \ldots$ generated by state transition equation (1), $V(x_{t+1}) \equiv V(x_t)\ \forall t = 0, 1, \ldots$*

A sufficient condition for a conservation function to be invariant is that the value of the conservation function remains unchanged for a sequence of state transitions allowable under the available mechanisms.

Proposition 1. *Given an initial state $x \in \mathbf{X}$, if*

$$V(f(u, x)) \equiv V(x) \tag{2}$$

for all mechanisms $f \in \mathbf{F}$ and all $u \in \mathbf{U}$, then V is invariant.

Proof. Since a state transition (cf. equation 1) requires a mechanism from $\mathbf{F}$ and an action from $\mathbf{U}$, the condition of the proposition is fulfilled for actual state trajectories:

$$V(x_{t+1}) = f_t(u_t, x_t)) \equiv V(x_t).$$

□

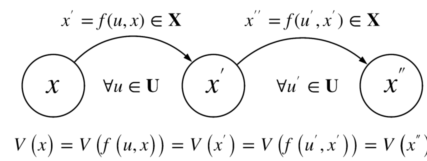

Fig. 1: Illustration of state transitions where the conservation function V is invariant for all $f \in \mathbf{F}$.

B. The Configuration Space

Although Proposition 1 is sufficient for a conservation function to be invariant, it is clearly not necessary as invariance is defined only over state transitions, i.e. transitions created from valid transactions. This raises the hope that by considering only that part of the state space $\mathbf{X}$ for which 1) state transitions are valid, and 2) the associated conservation function is invariant, there is a reduction in the degrees of the freedom of the system generating the sequence of observed states. In other words, the scope of the system's actually attainable states forms a proper subset of $\mathbf{X}$.

Definition 10. *The* ***configuration space*** *$\mathbf{X_C} \subset \mathbf{X}$ is a proper subset of the general state space, defined by state transition restrictions derived from valid transactions (a, u, f).*

To show that a configuration space exists requires a demonstration that the sequence of user action sets $\{U(X_a; x_t)\}$ and feasible mechanism sets $\{F(a; x_t)\}$ are each sequences of proper subsets of $\mathbf{U}$ and $\mathbf{F}$, respectively, so that the restrictions to $\mathbf{X}$ can be viewed as resulting from a set of constraints. If the constraints are well-behaved, an argument can be made that the configuration space is a submanifold of $\mathbf{X}$ defined by the constraint set.

A general theory supporting such a demonstration is not yet available and is relegated to future research, but a motivating example may help establish the role of the conservation function in determining the configuration space, and act as a prelude for the more general presentation in Section IV of the augmented bonding curve mechanism.

C. Example: Consumer Indifference and Invariance

Consider a resource allocation problem in which a representative consumer is deciding between differing consumption bundles.[4] Suppose that there are two goods, “beer” and “pizza”, with a representative quantity being denoted by (b, z), with b representing any quantity of beer (in, say, pints), and z representing any quantity of pizza (in, say, slices). We might suppose that quantities of beer and pizza can be infinitely divided, so that for simplicity $(b, z) \in \mathbf{X} := \mathbb{R}^2_+$. In this simple example, we define the *state* of the consumer as its selection $x := (b, z)$.

A consumer has preferences over different combinations of beer and pizza. For example, it might be that a ‘meal’ of only beer, i.e. a consumption bundle $(b, 0)$, is less preferred than a meal of twice as many slices of pizza as pints of beer, $(b, z) = (b, 2b)$. If the ordering over consumption bundles is well-behaved, there may exist a mapping between consumption bundles and the real line, such that any time one bundle is preferred to another by this consumer, that bundle receives a larger real value according to this mapping. Such a mapping $V : \mathbf{X} \to \mathbb{R}$ is called a *utility function*, and has a wide range of applicability in economics, finance and mathematical sociology, among other fields.

In general, a consumer may select any combination of beer and pizza they can afford. Supposing for this example that the consumer can afford any combination, any point in the entire state space $\mathbf{X}$ can represent the consumer’s state. But now suppose that the consumer is restricted to consuming bundles that achieve a particular level of utility, say $\bar{v}$. That is, the only consumption bundles that will be selected by the consumer are those for which

$$V(b, z) = \bar{v}. \tag{3}$$

This is an equality restriction on the consumption bundles that the consumer can select, and is referred to in the economics and finance literatures as an ‘indifference surface’ (or ‘indifference curve’ where there are only two consumption goods, as here). Mathematically, it is a *level set* of the function V.

We can add more structure and go further. Suppose that the utility function is continuously differentiable in both arguments and that it is strictly increasing in each argument. Then the implicit function theorem allows us to derive a *substitution function* $s : \mathbb{R}_+ \to \mathbb{R}_+$ between beer and pizza such that:

$$V(s(z), z) \equiv \bar{v}$$

with

$$s'(z) = -\frac{\partial V/\partial z}{\partial V/\partial b}.$$

In other words, given *any* quantity of pizza z, there exists a quantity of beer given by $s(z)$ such that the bundle $(b = s(z), z)$ has utility $\bar{v}$. The consumer’s state, then, has been *parametrized* by z, which is one-dimensional. The utility function V thus serves as a *conservation function*, because it holds the utility level invariant at $\bar{v}$ for any choice of z.

[4]For a comprehensive overview of consumer theory see e.g. [19].

Rather than examine states from the entire state space $\mathbf{X}$, then, it is sufficient to only consider those states for which the utility value $\bar{v}$ obtains, i.e. those $(s(z), z)$ combinations within $\mathbf{X}$. The set of all such combinations forms the *configuration space* for the consumer’s state, $\mathbf{X_C}$. The configuration state is one-dimensional because of the parametrization by z, and depends upon the utility value $\bar{v}$ because a different utility level selection creates a different configuration space for the consumer.

Finally, if dynamics were introduced into this (partial equilibrium) economy, and the consumer were allowed to change their consumption bundle over time, all the while respecting the utility restriction[5] to $\bar{v}$, then the resulting trajectory of states would be confined to $\mathbf{X_C}$. In this simple example such a confinement does not provide much in the way of savings, but with more restrictions over a larger state space the dimension reduction can be significant, as the following Section demonstrates.

IV. Augmented Bonding Curve Example

Public goods funding is a serious challenge in all sectors but it can be especially challenging for internet native communities who share an attention space but not a geographic space, such as open source development communities. Lacking a shared nation-state or other body charged with oversight of public goods, or tight knit social networks that include wealthy or connected individuals, it is all but impossible to secure sustainable funding without promising financial returns. The augmented bonding curve is a minimalist design which binds a community stakeholdership token to a set of rights or privileges within that community, including but not limited to governance rights over a pool of funds controlled by that community. Another example of such a right would be discounts on paid services provided by that community, [20].

The motivating requirements for this design are drawn from commons principles [21] and more broadly the field of ecological economics [22]. A key aspect of the design is that it allows the community members to freely increase or decrease their holding in these tokens through the bonding curve based on a variety of factors unique to both the community and the individuals. The bonding curve exists as a piece of political and economic infrastructure which serves the community in achieving its own ends, even when those ends are not simply to maximize shareholder value, as fiduciary duty would dictate in an equity based environment.

A. Augmented Bonding Curve State Space

The state space for an augmented bonding curve is comprised of various quantities of tokens which are implemented as very large integers, and may be reasonably approximated as real valued.

Definition 11. *The **Reserve** $R \in \mathbb{R}_{++}$ is the total quantity of reserve currency tokens bonded to the augmented bonding curve contract.*

[5]This restriction is used, for example, to derive the Hicksian *compensating variation* in consumer theory; see e.g. [19].

The first quantity in our state space represents a reserve currency, which is provided by a contract external to the community deploying the augmented bonding curve. This could be the native currency from the network providing consensus such as Ethereum, it may be a tokenized fiat such USDC, or any other token with provable state in the economic network.

Definition 12. *The **Supply** $S \in \mathbb{R}_{++}$ is the total quantity of local asset issued by the augmented bonding curve contract.*

The supply is the total quantity of the community asset that exists. Individual community members will hold these tokens, and the community may be considered the owners of the shared state addresses (cf. Definition 2):

Definition 13. *The **Community** $\mathcal{C} \subseteq \mathbf{A}$ is the set of addresses controlling the community tokens. That is to say $\mathcal{C} = \{a \in \mathbf{A} | s_a > 0\}$ where s_a is the quantity of the supply that is mapped to address a.*

The total supply S therefore always satisfies the constraint that

$$S = \sum_{a \in \mathcal{C}} s_a \tag{4}$$

Individual community members may assert their tokens s_a as part of any process defined within the community. For the purpose of the augmented bonding curve, it is assumed that this process is any voting process through which community members choose to fund initiatives.

Definition 14. *The **Funding Pool** $F \in \mathbb{R}_{++}$ is the total quantity of reserve currency tokens available for the community to allocate to initiatives.*

Some voting processes that may be used include: (i) one vote per address $a \in \mathcal{C}$, potentially with some threshold $s_a > s_{\min}$, (ii) one vote one token, where the voting power of each address a is s_a, (iii) quadratic voting, where the voting power of each address a is $\sqrt{s_a}$, [23]. Each of these methods has pros and cons, most notably their relative reliance on uniqueness of the mapping between address and individual identity. Tokenization also allows for dynamic voting processes such as Conviction Voting which are derived from dynamic optimization in the context of sensor fusion [24] by building on the theory of social choice [25], but viewing it as a dynamic process, [26].

The augmented bounding curve is designed such that individual community members can increase or decrease their holdings in the community asset by depositing the reserve currency to mint new community assets or burn their community assets to withdraw the reserve currency. The bonding curve is stateful, meaning that given the Supply and Reserve quantities it is possible to compute a spot price deterministically.

Definition 15. *The **Spot Price** $P \in \mathbb{R}_{++}$ is the instantaneous estimate of the value of the local asset whose units are the units of R per units of S.*

Since community members can freely move into and out of the bonding curve, the spot price may be interpreted as a dynamic estimate of the value of the community asset. The justification for this claim is further borne out by the characterization of the configuration space.

B. Configuration Space

Definition 16. *The **System State** $x := \{R, S, P, F\} \in \mathbf{X_C}$, where the configuration space $\mathbf{X_C} \subset \mathbf{X} := \mathbb{R}^4_{++}$ due to restrictions provided by the bonding curve mechanisms.*

The purpose of the state space mechanism design is to assert the state space properties and to derive the appropriate mechanisms from these properties. In the case of the augmented bonding curve, the purpose is to establish diminishing returns for both depositing and withdrawing reserve currency from the bonding curve. This may be established through restricting the relationship between R and S with an invariant.

Definition 17. *The (parametrized polynomial) **conservation function** is given by*

$$V(x) = V(R, S) := \frac{S^\kappa}{R} = V_0 \tag{5}$$

where $V_0 = V(R_0, S_0) = \frac{S_0^\kappa}{R_0}$ is a constant defined when the system is initialized with Supply S_0 and Reserve R_0. The parameter κ defines the curvature of the bonding curve.

Definition 17 allows us to characterize the spot price as a consequence of the conservation function acting to define the configuration space $\mathbf{X_C}$.

Proposition 2. *Consider the two dimensional phase space made up of all combinations R and S such that $(R, S) \in \mathbb{R}^2_{++}$, and let*

$$G := \{(R, S) \mid V(R, S) \equiv V_0\}$$

be the graph of the restriction of the conservation function V to the constant V_0. Then the spot price P is the slope of the tangent line to this graph, i.e.

$$P = p(R, S) := -\frac{\partial V / \partial S}{\partial V / \partial R}$$

at every $(R, S) \in G$, with $p(R, S)$ being the spot price at each point in G.

Proof. The conservation function V is infinitely differentiable, strictly increasing in S and strictly decreasing in R (cf. Definitions 11, 12 and 17). Given the identity $V(R, S) \equiv V_0$, then, the implicit function theorem can be applied and so there exists a function, say $\hat{p}(S)$, such that

$$V(\hat{p}(S), S) \equiv V_0$$

with

$$\hat{p}'(S) = -\frac{\partial V / \partial S}{\partial V / \partial R}.$$

From Definition 15 the spot price P is the instantaneous rate of substitution between R and S. But this is just the slope $\hat{p}'(S)$. Defining a function $p(R, S)$ by

$$p(R, S) := \hat{p}'(S)$$

for all $(R, S) \in G$ completes the proof. $\square$

TABLE II: Summary of Configuration Space Restrictions

Given State	Computed State		
	Reserve	*Supply*	*Spot Price*
Reserve	R	$\sqrt[\kappa]{V_0 R}$	$\frac{\kappa R^{(\kappa-1)/\kappa}}{V_0^{1/\kappa}}$
Supply	$\frac{S^\kappa}{V_0}$	S	$\frac{\kappa S^{\kappa-1}}{V_0}$
Both	R	S	$\frac{\kappa R}{S}$

Definition 18. *The **Configuration Space** $\mathbf{X_C}$ is a 2-manifold, created by applying two one-dimensional restrictions, $V(R, S) = V_0$ and $P = p(R, S)$ to the four dimensional state space $\mathbf{X}$:*

$$\mathbf{X_C} := \{x \in \mathbf{X} \mid V(R, S) = V_0,\ P = p(R, S)\}. \tag{6}$$

The funding pool dimension is unaffected by the restrictions, so another way of defining this configuration space is

$$\mathbf{X_C} = \mathcal{B} \times \mathbb{R}_{++} \tag{7}$$

where $\mathcal{B} := \{(R, S, P) \in \mathbb{R}^3_{++} | V(R, S) = V_0,\ P = p(R, S)\}$ is the configuration space for the bonding curve and $\mathbb{R}_{++}$ is the space for the Funding Pool F.

C. Mechanisms

The set of mechanisms is

$$\mathcal{F} := \{f_{bond}, f_{burn}, f_{allocate}, f_{deposit}\} \tag{8}$$

The first two mechanisms are the bonding curve mechanisms, whereas the latter two are related to the funding pool.

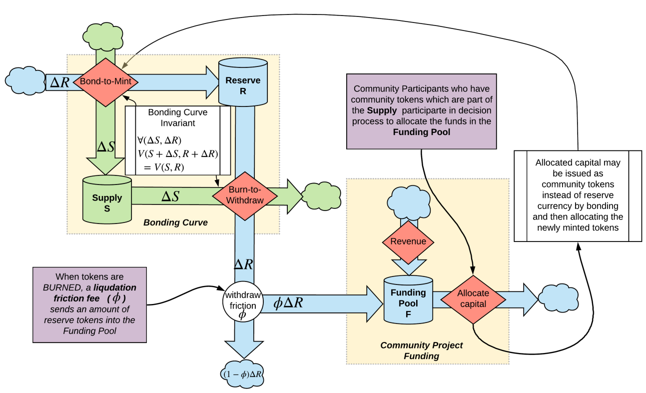

Fig. 2: Illustration of the bond-to-mint and burn-to-withdraw invariant preserving mechanisms as well as their structural relationship to the deposit and allocate mechanisms.

Definition 19. *The **Bond-to-Mint** mechanism $x' = f_{bond}(r, x)$ where $x \in \mathbf{X_C}$ is the state prior to the transaction and $x' \in \mathbf{X_C}$ is the posterior state. The action taken $r \in \mathbb{R}_{++}$ is a quantity of reserve currency transferred from the actor's address to the augmented bonding curve.*

$$R^+ = R + r \tag{9}$$

$$S^+ = \sqrt[\kappa]{V_0(R + r)} \tag{10}$$

$$P^+ = \frac{\kappa(R + r)^{(\kappa-1)/\kappa}}{V_0^{1/\kappa}} \tag{11}$$

$$F^+ = F. \tag{12}$$

The amount of tokens issued to the address that bonded r is

$$s = \sqrt[\kappa]{V_0(R + r)} - S \tag{13}$$

and the realized price is

$$\bar{P}(r) = \frac{r}{s} = \frac{r}{\sqrt[\kappa]{V_0(R + r)} - S}. \tag{14}$$

Lemma 1. *For $\kappa > 1$, the realized price $\bar{P}(r) > P$ for all $r > 0$ and the limit realized price is the current price P as the size of the bonded funds r tends to zero from the right:*

$$\lim_{r \to 0^+} \bar{P}(r) = P. \tag{15}$$

Proof. From Definition 19 equation (14) it follows that $\lim_{r\to 0^+} \bar{P}(r)$ is:

$$\lim_{r \to 0^+} \frac{r}{\sqrt[\kappa]{V_0(R + r)} - S}$$

which after substituting (5) in the denominator yields in the limit $\lim_{r\to 0^+}$ an expression of indefinite form "0/0". Applying l'Hôpital's rule converts the quotient to an expression that can be evaluated directly, where

$$\lim_{r \to 0^+} \frac{r}{\sqrt[\kappa]{V_0(R + r)} - S} = \lim_{r \to 0^+} \frac{\frac{\partial(r)}{\partial r}}{\frac{\partial(\sqrt[\kappa]{V_0(R+r)} - S)}{\partial r}}.$$

The denominator of this equation is 1. The numerator simplifies to $\lim_{r\to 0^+} \frac{1}{\kappa}(V_0(R + r))^{\frac{1-\kappa}{\kappa}} V_0$ after differentiation. Taking the limit and substituting (5) yields

$$\lim_{r \to 0^+} \frac{\partial(\sqrt[\kappa]{V_0(R + r)} - S)}{\partial r} = \frac{1}{\kappa}(\frac{S^\kappa}{R} R)^{\frac{1-\kappa}{\kappa}} \frac{S^\kappa}{R},$$

which simplifies to $\frac{S}{\kappa R}$. Thus,

$$\lim_{r \to 0^+} \bar{P}(r) = \frac{1}{\frac{S}{\kappa R}} = \frac{\kappa R}{S}. \tag{16}$$

From Proposition 2 we know that $P = -\frac{\partial V/\partial S}{\partial V/\partial R}$. Using equation (5) allows us to calculate the partial derivatives

$$\frac{\partial V}{\partial S} = \frac{\partial(S^\kappa/R)}{\partial S} = \frac{1}{R}\kappa S^{\kappa-1} = \frac{\kappa S^{\kappa-1}}{R}$$

and

$$\frac{\partial V}{\partial R} = \frac{\partial(S^\kappa/R)}{\partial R} = S^\kappa(-1)R^{-2} = -\frac{S^\kappa}{R^2}.$$

Thus,

$$P = -\frac{\frac{\kappa S^{\kappa-1}}{R}}{-\frac{S^\kappa}{R^2}} = \frac{\kappa R}{S}. \tag{17}$$

Comparing equations (16) and (17) concludes the proof. □

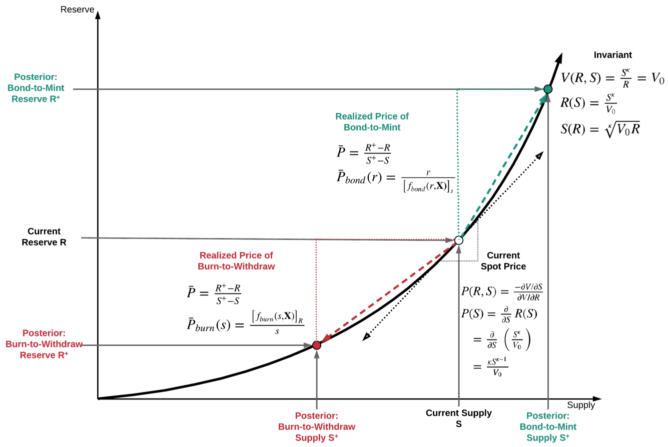

Fig. 3: Illustration of the bonding curve invariant, and the associated bond-to-mint and burn-to-withdraw mechanisms which respect it.

Definition 20. *The **Burn-to-withdraw** mechanism $x' = f_{burn}(s, x)$ where $x \in \mathbf{X_C}$ is the state prior to the transaction and $x' \in \mathbf{X_C}$ is the posterior state. The action taken $s \in \mathbb{R}_{++}$ is a quantity of tokens destroyed; furthermore, $s \leq s_a \leq S$ where $a \in \mathcal{C}$ is the account taking this action.*

$$S^+ = S - s \tag{18}$$

$$R^+ = \frac{(S-s)^\kappa}{V_0} \tag{19}$$

$$P^+ = \frac{\kappa(S-s)^{\kappa-1}}{V_0} \tag{20}$$

$$F^+ = F + \phi \cdot \left(R - \frac{(S-s)^\kappa}{V_0}\right). \tag{21}$$

The amount of reserve currency removed from the reserve as a result of burning s is

$$r = \left(R - \frac{(S-s)^\kappa}{V_0}\right), \tag{22}$$

and the realized price before the tax is

$$\bar{P}(s) = \frac{r}{s} = \frac{S^\kappa - (S-s)^\kappa}{s \cdot V_0}. \tag{23}$$

Accounting for the tax, the quantity of reserve currency received by the account which burned s is $(1-\phi)\cdot r$, and the realized price including the tax is

$$\frac{r \cdot (1-\phi)}{s} = (1-\phi)\bar{P}(s). \tag{24}$$

Lemma 2. *For $\kappa > 1$, the realized price $\bar{P}(s) < P$ for all $s > 0$ and the limit realized price is the current price P as the size of the burned funds s tends to zero from the right:*

$$\lim_{s\to 0^+} \bar{P}(s) = P. \tag{25}$$

Proof. From Definition 20 equation (23) it follows that $\lim_{s\to 0^+} \bar{P}(s)$ is:

$$\lim_{s\to 0^+} \frac{S^\kappa - (S-s)^\kappa}{s \cdot V_0},$$

which after forming the limit $\lim_{s\to 0^+}$ yields an expression of indefinite form "0/0". Applying l'Hôpital's rule converts the quotient to an expression that can be evaluated directly, where

$$\lim_{s\to 0^+} \frac{S^\kappa - (S-s)^\kappa}{s \cdot V_0} = \lim_{s\to 0^+} \frac{\frac{\partial(S^\kappa - (S-s)^\kappa)}{\partial s}}{\frac{\partial(s\cdot V_0)}{\partial s}}.$$

Differentiating and taking the limit of the denominator yields

$$\lim_{s\to 0^+} \frac{\partial(S^\kappa - (S-s)^\kappa)}{\partial s} = \lim_{s\to 0^+} -\kappa(S-s)^{\kappa-1}(-1) = \kappa S^{\kappa-1}.$$

The numerator simplifies to $V_0 = \frac{S^\kappa}{R}$ after differentiation, thus

$$\lim_{s\to 0^+} \bar{P}(s) = \frac{\kappa S^{\kappa-1}}{\frac{S^\kappa}{R}} = \frac{\kappa R}{S}. \tag{26}$$

From Proposition 2 we know that $P = -\frac{\partial V/\partial S}{\partial V/\partial R}$. Using equation (5) allows us to calculate the partial derivatives

$$\frac{\partial V}{\partial S} = \frac{\partial(S^\kappa/R)}{\partial S} = \frac{1}{R}\kappa S^{\kappa-1} = \frac{\kappa S^{\kappa-1}}{R}$$

and

$$\frac{\partial V}{\partial R} = \frac{\partial(S^\kappa/R)}{\partial R} = S^\kappa(-1)R^{-2} = -\frac{S^\kappa}{R^2}.$$

Thus,

$$P = -\frac{\frac{\kappa S^{\kappa-1}}{R}}{-\frac{S^\kappa}{R^2}} = \frac{\kappa R}{S}. \tag{27}$$

Comparing equations (26) and (27) concludes the proof. □

The latter two mechanisms relate to the funding pool. In this example, the augmented bonding curve funds projects by issuing the community token S, and the recipients may choose to burn some or all of those tokens using the burn-to-withdraw mechanism.

Definition 21. *The **allocate-with-rebond** mechanism $x' = f_{allocate}(u, x)$ where $x \in \mathbf{X_C}$ is the state prior to the transaction and $x' \in \mathbf{X_C}$ is the posterior state. The action taken $u = (r, a)$, where $a \in \mathcal{A}$ is the receiving address* *and $r \in \mathbb{R}_{++}$ is a quantity of reserve tokens allocated; furthermore, $r \leq F$.*

$$F^+ = F - r \tag{28}$$
$$R^+ = R + r \tag{29}$$
$$S^+ = \sqrt[\kappa]{V_0(R+r)} \tag{30}$$
$$P^+ = \frac{\kappa(R+r)^{(\kappa-1)/\kappa}}{V_0^{1/\kappa}} \tag{31}$$

The quantity of tokens allocated to the receiving address is

$$s = \sqrt[\kappa]{V_0(R+r)} - S. \tag{32}$$

This is a special case of the bond-to-mint mechanism where the bonded tokens come from the funding pool, and the minted tokens are allocated to an address chosen by the community.

The above mechanism is an intentional composition of a simple allocation $R^+ = R - r$ and a bond-to-mint of the amount r. It is constructed as a means of preferentially supporting community member efforts over payment to outside contractors. It is possible to simply compose to burn these tokens, but since the value is leaving the community it is taxed.

Finally, consider the case where the collaborative efforts of the community produce some revenues. In this case, those revenues may be deposited directly into the funding pool in order to fund future projects.

Definition 22. *The* ***deposit*** *mechanism $x' = f_{deposit}(r, x)$ where $x \in \mathbf{X_C}$ is the state prior to the transaction and $x' \in \mathbf{X_C}$ is the posterior state. The action taken $r \in \mathbb{R}_{++}$ is a quantity of reserve tokens deposited.*

$$F^+ = F + r \tag{33}$$
$$(R^+, S^+, P^+) = (R, S, P) \tag{34}$$

This action has no immediate effect on any state other than F. Large deposits may increase the perceived value of the community tokens which steer these funds, thus driving future bond-to-mint activity.

D. Initialization

The transaction driven system dynamics presented above have explicit state dependence and are sensitive to their initial conditions. The authors refer to the act of raising funds from a community and launching an augmented bonding curve as *hatching* to invite an organic vision of the community growth as opposed to a mechanical one. Hatching or initializing the system requires the selection of the parameters: the fraction of initial reserve funds which will go to the funding pool θ, the exit tax ϕ, and the curvature of the invariant κ.

Definition 23. *The* ***Hatch*** *mechanism initializes the bonding curve state. Given the parameter choices (θ, ϕ, κ) and hatch raise of R_{hatch}, associated with a commitment to issue S_{hatch} tokens, purchased for the hatch price $P_{hatch} = \frac{R_{hatch}}{S_{hatch}}$, the initial state is given by:*

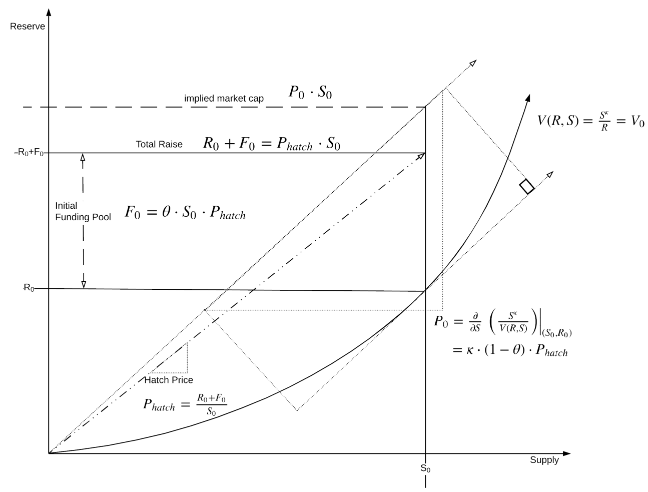

Fig. 4: Illustration of the relationships between the system parameters and initial states. Curvature $\kappa > 1$ is assumed.

$$R_0 = (1-\theta)R_{hatch} \tag{35}$$
$$F_0 = \theta R_{hatch} \tag{36}$$
$$S_0 = S_{hatch} \tag{37}$$
$$V_0 = V(R_0, S_0) \tag{38}$$
$$P_0 = \frac{\kappa(S_{hatch})^{\kappa-1}}{V_0}. \tag{39}$$

The relationships between these quantities are shown in Figure 4; upward curvature in the figure is indicative of $\kappa > 1$.

Lemma 3. *Hatching an augmented bonding curve results in a hatch return rate ρ*

$$\rho = \frac{P_0}{P_{hatch}} = \kappa \cdot (1-\theta). \tag{40}$$

Proof. This follows directly from substitution of equations from Definition 23 into equation (40):

$$\begin{aligned}
\rho &= \frac{P_0}{P_{hatch}} = \frac{\frac{\kappa(S_{hatch})^{\kappa-1}}{V_0}}{P_{hatch}} = \frac{\frac{\kappa(S_{hatch})^{\kappa-1}}{\frac{(S_{hatch})^\kappa}{(1-\theta)R_{hatch}}}}{\frac{R_{hatch}}{S_{hatch}}} = \\
&= \frac{\kappa(S_{hatch})^{\kappa-1}}{\frac{(S_{hatch})^\kappa}{(1-\theta)R_{hatch}}} \frac{S_{hatch}}{R_{hatch}} = \\
&= \frac{\kappa(S_{hatch})^{\kappa-1}}{1} \frac{(1-\theta)R_{hatch}}{(S_{hatch})^\kappa} \frac{S_{hatch}}{R_{hatch}} = \\
&= \kappa \cdot (1-\theta)
\end{aligned}$$

□

Due to the fact that $\rho > 1$ for a wide range of parameter choices, the augmented bonding curve should be implemented with a vesting schedule for all tokens created as part of S_{hatch}. A range of vesting policies are available, the simplest of which

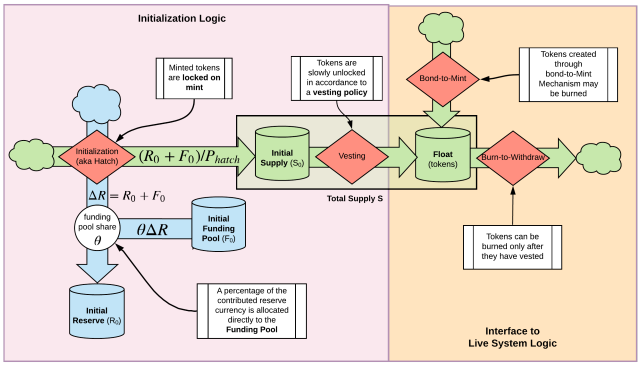

Fig. 5: The mechanics of initialization of an augmented bonding curve result in returns ρ for participants in the hatch so a vesting policy is used to restrict pump and dump strategies.

is a lockup that allows the tokens to be used for decision making but makes them invalid as inputs to burn-to-withdraw. A vesting date may cause a shock, so the authors recommend a half-life vesting strategy where the fraction of tokens from S_{hatch} which may be burned is

$$S_{vested} = \left(1 - 2^{-\gamma(k-k_0)}\right) S_{hatch} \tag{41}$$

where γ is the decay rate in blocks, k is the current block height and k_0 is the block height when the augmented bonding curve was deployed. We note, as shown in Figure 5, that the floating supply of tokens which can be burned is

$$S_{float} = S - \left(2^{-\gamma(k-k_0)}\right) S_0. \tag{42}$$

Supposing that blocks are created every 20 seconds on average then there will be an expected 131400 blocks per month. Using this conversion, $\hat{\gamma} = \gamma/131400$ is the monthly half-life, which is more legible to human users. Figure 6 illustrates half-life vesting schedule with $\hat{\gamma} = 1$, a one month half-life.

In principle one may use any positive on-chain measurable signal as a measure of progress, or key performance indicator (KPI), and vest as a function of this KPI in place of blocktime, as discussed in [16]. This is accomplished by substituting any strictly positive, non-decreasing measure for block height k in Equations (41) and (42).

E. Numerical Demonstration

In this section, the properties thus far discussed are demonstrated numerically. A critical parameter in the augmented bonding curve is the curvature κ. The larger κ is the sharper the diminishing returns and the greater the hatch return rate. Practically speaking, a larger κ favors the community members present for the hatch, over those who join later.

Although it was easier to manipulate the invariant $V(R, S) = \frac{S^\kappa}{R}$ analytically with supply S as the independent variable, the Reserve R is placed on the x-axis in these experiments because in practice it represents an asset whose value is exogenous to the system. It thus makes a more intuitive independent variable.

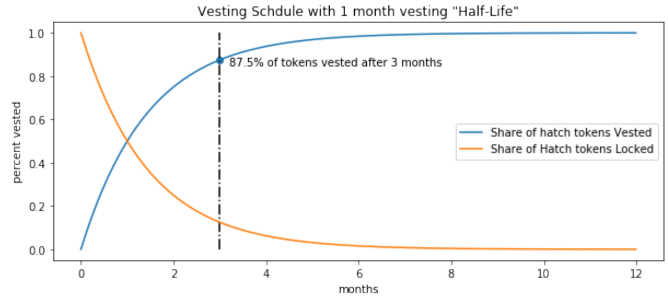

Fig. 6: The half-life vesting schedule smoothly releases tokens from the locked state to the floating state with half-life $\hat{\gamma} = 1$.

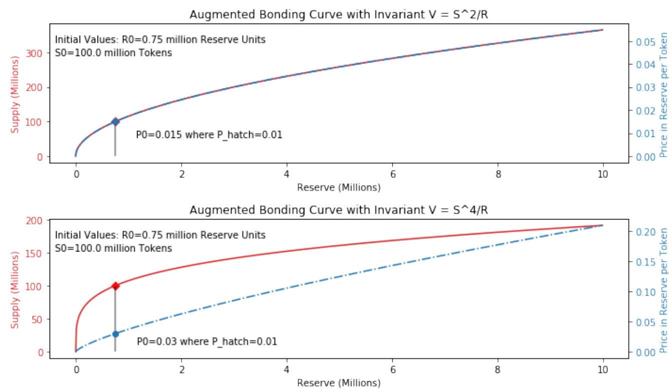

Fig. 7: Top: illustration of supply per unit Reserve decreasing with curvature $\kappa = 2$. Bottom: supply per unit Reserve decreasing with curvature $\kappa = 4$

Consider an example case where the hatch raise is $R_{hatch} = 1$ Million with $\theta = .25$ so that $R_0 = 0.75$ Million Reserve Dollar equivalent Units and $S_0 = 100$ Million tokens implying a hatch price of 1 cent per token. In figure 7, $\kappa = 2$ and $\kappa = 4$ are illustrated. Observe that increasing the curvature from 2 to 4 increases P_0 from 1.5 cents per token to 3 cents per token, which is equivalent to increasing ρ from 1.5 to 3, a significant increase in paper gains on the part of the hatching community. It is also worth noting that when $\kappa = 2$ the price curve and supply curve are both the same shape, proportional to $\sqrt{R}$, whereas in the case of $\kappa = 4$, Supply is proportional to $\sqrt[\kappa]{R}$ whereas the price is proportional to $\sqrt[4]{R^3}$. As κ gets larger the price function becomes closer to linear: $\sqrt[\kappa]{R^{\kappa-1}}$.

Having observed that the choices of κ and θ are the drivers of the hatch event, Figure 8 displays a grid of values ρ which are independent of the other parameters. It is important to note that augmented bonding curves are meant to support communities continuously. A ρ which is too large will likely contract as there is a strong incentive to burn tokens as they vest. A moderate $\rho \leq 3$ is recommended.

Another practical consideration for this system is how much the price slips for any particular transaction. Slippage for any

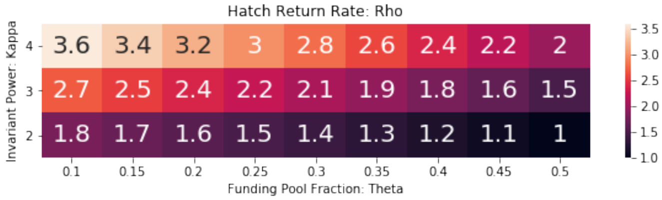

Fig. 8: Parameter Sweep of κ and θ to exploring the hatch return rate ρ

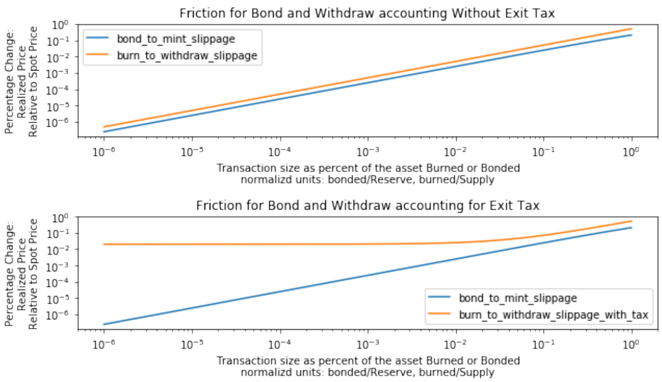

Fig. 9: Top: illustration of the slippage as a function of transaction size without the exit tax. Bottom: slippage as a function of transaction size with the tax $\phi = 0.02$.

transaction may be defined as the difference between the spot price P before the transaction and the realized price $\bar{P}$ of that transaction. As shown in Lemmas 1 and 2, the realized prices tend to the spot prices as the the transactions get smaller. In Figure 9, $\kappa = 2$ is used. In the top Figure 9, it is shown that bond-to-mint slippage $\bar{P}(r) - P$ is proportional to r/R and that burn-to-withdraw slippage $\bar{P}(s) - P$ is proportional to s/S. This means that as long as day-to-day transactions in and out of the augmented bonding curve are small compared to the total liquidity, users will experience very little slippage. Furthermore, if the state changes include a mixture of bond-to-mint and burn-to-withdraw which results in small net change $(\Delta R, \Delta S)$, then the change in the spot price is bounded.

The apparent symmetry between bond-to-mint and burn-to-withdraw is broken by the exit fee. In order to opt to burn tokens, the user either must have a real need for the reserve tokens, or be realizing a gain which sufficiently exceeds the exit fee. The bottom of Figure 9 shows the prices a user experiences when $\phi = .02$.

Note that the tax provides a counter-measure to sandwich attacks where an attacker sees a bond-to-mint and includes their own bond-to-mint beforehand, and a burn-to-withdraw afterwards, to take immediate gains. Gains would need to exceed the tax, and the tax being applied would benefit the community. In environments where such attacks are common, a community may choose a higher ϕ in order to simultaneously disincentivize such attacks, and to capture more funds from attackers that engage in such activities.

V. Future Work

The augmented bonding curve as discussed in Section IV is under development by The Commons Stack [27]. The ongoing development and testing of this mechanism will proceed to the launch of one or more community funds in support of not-for-profit activities. Empirical and ethnographic studies of behavior within these communities will be conducted. Furthermore, integration with SourceCred [28] will occur in order to increase the transparency and accountability of work financially supported by these community funds.

In parallel with the development of the augmented bonding curve software, a wide range of computational experiments are being undertaken to study the dynamics of the games which play out on these manifolds. Both agent-based models and population games are considered using the cadCAD [29] python modeling framework. Computational experiments are underway with a focus on exploring the failure modes of this system, as well as the sensitivity of the system trajectories to parameters and assumptions about the agents' strategies.

Further work on the bonding curve as an economic primitive will be focused on its capacity as an estimator. Our preliminary numerical experiments show that it provides a robust price estimate by aggregating the revealed preferences of the agents into a system level revealed preference under modest assumptions. Additional technical considerations include handling the numerical precision errors created by modeling large integers as real values. Work is also underway by the Balancer project [10] team which has applied the invariant based design methodology to their product.

References

[1] S. Voshmgir and M. Zargham, "Foundations of cryptoeconomic systems," Research Institute for Cryptoeconomics, Vienna, Working Paper Series / Institute for Cryptoeconomics / Interdisciplinary Research 1, November 2019. [Online]. Available: https://epub.wu.ac.at/7309/

[2] S. Voshmgir, *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*. BlockchainHub, June 2019a, vol. 1.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, Dec 2008, accessed: 2015-07-01. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] K. Dopfer, J. Foster, and J. Potts, "Micro-meso-macro," *Journal of Evolutionary Economics*, pp. Springer–Verlag, 2004.

[5] J. Goldstein, "Emergence as a construct: History and issues," *Emergence*, vol. 1, no. 1, pp. 49–72, 1999. [Online]. Available: https://doi.org/10.1207/s15327000em0101_4

[6] T. Galla and J. D. Farmer, "Complex dynamics in learning complicated games," *Proceedings of the National Academy of Sciences*, vol. 110, no. 4, pp. 1232–1236, 2013.

[7] S. de la Rouviere, "Tokens 2.0: Curved token bonding in curation markets," November 2017. [Online]. Available: https://medium.com/@simondlr/tokens-2-0-curved-token-bonding-in-curation-markets-1764a2e0bee5

[8] S. Balasanov, "Bonding curves in depth: Intuition & parametrization," December 2018. [Online]. Available: https://blog.relevant.community/bonding-curves-in-depth-intuition-parametrization-d3905a681e0a

[9] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, and T. Chitra, "An analysis of uniswap markets," 2019.

[10] F. Martinelli and N. Mushegian. (2019) Balancer: A non-custodial portfolio manager, liquidity provider, and price sensor. [Online]. Available: https://balancer.finance/whitepaper.html

[11] T. Favre, "Continuous organizations," October 2019. [Online]. Available: https://github.com/c-org/whitepaper

[12] A. Titcomb, "Deep dive: Augmented bonding curves," April 2019. [Online]. Available: https://medium.com/giveth/deep-dive-augmented-bonding-curves-3f1f7c1fa751

[13] J. R. Marden and J. S. Shamma, "Game theory and distributed control," in *Handbook of game theory with economic applications*. Elsevier, 2015, vol. 4, pp. 861–899.

[14] R. Ghrist, "Configuration spaces, braids, and robotics," in *Braids: Introductory Lectures on Braids, Configurations and Their Applications*. World Scientific, 2010, pp. 263–304.

[15] M. Zargham, Z. Zhang, and V. Preciado, "A state-space modeling framework for engineering blockchain-enabled economic systems," in *International Complex Systems Conference*. https://arxiv.org/pdf/1807.00955.pdf: ArXiv.org, 2018.

[16] Z. Zhang, M. Zargham, and V. Preciado, "On modeling blockchain-enabled economic networks as stochastic dynamical systems," in *Applied Network Science: Blockchain and Cryptocurrency*. [Forthcoming]: Springer, 2019.

[17] W. H. Sandholm, *Population games and evolutionary dynamics*. MIT press, 2010.

[18] S. Park, N. C. Martins, and J. S. Shamma, "Payoff dynamics model and evolutionary dynamics model: Feedback and convergence to equilibria," 2019.

[19] A. Mas-Colell, M. Whinston, and J. Green, *Microeconomic Theory*. Oxford University Press, 1995.

[20] M. Zargham, A. Bulkin, and J. S. Nelson, "Raising social capital: Tokenizing a customer-driven business," *Sweetbridge Technical White Paper Series*, vol. 2, 2017.

[21] E. Ostrom, "Beyond markets and states: polycentric governance of complex economic systems," *American economic review*, vol. 100, no. 3, pp. 641–72, 2010.

[22] M. Common and S. Stagl, *Ecological Economics: An Introduction*. Cambridge University Press, 2005.

[23] S. P. Lalley and E. G. Weyl, "Quadratic voting: How mechanism design can radicalize democracy," *AEA Papers and Proceedings*, vol. 108, pp. 33–37, May 2018. [Online]. Available: http://www.aeaweb.org/articles?id=10.1257/pandp.20181002

[24] M. Zargham, "Sensor fusion and social choice." [Online]. Available: https://github.com/BlockScience/conviction/blob/master/social-sensorfusion.pdf

[25] K. J. Arrow, *Social choice and individual values*. Yale university press, 2012, vol. 12.

[26] B. Skyrms, *Evolution of the social contract*. Cambridge University Press, 2014.

[27] CommonsStack. A non-profit organisation building cryptoeconomic primitives for public goods. [Online]. Available: https://commonsstack.org/abc

[28] SourceCred. A reputation protocol for open collaboration. [Online]. Available: https://sourcecred.io

[29] cadCAD. An open-source python package that assists in the processes of designing, testing and validating complex systems through simulation. [Online]. Available: https://cadcad.org