From Curved Bonding to Configuration Spaces

Michael Zargham*, Jamsheed Shorish† and Krzysztof Paruch‡
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. 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. 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.**

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].

As multiscale systems they often possess complex properties such as nonlinear dynamics and feedback effects, leading to emergent properties [3] that cannot be discerned from an isolated examination at each scale. Complexity is compounded when multiple mechanisms are available concurrently, [4]. 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 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 such mechanism, token bonding curves have gained attention in the cryptoeconomics community [5], [6] as an alternative means of funding (replacing ICOs) and as a financial instrument [7], [8] for tokens. A common implementation is a reserve ratio persevering variant attributed to Bancor [9].

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 [10] and may be further enforced as *conservation functions*, which simplifies the possible system trajectories. This dimensionality reduction causes the reachable state space, known as the *configuration space* [11], to guarantee desired properties that are not guaranteed in the *ex ante* state space [12].

978-1-7281-6680-3/20/$31.00 ©2020 IEEE

II. Deriving the Configuration Space

The following framework incorporates the micro, meso and macro [13] economic properties into a discrete-time dynamical system, so that system requirements and participating agent actions spaces can be defined and analyzed formally.

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.). Agents, acting through some address, may condition upon information in that address' 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 2. *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 $x' := f(x, u)$.*

Definition 3. *An **admissible action** $u \in U(X_a; x) \subset \mathbf{U}$ for an address a is an input to a mechanism f which has dependence on a and a portion of the state 'local' to a, denoted $X_a \subseteq X$.*

Definition 4. *A **state transition** is a discrete event characterized by (a, u, f) resulting in the posterior state x'*

$$x' = f(u, x),\ u \in U(X_a; x) \subset \mathbf{U},\ f \in \mathbf{F}. \tag{1}$$

TABLE I: Relating Agent Behavior to System State

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

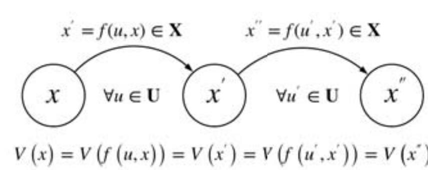

Fig. 1: Let Conservation function V be invariant for all $f \in \mathbf{F}$.

The configuration space is characterized by *conservation functions* which enforce desired properties of the system, while retaining sufficient degrees of freedom for the agents to express their private preferences through actions $u \in U(X_a; x)$ under mechanism $f \in \mathbf{F}$.

Proposition 1. *The **conservation function** $V : \mathbf{X} \to \mathbb{R}$ is **invariant** under the mechanisms $\mathbf{F}$, if given an initial state $x \in \mathbf{X}$, $V(f(u,x)) \equiv V(x)$ for all mechanisms $f \in \mathbf{F}$ and all admissible actions $u \in \mathbf{U}$.*

Corollary 1. *The **configuration space** $\mathbf{X_C}$ is a proper subset of the state space $\mathbf{X}$, and precisely the space reachable via legal state transitions induced by actions $u \in \mathbf{U}$, under mechanisms $f \in \mathbf{F}$.*

No matter what actions the agents choose, all possible trajectories will lie within the configuration space. Thus critical constraints may be directly encoded and enforced via conservation functions.

III. Bonding Curve As Configuration Space

A bonding curve is a system where agents may bond reserve tokens to mint supply tokens, and may conversely burn supply tokens to withdraw reserve tokens. A polynomial conservation function is imposed on the phase space (R, S) inducing a spot price P in units of reserve per supply.

Definition 5. *The Bonding Curve state: **reserve** R, **supply** S and **spot price** P, is $x = (R, S, P) \in \mathbf{X} = \mathbb{R}^3_{++}$.*

Proposition 2. *Given the **conservation function***

$$V(x) = V(R, S) := \frac{S^\kappa}{R} = V_0 \tag{2}$$

the curvature κ characterizes the reserve ratio $\frac{R}{PS} = 1/\kappa$.

A critical substep in the proof of Proposition 2 is derivation of the differential relation between R and S under V:

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

Definition 6. *The **bond-to-mint** mechanism $(R', S', P') = f_{bond}(r, x)$ where $x \in \mathbf{X_C}$ has admissible action space $r \in \mathbb{R}_{++}$ resulting in posterior state $R' = R + r$, $S' = \sqrt[\kappa]{V_0(R + r)}$ and $P' = p(R', S')$.*

Definition 7. *The **burn-to-withdraw** mechanism $(R', S', P') = f_{burn}(s, x)$ where $x \in \mathbf{X_C}$ has admissible action space $s \in (0, S) \subset \mathbb{R}_{++}$ resulting in posterior state $S' = S - s$, $R' = \frac{(S-s)^\kappa}{V_0}$ and $P' = p(R', S')$.*

Proposition 3. *Denote the **realized price** for a state transition as $\bar{P} = \frac{R'-R}{S'-S}$. Under f_{bond}, $\lim_{r\to 0_+} \bar{P} = \kappa \frac{R}{S} = P$, and under f_{burn}, $\lim_{s \to 0_+} \bar{P} = \kappa \frac{R}{S} = P$.*

Proposition 4. *Both mechanisms f_{burn} and f_{bond} result in diminishing returns, e.g. $\bar{P}$ is monotonic increasing in the action r under f_{bond} and monotonic decreasing in the action s under f_{burn}.*

TABLE II: Summary of Configuration Space Restrictions

Given States	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	$\frac{\kappa S^{\kappa-1}}{V_0}$

Proposition 5. *Given the mechanism set $\mathbf{F} = \{f_{burn}, f_{bond}\}$ the **configuration space** is the 1-manifold*

$$\mathbf{X_C} := \{x \in \mathbf{X} \mid V(R, S) = V_0,\ P = p(R, S)\} \subset \mathbb{R}^3_{++}. \tag{3}$$

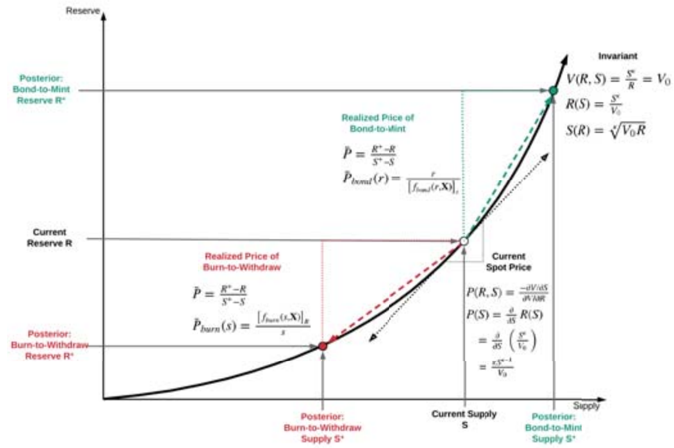

Fig. 2: Invariant preservation under $\mathbf{F} = \{f_{burn}, f_{bond}\}$.

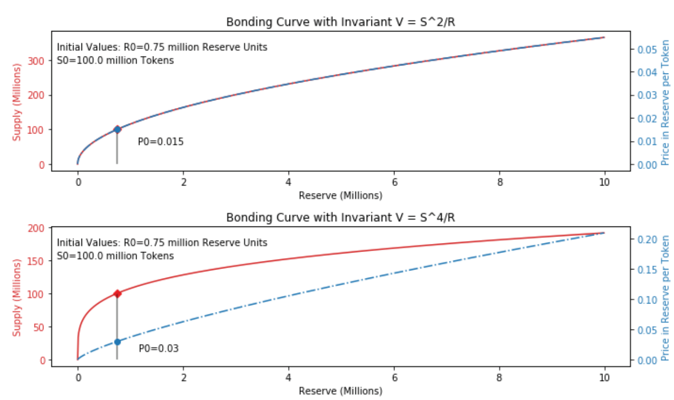

Fig. 3: **Numerical Demonstration**: S and P plotted per R with initial conditions $R_0 = 750$ and $S_0 = 100$ Million tokens. Top: curvature $\kappa = 2$. Bottom: curvature $\kappa = 4$

IV. Challenges and Opportunities

The approach described above facilitates the creation of games with well defined state space properties, specifically that all trajectories will respect conservation principles regardless of the agents' actions. Moreover, the introduced formalism provides access to methods from robotics and control theory disciplines for design and analysis of economic systems.

Agents may also leverage the guaranteed invariant properties to their advantage; the state dependence makes price very sensitive to transaction order, which has incentivized front running. These exploitative strategies may be mitigated by refinements such as batching transactions [14].

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] 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

[4] 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.

[5] 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

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

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

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

[9] E. Hertzog, G. Benartzi, and G. Benartzi, "Bancor protocol," 2017.

[10] 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.

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

[12] 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.

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

[14] B. Rennekamp. (2019) Batched bonding curves. [Online]. Available: https://medium.com/@billyrennekamp/batched-bonding-curves-ce69a57d8ae4