# Hedonic Pricing of Cryptocurrency Tokens

Jamsheed Shorish\*

Shorish Research<sup>†</sup> Meerbeek, Belgium jamsheed@shorishresearch.com

November 15, 2018

This version: January 14, 2019

#### Abstract

A cryptocurrency token offers a method of incentivizing behavior in a way that supports trusted interaction (through its blockchain-based infrastructure). It also acts as a multipurpose instrument that may fulfill a variety of roles, such as facilitating digital use cases or acting as a store of value. Understanding how to value such an instrument is complicated by these multiple roles because the relative valuation of one role cannot be disentangled from another role—a token is a 'bundled' good. In this work a general pricing model for cryptocurrency tokens is derived, based upon and extending the hedonic pricing framework of Rosen (1974) in a partial equilibrium framework. It is shown that individual roles (or characteristics) of a token may be priced by inverting in a special way the relationship between the token's aggregate quantity and its provision of characteristics. Interaction between a monopolistic token seller and a representative buyer results in an equilibrium that clears both the aggregate token market and the characteristic market. Particular attention is given to the case in which a token possesses a security role, as this has been a focus of existing discussions regarding the regulation of the cryptocurrency market.

Keywords: cryptocurrency, blockchain, token economics, hedonic pricing, Moore-Penrose inverse

Journal of Economic Literature Codes: D46, C60

<sup>\*</sup>Thanks are given to the participants of the 2nd Berlin Conference 'Crypto-Currencies in a Digital Economy' and to Krzysztof Paruch (Research Institute for Cryptoeconomics, Vienna University of Economics and Business) for very helpful comments and insights.

<sup>&</sup>lt;sup>†</sup>Shorish Research provides strategic consulting services built upon academic and real-world application expertise in the area of Computational Business.

### 1 Introduction

The adoption and widespread exposure of cryptocurrencies such as Bitcoin has promised to bring forth a revolution in both database technology (through the use of blockchain as a decentralized ledger) and, so proponents claim, in the way economic value is created and transferred [see e.g. Berentsen and Schar (2018), Böhme et al. (2015), Lachance (2016), and Marr (2016)]. The nascent field of 'token economics' is currently exploring to what extent value creation, transfer and storage facilitated by cryptocurrencies are similar to (or are markedly different from) existing mechanisms of value, such as fiat money and traditional equity and debt assets [cf. Conley (2017), Hargrave et al. (2018)].

One of the key challenges in assessing the impact of cryptocurrencies is providing a methodology that can relate the sometimes multifaceted use of a cryptocurrency unit, or 'token', to the requirements and objectives of both a token issuer and a token purchaser. The token issuer (or 'seller') may, for example, issue the token to

- 1. facilitate a particular use of the underlying ledger technology offered by the seller;
- 2. facilitate an investment in the seller;
- 3. facilitate governance of the seller;
- 4. facilitate advertising or brand awareness; or
- 5. facilitate transfer and/or store of value.

In the parlance of cryptocurrency tokens, the first case listed above defines a **utility** aspect<sup>1</sup> to the token, where the token confers usage rights as part of the product offering by the seller. Perhaps the most popular example of a utility token is the 'ether' token created by Ethereum, which acts as a resource required to run automated pieces of programming code known as *smart contracts* on the Ethereum blockchain. The second case listed defines a **security** aspect to the token, either as a mechanism for crowdfunding/fundraising via an Initial Coin Offering (ICO) or Token Generation Event (TGE), or as an equity investment with a return similar to a dividend or bond.<sup>2</sup> The third case creates a **governance** aspect, and is often tied together with the security aspect to provide voting representation in the seller's decision-making [cf. Leonhard (2017)]. The fourth case could be called an **ambassador** aspect, in that the token adopts a voucher, discount or brand dissemination role designed to attract future holders of the token [see e.g. Bogart (2018) for a description

<sup>&</sup>lt;sup>1</sup>It is important that this usage of the word *utility* is not confused with the general benefit to a buyer of a token, as given by the buyer's *utility function*, which will also be heavily referenced in this work. Context should prevent confusion between the two meanings.

<sup>&</sup>lt;sup>2</sup>Recently, public comments by the U.S. Securities and Exchange Commission have indicated that there is no *a priori* reason to categorize a token as a security by default, in the same sense as a stock or bond is a security, because tokens may provide other uses (e.g. in a utility capacity). See Hinman (2018).

of the 'airdrop' phenomenon and its relation to the distribution of tokens via hard fork programming code changes]. Finally, and probably best known by the public, the token can confer a **market** or speculative aspect–Bitcoin was in principle designed to act as a medium of exchange, and recent token innovations have created equity- or commodity-backed tokens that act in way similar to derivatives.

The novel feature of a cryptocurrency token is that some or all of these aspects may be present simultaneously, in much the same way that a traditional equity security may confer the right to a claim on the firm (a dividend) as well as a say in governance (a voting share proportional to holdings). For this reason one is tempted to value a token using traditional market-based valuation tools for debt or equity assets, attempting to separate out dividend rights from control rights ('security' from 'governance') using the standard models in the literature. But this program is severely hampered when the utility and ambassador aspects must also be valued—not only is there not an explicit market for these aspects, but to a token holder these values may be consumption-based rather than wealth-based. In other words, valuation will require an understanding of the preferences of the buyer for a collection of aspects, some of which may confer immediate consumption benefits while others may confer future benefits (e.g. as a store of wealth and hence future consumption).

A more natural valuation approach is to begin with a model of a bundled good, in which there exists one explicit market for the good itself, but aspects, or 'characteristics' of the good are missing markets and hence must be implicitly valued. Following the seminal work of Houthakker (1952) and Lancaster (1966), Rosen (1974) proposed a hedonic pricing model for such goods. This model has been applied most naturally to the real estate and housing markets—a house, for example, is a bundled good of alternative benefits, such as number of rooms, location and amenities, which cannot in and of themselves be disentangled from the house. Rosen demonstrated that it is possible to provide an interpretation of the characteristics of a bundled good such that individual characteristics may be valued, and showed that the resulting market for such goods clears. Rosen's approach, shown to be empirically applicable (with some caveats) by e.g. Epple (1987) and others, has made hedonic pricing models (and the regression approach to empirical estimation it facilitates) the main approach to bundled good valuation available today.

In this work we apply a hedonic pricing approach to cryptocurrency tokens, in order to create, as in Rosen, a way to understand the valuation of implicit characteristics both from the token seller's and the token buyer's perspectives. With this approach the seller selects not just a price and quantity of a token but also a *characteristic mix* that the token possesses (in much the same way that an architect would select the composition of a home, and a real estate developer the location of that home) in order to maximize an objective, such as net profit from token sales and any claims on the firm from tokens acting in their

security aspect. The buyer, by contrast, values some characteristics for immediate consumption (a utility characteristic of the token), while using other characteristics as stores and transfers of value for future consumption (security or market characteristics, etc.). The buyer selects their optimal token characteristic demand by maximizing their overall utility from purchasing the token, depending upon the various characteristics present.

Although based upon and extending the approach of Rosen (1974), the mechanism adopted here by which token characteristics are priced differs from its implicit valuation as the (marginal) change in the price of the token from a change in a characteristic included. Here we disentangle individual characteristics from the token by applying a kind of inverse transform, the Moore-Penrose inverse, to turn the token quantity selection problem into a characteristic mix selection problem. This allows the buyer to submit characteristic demands (for a given token price and characteristic mix) to the seller, who—assumed to be acting as a monopolist—sets the price of the token and hence clears the token market. Finally, equilibrium in the characteristic market is obtained when the seller selects the optimal characteristic mix, such that characteristic markets clear at the token market clearing price.

The paper is organized as follows. Section 2 introduces the hedonic pricing model and demonstrates the existence of a market clearing equilibrium for the token and its associated characteristics. A comparison with Rosen (1974) is also provided to compare the derivative-based approach and the Moore-Penrose inverse approach. Section 3 then introduces a simplified model in which there are only two types of characteristics, a collection of utility characteristics that the buyer values for consumption, and a single security characteristic that the buyer values only through its use as a transfer of wealth across time, i.e. for future consumption. A fundamental equation relating the optimal buyer demands to the seller's optimal token price selection is derived and discussed. Section 4 concludes with avenues for future research and speculation on the role of the characteristic mix in generating a valuation mechanism to help regulators and designers achieve relevant—and clear—cryptocurrency regulation.

### 2 A Hedonic Pricing Model

#### 2.1 Overview

Consider an instrument that is issued by a monopolistic token issuer (the "seller") to a pool of potential buyers—for simplicity, assume that there is a single 'representative' buyer.<sup>3</sup> Here the motivating example of such an instrument is a cryptocurrency token.

<sup>&</sup>lt;sup>3</sup>A 'representative agent' thus defined is standard in consumer theory. Note that in spite of being a single representative buyer, this representation does not imply market power—the representative buyer is

Following Rosen (1974) we consider the instrument as representing a hedonic good that possesses characteristics that are valued by the buyer, but that cannot be purchased directly. For example, a token might provide two characteristics that are of interest to the buyer:

- the use of the token as a claim on (some part or all of) the value of the seller: this is the token's **security** characteristic; and
- the use of the token as a grantor of seller-generated services: this is the token's utility characteristic.

Because the token is a composite (or bundled) good, the buyer cannot clearly disentangle the value of the token—which may be listed e.g. on an exchange or in a market—from the value of its characteristics, which are unobserved. Since the buyer has preferences not over the token itself but rather over the characteristics the token possesses, she<sup>4</sup> attempts to find the proper number of tokens to purchase that just balances the benefit of an extra token against the next best use of her resources (her *opportunity cost*). In what follows, we assume that the buyer's alternative resource use is to store value in a traditional medium of exchange (possibly with a non-zero return)—in other words, the buyer also has preferences over a stock of traditional fiat money as a proxy for future consumption.

The seller issues tokens with a particular combination, or 'mix', of characteristics associated with each token. Once this mix is determined, the token's set of characteristics is fixed for every token of that kind that is issued. The seller would like to maximize its *profit*, i.e. some combination of

- revenue from a token sale less the cost of creating and/or maintaining a stock of tokens, and
- the future value of tokens left unsold and held by the seller.

Since the token seller is a monopolist, they have the discretion to set the price of the token, as well as the characteristic mix within each token, and finally the total number of tokens created.

An equilibrium is a price, characteristic mix, and quantity of tokens created that both maximizes the profit of the seller and simultaneously the benefit, or utility,<sup>5</sup> of the buyer, so that all tokens offered for sale are purchased. The optimal mix of characteristics for each token is part of the larger token design problem facing a token seller, in addition to the token's price and quantity setting.

not a monopsonist as it is shorthand for a large number of price-taking, individual buyers.

<sup>&</sup>lt;sup>4</sup>Where a gender-specific pronoun is used in this paper, a gender-agnostic meaning is conferred.

<sup>&</sup>lt;sup>5</sup>Here is meant a benefit that will shortly be proxied using a utility function, as is standard in consumption theory.

In what follows the formal model is presented and an equilibrium derived, with attention given to how the characteristics market can clear without an *ex ante* restriction on the demand for characteristics from the buyer. In addition, a comparison with the seminal hedonic pricing model of Rosen (1974) is made, showing how the adopted methodology differs from that approach while providing the advantage of a potentially lower computational burden for calculating characteristic prices.

#### 2.2 Formalism

There is a seller of a single hedonic good which embodies, or 'bundles',  $d \in \mathbb{N}$  types of *characteristics*. A characteristic  $z_i$  indexed by i = 1, 2, ..., d is defined to be one component, or aspect, of a good that brings value to the holder of a token. In the present model we assume that these characteristics are both common knowledge<sup>6</sup> and available in potentially infinitesimal quantities, so that  $z_i \in \mathbb{R}_+$ .

There is a single buyer with preferences over characteristic amounts  $z := (z_1, z_2, \dots, z_d)$  and a unit of account  $m \in \mathbb{R}_+$ , acting as a numeraire—in the following we will consider this to be a holding of fiat money, and this holding may proxy for the buyer's consumption of non-token-related goods. Buyer preferences are represented by a utility function U(z, m) where  $U : \mathbb{R}^d_+ \times \mathbb{R}_+ \to \mathbb{R}$  and has standard properties. The buyer possesses an exogenous resource amount  $y \in \mathbb{R}_{++}$  ("income") to spend on tokens and the unit of account. As mentioned in the preamble, the buyer is 'representative': preferences held by a population of individual buyers are such that their aggregated demand behaves as if it was the result of the decision-making of a single buyer, whose demand coincides with their aggregate demand for the token.

On the supply side, the available characteristics sold by the seller *per token* are given by  $a := (a_1, a_2, \ldots, a_d) \in \mathbb{R}^d_+$ . In other words, a holder of n tokens possesses na units of the characteristics provided by the token seller. The seller is a monopolist, so that characteristics are uniquely available to the seller and cannot be substituted by the buyer with competing goods (this assumption may naturally be relaxed in a more realistic model of imperfect competition). The seller thus sets a token price q given the demand of the buyer.

### 2.3 The Buyer's Problem

The buyer seeks to maximize her utility over characteristics z and money m by selecting a token amount n, while respecting her budget constraint and taking the price q of the token as given:

 $<sup>^6</sup>$ This excludes the interesting (but significantly more complicated) case where characteristics are 'in the eye of the beholder', leading to subjective assessments that match characteristics to goods.

$$\max_{z,m} U(z,m)$$
 such that 
$$(2.1)$$
 
$$y \ge qn + m,$$

where n is the number of tokens purchased by the buyer.

Note that buyer values characteristics z and not token quantity n per se—this problem as written is ill-defined until a connection between z and n can be obtained. Since the vector of characteristics possessed by a single token is denoted by a, we have z = na as the equilibrium relationship between z and n, given a—but this is not what the buyer necessarily demands out of equilibrium, since the buyer values z and not n. What is needed is a way to represent n as a function of a and z. Although there are several possible approaches, an appealing method is to use the Moore-Penrose inverse of the vector a to write the number of tokens purchased in terms of the characteristics desired by the buyer:

$$n = a^{-1} \cdot z, \tag{2.2}$$

where  $a^{-1} := \frac{1}{\|a\|^2}(a_1, \dots, a_d) = \frac{1}{\|a\|}(\hat{a}_1, \dots, \hat{a}_d)$  is the Moore-Penrose inverse of a,  $\hat{a} := (\hat{a}_1, \dots, \hat{a}_d) \in S^{d-1}$  is the unit vector in the a direction, '·' represents the usual inner product, and  $S^{d-1}$  is the (d-1)-dimensional unit sphere.<sup>8</sup>

This makes the budget constraint

$$y \ge \frac{q}{\|a\|} \hat{a} \cdot z + m,\tag{2.3}$$

and we can define  $p_i := \frac{q}{\|a\|} \hat{a}_i$  as the **imputed price** of  $z_i$  for each i. We denote  $p := (p_1, \ldots, p_d)$  to be the vector of such imputed characteristic prices.

Thus problem (2.1) can be rewritten in a way standard for a consumer's problem:

$$\max_{z,m} U(z,m)$$
 such that 
$$y \ge p \cdot z + m.$$
 (2.4)

<sup>&</sup>lt;sup>7</sup>The Moore-Penrose inverse is appealing because it generates a set of (in this case unique) numbers  $\hat{n}$  that minimize the Euclidean norm  $||z - \hat{n}a||$ , and acts as an 'inverse' for a–for this reason it is also known as a 'least-squares' pseudo-inverse. Its application is widespread for matrices and not vectors, as used here. See Ben-Israel and Greville (2003) esp. p. 40 for an in-depth discussion, and Barata and Hussein (2011) for a comprehensive overview.

<sup>&</sup>lt;sup>8</sup>We will assume in what follows that context defines which vector is a 'row' vector and which is a 'column' vector when forming inner products, and we shall always place row vectors before column vectors.

The first-order conditions for the buyer's problem are straightforward:

$$\nabla_z U = \lambda p,$$

$$\frac{\partial U}{\partial m} = \lambda,$$
(2.5)

where  $\lambda \geq 0$  is the Lagrange multiplier associated with the budget constraint and by  $\nabla_z U$  we mean the usual gradient vector  $(\partial U/\partial z_1, \dots, \partial U/\partial z_d)$ .

These conditions may be combined to form:

$$\frac{1}{\partial_m U} \nabla_z U = p. \tag{2.6}$$

Equation (2.6) states that the marginal rate of substitution between characteristics and money is proportional to the characteristics available in each token, but only in their relative quantities. This makes sense as only fixed ratios may be purchased, and is even clearer when examining the marginal rate of substitution between characteristics:

$$\frac{\partial U/\partial z_i}{\partial U/\partial z_j} = \frac{\hat{a}_i}{\hat{a}_j}, \ i \neq j \in \{1, 2, \dots, d\}.$$
(2.7)

The buyer's token purchasing decision depends only upon the marginal utility of consuming an additional unit of the token as compared with the marginal utility of money, and not upon the relative distribution of the characteristics within the token—in other words, the buyer will continue to purchase tokens as long as

$$\nabla_z U \cdot a > \lambda, \tag{2.8}$$

and (provided enough real income, y/q, is available) will stop purchasing when  $\nabla_z U \cdot a = \lambda$ . Any excess income will then be held as money.<sup>9</sup> The optimal demand for characteristics is then given by that vector  $z^* = z^*(q, \hat{a}; y)$  which solves (2.8) with equality.

#### 2.4 The Seller's Problem

The seller seeks to maximize revenue (net of costs) from token sales, while at the same time earning a future return (or, if tokens act as an obligation, bearing a future cost) from either the stock of sold tokens, the stock of unsold tokens, or both. The seller *designs* the token by selecting a particular mix of characteristics—we suppose for simplicity that the

<sup>&</sup>lt;sup>9</sup>The constancy of the marginal utility of money is a convenient assumption here and is often made within the quasi-linear utility specification U(z, m) := u(z) + m, so that money acts as a representative of 'the rest of consumption' outside of the token.

seller selects a unit vector<sup>10</sup>  $\hat{a} \in S^{d-1}$  with an associated cost (a 'production mix' cost). In addition, the seller chooses the price of the token q and the total number of tokens  $\bar{n}$ , also with an associated cost (a 'production scale' cost). We encapsulate production mix and production scale costs in a cost function  $c(\bar{n}, \hat{a}) : \mathbb{R} \times \mathbb{R}^d_+ \to \mathbb{R}_+$ .

It may seem at first blush that cryptocurrency tokens are costless to produce, since they are by definition digital software. But the implementation of a cryptocurrency token by a token issuer is not generally costless—for example, tokens that conform to Ethereum's ERC20 token reference standard are built on top of the Ethereum platform, and smart contracts implementing such tokens are subject to a processing charge denominated in the Ethereum blockchain's unit of account (which is itself a token), ether, known as 'gas'. Releasing larger quantities of the token requires smart contract operations that expend gas, resulting in a scale cost to the token issuer. Moreover, creating the token characteristic mix is costly for a variety of reasons: if the token possesses a security characteristic, for instance, then it is subject to regulatory requirements that need legal support; if a utility characteristic is incorporated, then smart contract costs (e.g. development and running expenses) must be included. The presented cost function is clearly a simplification of what could be a complicated trade-off between different production mixes, and between production scale and mix costs, but serves as a point of departure for future investigation.

Finally, there exists an exogenous value function  $v(\bar{n}, n_s)$ ,  $v: \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}$ , where  $n_s$  is the quantity of tokens sold to the buyers. The value function is a proxy for future returns or obligations associated with 1) holdings of unsold tokens  $\bar{n} - n_s$ , which may have a positive future value, and 2) sold tokens  $n_s$ , which may have a negative future value if the token has (for example) a security characteristic and pays a return to a token holder. We will simplify this value function to examine the implications of a security characteristic for a token in Section 3.

The seller's problem is to find the optimal token design  $\hat{a}$ , the total token production  $\bar{n}$ , and the price q, taking the number of tokens  $n_s \leq \bar{n}$  to be equal to  $n_d = a^{-1} \cdot z^*$  demanded by the buyer, to solve:

$$\max_{\hat{a},\bar{n},q} q n_s - c(\bar{n},\hat{a}) + \mathbb{E} \left\{ v(\bar{n}, n_s) \right\}$$
such that
$$n_s = a^{-1} \cdot z^*.$$
(2.9)

with  $\mathbb{E}\{v\}$  representing the expectation (under the seller's beliefs) of the future value given by v.

As with the buyer's problem, we could in the seller's problem introduce a characteristic

<sup>&</sup>lt;sup>10</sup>The reason the seller selects only the direction and not the magnitude of the characteristic mix is discussed below.

<sup>&</sup>lt;sup>11</sup>See e.g. What is Ether?, an overview of ether at https://www.ethereum.org; retrieved January 2019.

price  $p = \frac{q}{\|a\|} \hat{a}$ . We note instead that selecting such a price p is actually the result of two separate decisions: the production mix decision, reflected in the choice of  $\hat{a}$ , and the production scale decision, reflected in the choice of  $q/\|a\|$ . The mix decision picks a direction in the characteristic space of the token and hence a direction of the characteristic price vector p in  $\mathbb{R}^d$ . By contrast, the token's price q (weighted by the mix vector's length) picks the overall length of the characteristic price vector. While these are two different degrees of freedom, we note from the buyer's problem that changing the price q of the token is a pure income effect and hence has no impact on the relative demand for characteristics. Hence in what follows we shall for simplicity set q = 1 and examine only the effects of optimizing over the characteristic mix, returning to the scale selection later. We shall also set  $\|a\| = 1$  for the same reason—we will see when discussing the market clearing condition for characteristics in Section 2.5 that this is not restrictive, and so does not change the seller's problem.

Rewriting, the seller's problem becomes

$$\max_{\hat{a},\bar{n}} \hat{a} \cdot z^* - c(\bar{n},\hat{a}) + \mathbb{E}\left\{v(\bar{n},\hat{a} \cdot z^*)\right\}. \tag{2.10}$$

This has the associated first order conditions

$$(1 + \mathbb{E} \{\partial_{\bar{n}_s} v\}) (z_i^* + \hat{a} \cdot \nabla_{\hat{a}_i} z^*) = \partial_{\hat{a}_i} c, \ i = 1, \dots, d,$$
  
$$\partial_{\bar{n}} c = \mathbb{E} \{\partial_{\bar{n}} v\}.$$
(2.11)

The second condition states that expected future returns on unsold tokens held by the seller must equal, on the margin, their marginal cost of production. We will return to this condition when examining the consequences of a token possessing a security characteristic. The first condition contains the marginal benefit - marginal cost relationships for the characteristic mix decision, and is dependent upon the functional form of the buyer's utility function. For example, if the buyer's utility function is Cobb-Douglas in characteristics:

$$U(z,m) := \prod_{i=1}^{d} z_i^{\alpha_i} + m, \ \sum_{i=1}^{d} \alpha_i = 1,$$

with the  $\alpha_i$  denoting the income share of characteristic i (or equivalently, the Arrow-Pratt coefficient of relative risk aversion for  $z_i$ ), then  $d(\hat{a} \cdot z^*) = 0 \,\forall \hat{a}$  and an interior solution for  $\hat{a}^*$  cannot be found.

In addition, we haven't (yet) placed restrictions upon  $c(\bar{n}, \hat{a})$  and  $v(\bar{n}, n_s)$  to determine whether or not an equilibrium exists given the buyer's optimal demand function  $z^*$ . Some headway can be made regarding characteristic selection, however. Note that provided  $1 + \mathbb{E} \{\partial_{\bar{n}_s} v\}$  and  $\nabla_{\hat{a}} c$  are both non-zero (component-by-component for the latter) then

at the optimal value  $\hat{a}^*$ , the first condition of relation 2.11 implies

$$z_i^* \lessgtr \sum_{j=1}^d \hat{a}_j^* \cdot \left( -\frac{\partial z_j^*}{\partial \hat{a}_i} \right) \, \forall i, \tag{2.12}$$

or

$$\hat{a}^* \cdot z^* \leqslant -\hat{a}D_{\hat{a}}z^*\hat{a},\tag{2.13}$$

where  $D_{\hat{a}}z^*$  is the  $(d \times d)$  Jacobian matrix of  $z^*$  with respect to  $\hat{a}$  (evaluated at  $\hat{a}^*$ ).

By the separating hyperplane theorem we could ensure that (2.13) holds if  $\hat{a}$  comes from an open convex set ( $z^*$  comes from a convex set by construction). Unfortunately this is not generally the case as values  $\hat{a}_j = 0$  for some j are admissible, and hence the set of characteristic mixtures available to the seller is closed. In order to prevent this we impose the assumption that the only offered characteristics within a particular mixture are those with a non-zero amount in the token, i.e.

**Assumption 1.** The set of admissible unit mixtures A is given by

$$\mathcal{A} := \left\{ \hat{a} \in \mathbb{R}_{++}^d \mid \sum_{j=1}^d \hat{a}_j^2 = 1 \right\}. \tag{2.14}$$

With Assumption 1 in hand we can ensure that (2.13) holds and that an interior solution to the optimal mixture problem can be found.

### 2.5 Market Clearing

In specifying the seller as a monopolist we have already imposed market clearing for the token, i.e.  $n_s = n_d$  automatically because the seller takes the entire demand function  $z^*$  as given. But clearing the token market does not necessarily clear the (imputed) characteristic market—this is an additional requirement because otherwise the characteristics demanded by the buyer may not be supplied by the seller.<sup>12</sup> Thus the full definition of market equilibrium is

**Definition 1.** A token market equilibrium is a token price  $q^*$ , a characteristic distribution mix  $a^*$ , and a token supply  $\bar{n}^*$  such that given buyer income y, buyer preferences  $U(\cdot,\cdot)$ , seller cost function  $c(\cdot,\cdot)$  and seller return function  $v(\cdot)$ ,

 $<sup>^{12}\</sup>mathrm{This}$  is a consequence of using the Moore-Penrose inverse to break the lock-step selection of characteristics offered and token quantity demanded by the buyer that would otherwise occur if, say, the buyer were restricted only to choose the token quantity  $n_d$  demanded, taking the relative supply of characteristics per token a and hence total characteristics consumed  $z=n_da$  as given. See Section 2.6 for further details.

1. the token market clears, i.e.

$$n^* \coloneqq n_s^* = n_d^*, \tag{2.15}$$

2. the characteristic market clears, i.e.

$$z^* = n^* a^*, (2.16)$$

- 3. the buyer's problem (2.4) is solved, and
- 4. the seller's problem (2.10) is solved.

Imposing condition (2.16) ensures that in the end the characteristics demanded by the buyer are supplied by the seller, at the token market price  $q^*$  and imputed characteristic prices  $p^* = \frac{q^*a^*}{\|a^*\|^2}$ . The Definition is stated using  $a \in \mathbb{R}^d_{++}$  rather than using the unit vector representation  $\hat{a} = a/\|a\|$ , but this is a formality only and it will be demonstrated shortly that only the unit vector representation is germane to the optimization problems of the buyer and seller when market clearing is taken into consideration.

#### 2.5.1 Clearing the market for characteristics

Condition (2.16) restricts the set of feasible characteristic mixes a that a firm can select. Here we remain agnostic as to the exact mechanism that clears the market, much as in general equilibrium theory where recourse is sometimes made to a 'Walrasian auctioneer'. But in practical terms it will generally be the seller, possibly in cooperation with e.g. marketing or advertising firms, who will understand the underlying demand for characteristics (as assumed here) and adjust their a's accordingly.

In order to see if condition (2.16) can be fulfilled we first restate it with a small change in notation, to emphasize that both  $z^*$  and  $n^*$  explicitly depend upon a (they also may depend upon other parameters—such as the token price q, for instance—but we abstract away from this in the second argument of these functions).

With this change the following Proposition demonstrates the existence of a marketclearing characteristic mix.

**Proposition 1.** There exists a mix  $a^* \in \mathbb{R}^d_{++}$  that clears the characteristic market. This mix induces a class  $C_{a^*} := \{a \in \mathbb{R}^d_{++} \mid a = ka^*, k \in \mathbb{R}_{++}\}$  whose members each clear the market.

*Proof.* To show existence, first define a mapping  $F: \mathbb{R}^d_{++} \times \mathbb{R}^d \to \mathbb{R}^d$  from (2.16) by

$$F(a,z) := (A(a) - I)z, \tag{2.17}$$

where  $A(a) := \frac{1}{\|a\|^2} a \otimes a$  is the matrix generated by a normalized (Kronecker) outer product of a characteristic mix a with itself. Then a market clearing mix a will satisfy  $F(a, z^*(a, \cdot)) = 0$ , since

$$z^*(a,\cdot) = n^*(a,\cdot)a \Leftrightarrow (a^{-1} \cdot z^*(a,\cdot))a = \frac{1}{\|a\|^2} a(a \cdot z^*(a,\cdot)) = A(a)z^*(a,\cdot), \text{ i.e.}$$
 (2.18)

$$A(a)z^*(a,\cdot) - z^*(a,\cdot) = 0 = F(a,z^*(a,\cdot)).$$
(2.19)

Because A(a) is a normalized outer product of a with itself for every a, A(a) has a non-degenerate unit eigenvalue with eigenvector a (because  $a \otimes a$  has a non-degenerate eigenvalue equal to  $||a||^2$  with eigenvector a). In other words,

$$F(a,a) = 0 \quad \forall a \in \mathbb{R}^d_{++}.$$

Let a market-clearing characteristic mix be denoted by  $a^*$ . The non-degeneracy of the unit eigenvalue immediately implies that at  $a^*$ , the demand function  $z^*(a^*, \cdot)$  must be proportional to  $a^*$ :

$$z^*(a^*, \cdot) = k(\cdot)a^*,$$

where k is a constant of proportionality that will in general depend upon other factors such as income, token price etc. Since the buyer's problem generates at least one positive demand  $z_i^*$  for some i, k must be non-zero. The set of all rays proportional to  $a^*$  thus defines the class  $C_{a^*}$ .

**Corollary 1.** Let the set of market clearing characteristics be given by

$$\bar{\mathcal{A}} := \{ a \in \mathbb{R}^d_{++} \mid F(a, z(a, \cdot)) = 0 \}.$$

Then the characteristic classes  $C_{a^*}$  partition  $\bar{A}$ .

*Proof.* The market clearing condition defines an equivalence relation  $\sim$  over  $\mathbb{R}^d_{++}$ , where  $a \sim a' \Leftrightarrow a, a' \in \mathcal{C}_a$ , i.e. a = ka' for some strictly positive constant k. Denote the set  $\{\mathcal{C}_{\alpha}\}$  of all characteristic classes by  $\mathcal{C}$  and the index set of  $\mathcal{C}$  by  $\mathcal{I}$ .<sup>13</sup> Note that for any two classes  $\mathcal{C}_{\alpha}$ ,  $\mathcal{C}_{\beta} \in \mathcal{C}$ ,  $\alpha, \beta \in \mathcal{I}$ ,

$$\mathcal{C}_{\alpha} \cap \mathcal{C}_{\beta} = \emptyset$$
.

In addition, because  $a \in \bar{\mathcal{A}} \Rightarrow \exists \alpha \in \mathcal{I} \ni a \in \mathcal{C}_{\alpha}$ , we must have

$$\bigcup_{\alpha\in\mathcal{I}}\mathcal{C}_{\alpha}=\bar{\mathcal{A}}.$$

 $<sup>^{13}</sup>$ The index set  $\mathcal{I}$  thus runs over all mixes which are not proportional to each other. We claim momentarily that this set must be at most countably infinite.

Thus, the classes in C partition  $\bar{A}$ .

With this result in hand we define a **representative** of the class  $C_{a^*}$  as any member of the class, and without loss of generality and for tractability we select the unit vector  $\hat{a}^*$  as the representative of  $C_{a^*}$  that is used by buyers and sellers in their decision-making. This makes sense because Proposition 1 states that it is sufficient for buyers and sellers to restrict their attention to the case where a is a unit vector, i.e. it is only the direction, and not the magnitude, of the characteristic mix which defines market clearing. This is also clear in the relation z = na, since we can always define  $\hat{n} := n||a||$  and  $\hat{a} := a/||a||$  and  $z = \hat{n}\hat{a}$  remains unchanged.

**Definition 2.** The admissible set  $\hat{A}$  of characteristic mixes is the set of all (non-zero component) unit vector representations of market clearing characteristics, i.e.

$$\hat{\mathcal{A}} := \{ a \in \mathcal{A} \cap \bar{\mathcal{A}} \}.$$

Without further assumptions on the buyer's demand functions  $z^*$  it is not possible to demonstrate that  $\mathcal{C}$  contains only one member, i.e. that the market clearing characteristic mix is unique (up to direction). However, we shall appeal to genericity to argue that there does not exist a continuum of market clearing characteristic mixes, as then infinitesimal perturbations of buyer preferences would destroy them.<sup>14</sup> This implies that the number of market clearing characteristic mixes is at most a countable infinity, and each mix is locally isolated.

This has an important consequence for the seller's problem: because the market clearing characteristic mixes are locally isolated, the seller does not need to explore how profit varies with infinitesimal changes in the characteristic mix a, but must instead rank market clearing mixes to achieve the highest level of profit after selecting the token price q and the number of tokens to sell  $n_s$  (which, because the seller is a monopolist, is assumed to equal the buyer's demand function  $n_d$ ). This may considerably simplify the seller's token design problem, particularly if—it is to be hoped—the buyer's demand function is such that only a few (or one) market clearing characteristic exists. An explicit example is given in Section 3.

# 2.6 Comparison with Rosen (1974)

Rosen (1974) introduced the seminal hedonic pricing paradigm for understanding how markets clear when goods may be considered as bundles of non-market characteristics.

<sup>&</sup>lt;sup>14</sup>We can also appeal to index theory as in general equilibrium models, and impose conditions upon preferences such that 1) the market clearing characteristic mixes are locally isolated, and 2) the number of such mixes is odd. Although this is interesting in its own right, we shall adopt the genericity argument to claim local isolatedness and leave the index of the set of equilibria to later analysis.

The prices of these characteristics are imputed from a buyer's willingness to pay (on the margin) for a characteristic. For the buyer, Rosen treats the quantity decision (i.e. choosing the number of units of the good n to consume) and the characteristic decision (i.e. choosing the level of characteristic  $z_i$  to consume, for each i) as independent degrees of freedom. This leads to the first order conditions

$$\frac{\partial U(n, z, m)}{\partial n} = P(z) \frac{\partial U(n, z, m)}{\partial m},$$

$$\frac{\partial U(n, z, m)}{\partial z_i} = n \frac{\partial P(z)}{\partial z_i} \frac{\partial U(n, z, m)}{\partial m},$$
(2.20)

where U is the utility function over the quantity n of the good, the characteristics z contained therein, and money m, P is the price of the good that depends upon z, the budget constraint is given by  $y \ge m + nP(z)$  and the condition  $\lambda = \partial U/\partial m$  has been substituted throughout for the Lagrange multiplier associated with the budget constraint.

This approach is especially fruitful for defining indifference surfaces for the buyer based upon their willingness to pay for a particular characteristic, all other characteristics (and income) held constant. Importantly, the optimal selection of n may be 'folded in' to this willingness to pay, so that the submitted demand functions to the market do not contain n at all.

This latter conclusion is the point of departure for the approach presented here, which is somewhat different from Rosen's because the quantity of tokens demanded by the buyer is not a degree of freedom—rather, it is a consequence of the buyer's demand for characteristics, and cannot be independently selected. Rosen includes the quantity of the good (treated as a 'brand' or 'model') in the utility function of the buyer, i.e. U = U(n, z, m) as above. By contrast, here we assume that the quantity of the token carries no independent value from its characteristic use, and hence n is only a derived quantity rather than a fundamental one. In addition to supporting a possible argument for greater realism when applied to preferences over tokens (which may, more than physical goods, be thought of as providing essentially no value apart from their characteristics), in the end the demand functions that are considered by the seller when making characteristic and quantity decisions are, as in Rosen (1974), independent of the quantity demanded.

On the seller side, the present approach and Rosen's approach both assume that there exists a cost function that depends upon characteristics and the quantity of the good/token produced. The main difference is that in Rosen's model firms are competitors (the price of the good P(z) is assumed to be independent of n), while here the token supplier is assumed to be providing a token with some form of uniqueness, and hence the supplier is a monopolist. This reflects the notion that tokens with a utility characteristic

are presumed to differentiate their use from those of other tokens. 15

Rosen's approach uses market clearing to solve the optimal price function P(z) as a function of z. This is cleverly achieved by using the willingness-to-buy (and the seller's associated willingness-to-sell) functions to define a set of partial differential equations that P(z) must satisfy, and to provide conditions under which a solution exists. By contrast, in our approach market clearing does not impose this potentially heavy computational burden upon a market auctioneer mechanism. Rather, a more traditional partial equilibrium approach is provided which can give the seller, in selecting the characteristic mix as well as the token's price, a straightforward computational method for determining the equilibrium token design and hence market clearing conditions.

Finally, it is important to underscore that in the present model the buyer does not recognize the impact of their characteristic demand upon the price of the token, beyond the impact upon the quantity of the token demanded. Rather than rely upon the partial derivative of the price function to define an imputed price system, as in Rosen (1974), the Moore-Penrose inverse fulfills the same purpose by allowing a buyer to disentangle their demand for characteristics in a way that preserves their quantity demanded. At first this appears to introduce an unrealistic state of affairs—one might argue to the contrary that as the vector of characteristics a is 'primal', the quantity of characteristics demanded by a buyer (i.e., z) should be fixed for all time by the token demand  $n_d$ , such that

$$z \equiv n_d a$$
.

In other words, since only multiples of a are available anyway, it could be argued that the buyer's demand for characteristics should be placed on a grid of such multiples.

This is not the case, however—by using the Moore-Penrose inverse, a decomposition of  $n_d$  is made such that z is demanded conditional upon, but without fixed multiples of, the characteristic mix a. Of course, in equilibrium the quantity and characteristic mix offered by the seller will be that demanded by the buyer, so that the implicit market for characteristics—and the explicit market for the token—both clear. But there is no ex ante need for buyer demand to be restricted to lie on a grid defined by multiples of a.

# 3 Security Tokens and Intertemporal Optimization

If one of the characteristic roles of a token is as a security, i.e. as a claim on the current/future value of the token issuer, then the general model in Section 2 can be sharpened to provide additional insight.

<sup>&</sup>lt;sup>15</sup>Of course, as the token market continues to become saturated with new offerings, the model presented here may be extended to allow for e.g. imperfect competition or (as a limiting/benchmark case) perfect competition.

To that end, suppose that there are now two periods, 1 and 2, in which the token is sold only in period 1 and there is no uncertainty about the state of nature in period 2. As before a token contains d characteristics and we let one of the characteristics, k, be a security characteristic. The associated characteristic amount  $z_k$  confers upon the holder of the token a return in period 2, which may be spent on non-token-related consumption x.<sup>16</sup> Let this return be defined as  $rz_k$ , with  $r \in \mathbb{R}_+$  acting as rate of return for k.

In this way the token acts in two different ways: first, as a bearer instrument granting the holder the right to a return that can be used for non-token-specific consumption in period 2, and second as a good granting token-specific consumption (i.e. the benefit or utility of using the token) in period 1.

The role of money is relegated here to an additional savings channel—in principle this prevents the seller from extracting ex ante 100% of the buyer's resource y, as the buyer may substitute token consumption with money m as a transfer of wealth to the second period (although the seller may select prices to induce the buyer to freely choose m=0). This immediately implies that non-zero demand of both the security characteristic and money can only occur when the rates of return for each are identical—if this is not the case then one will dominate the other as a means of wealth transfer. As we shall see, in order to ensure a non-zero demand for the security characteristic the seller must set the discounted rate of return  $r/p_k$  (where  $p_k$  is the imputed price of security characteristic k) to a value greater than the rate of return on money. Finally, we assume that both the seller and the buyer have the same access to money, and that there is a risk-free rate of return on m given by  $r_f > 0$ .

### 3.1 The Modified Buyer's Problem

With a security token we can be more explicit about the buyer's preferences over characteristics. Recalling that characteristic k is the security characteristic, we define the modified buyer's problem as

$$\max_{z,x,m} u_1(z_{\sim k}) + \beta u_2(x)$$
such that
$$y \geq p \cdot z + m,$$

$$rz_k + (1 + r_f)m \geq x,$$

$$z_i \geq 0, \ m \geq 0,$$
(3.1)

 $<sup>^{16}</sup>$ Consumption x is assumed to take place only in period 2. In contrast to the general model in Section 2, the unit of account m is no longer simply a proxy for non-token-related consumption. Rather, we assume instead that period 2 consumption x is financed through holdings of the token and holdings of m as an alternative, safe investment described further below.

where  $\beta \in (0,1)$  is the buyer's subjective discount factor,  $z_{\sim k}$  denotes the vector of characteristics excluding characteristic  $k, x \in \mathbb{R}_+$  is second period consumption, prices are once again given by  $p := q\hat{a}$ , and m is money.<sup>17</sup> Per-period utility functions  $u_1 : \mathbb{R}_+^{d-1} \to \mathbb{R}$  and  $u_2 : \mathbb{R}_+ \to \mathbb{R}$  are assumed to have standard properties with respect to their arguments. The discount factor  $\beta$  is introduced as usual to connect preferences across time, acting as a conversion factor between enjoyment today and enjoyment tomorrow. Finally, we explicitly mention the non-negativity constraints given the trade-off between  $rz_k$  and m in funding second period consumption (the non-negativity constraint on x is satisfied immediately given the monotonicity of  $u_2$ ). The Lagrange multipliers for the problem are, in order of constraints above,  $\lambda$  for the period 1 resource constraint,  $\mu$  for the period 2 constraint,  $\tau_i$  for each non-negativity constraint on  $z_i$  and  $\delta$  for the constraint on m.

The buyer's problem can be divided into three mutually exclusive cases, depending upon the selection of r and q from the seller (which the buyer takes as given). Ultimately the case we are interested in is when the seller provides incentives to the buyer to purchase the token in order to facilitate all period 2 consumption, to the exclusion of money. The first two cases treated below cover this particular equilibrium outcome for the buyer.

#### **3.1.1** Case I: $m = 0, z_k > 0$

If m = 0 and  $z_k > 0$ , the Lagrange multiplier condition requires that  $\tau_k = 0$ . The first order conditions for problem (3.1) then imply

$$p_k \lambda = r\mu \Leftrightarrow (1 + r_f)\mu + \delta = \frac{r}{p_k}\mu.$$

With m=0 the Lagrange multiplier  $\delta$  may be zero or positive. Considering for the moment the sub-case  $\delta > 0$ , we have as a result that

$$\frac{r}{p_k} = \frac{r}{qa_k} > 1 + r_f$$

as the condition for  $z_k > 0$  when m = 0, indicating that the rate of return on the security role exceeds the rate of return on m, which equals  $1 + r_f$ .<sup>18</sup>

In this situation, the first-order conditions further imply that for all characteristics i not equal to the security characteristic k,

$$\beta \frac{\partial u_2/\partial x}{\partial u_1/\partial z_i} = \frac{p_k/r}{p_i} = \frac{1}{r} \frac{\hat{a}_k}{\hat{a}_i}, \ i \neq k. \tag{3.2}$$

<sup>17</sup>Recall that an equilibrium characteristic mix a will have ||a|| = 1, so that the characteristic mix is a unit vector.

<sup>&</sup>lt;sup>18</sup>One may perhaps wonder why, since the buyer only values second period consumption x, the marginal utility of consumption  $\partial u_2/\partial x$  is not factored into the returns of m and  $z_k$ . This is because both provide the *same* marginal utility per unit, and so only the wealth-equivalent comparisons matter for demand.

This relates the intertemporal marginal rate of substitution between consumption of c tomorrow and consumption of  $z_i$  today—it must be equal to the ratio of the return-discounted
price of facilitating x tomorrow by purchasing units of the security characteristic,  $p_k/r$ ,
and the price of characteristic i today,  $p_i$ . This ratio is in turn given solely by the returndiscounted ratio of characteristics available in the token.

#### **3.1.2** Case II: $m \ge 0, z_k \ge 0$

The subcase where m=0 and  $\delta=0$  from the previous case is incorporated here into the situation when the buyer is indifferent between holding m or  $z_k$ . It is not hard to show from the first order conditions (and is intuitively clear) that this occurs when  $z_k \geq 0$  and  $\tau_k = 0$ , and the condition is that the rates of return for the two instruments are identical, i.e.

$$\frac{r}{p_k} = \frac{r}{q\hat{a}_k} = 1 + r_f. {(3.3)}$$

In the seller's problem we shall see that this case is the limiting choice of r and q that maximizes profit, because when m=0 the seller captures the buyer's entire period 1 resource allocation y. Thus the seller seeks to drive r down to the lowest level possible while maintaining m=0, arriving in the limit to relation (3.3).

### **3.1.3** Case III: $m > 0, z_k = 0$

Finally, the case in which money demand is positive and the security characteristic demand is zero is symmetric to Case I and will obtain if

$$\frac{r}{p_k} = \frac{r}{q\hat{a}_k} < 1 + r_f.$$

It is straightforward to show that this will not be an equilibrium selection for the seller because this choice of q and r, although providing positive profit to the seller if  $z_k > 0$ , forces the buyer to select  $z_k = 0$ . The seller would then be forced to adjust r and q until relation (3.3) just obtains, where a positive value of  $z_k$  is a utility-maximizing choice for the buyer.

#### 3.1.4 Demand functions

We note in passing that since this is a standard constrained optimization problem, when m=0 there exist continuous demand functions<sup>19</sup>

$$z_i^*(p,r;y) = z_i^*(q,r,a;y), i \neq k; \ x^*(q,r,a;y); \ z_k^*(q,r,a;y) = \frac{x^*}{r}$$
(3.4)

<sup>&</sup>lt;sup>19</sup>cf e.g. Mas-Colell et al. (1995).

that solve the buyer's problem (we will generally suppress the dependence of the buyer's demands  $z^*$  and  $x^*$  on y in what follows).

#### 3.2 The Modified Seller's Problem

The seller acts as a monopolist in token sales, as before. In order to focus solely upon the allocation problem when the token has a security role we dispense with the outside option for unsold tokens and concentrate upon the problem where the seller supplies only the buyer's demand for tokens in period 1, and assumes a debt obligation associated with the buyer's security role holdings  $z_k^*$  in period 2. This obligation is funded by taking a part of period 1 profit and setting it aside in a risk-free account paying interest  $r_f$ . The seller wishes to select a token price q, an 'interest' rate r and a characteristic mix a to solve, conditional upon their cost function c(n, a), the problem<sup>20</sup>

$$\max_{q,r,a} q(a^{-1} \cdot z^*(q,r,a)) - c(a^{-1} \cdot z^*(q,r,a),a) - \frac{1}{1+r_f} r z_k^*(q,r,a).$$
 (3.5)

We fix ||a|| = 1 as per the discussion in Section 2.5.1. Before delving into the first-order conditions we note that as described in Section 3.1, the potential for a non-zero level of demand for characteristic k,  $z_k \geq 0$ , and hence extraction of the buyer's full period 1 resource level y, requires that

$$r \ge (1 + r_f)p_k = (1 + r_f)q\hat{a}_k.$$
 (3.6)

The seller thus selects combinations (q, r) to fulfill this constraint, conditional upon  $\hat{a}$ .

We will argue below that the optimal price/interest rate combination will drive equation (3.6) to equality. One may think of this as being due, all other things equal, to the seller *losing* profit on sales of characteristic k, but making up for the loss from sales of the token as an aggregate good to the buyer. The security role creates an incentive for the buyer to purchase the token irrespective of its other uses—indeed, from the buyer's problem, the lower the marginal utility from non-security characteristics  $\partial u_1/\partial z_i$ ,  $i \neq k$ , the more the non-zero demand for k via  $z_k > 0$  pulls demand for the token as a whole, and hence for the other characteristics bundled therein, allowing the seller to make a profit on the token sale.<sup>21</sup>

<sup>&</sup>lt;sup>20</sup>As before n is the total number of tokens supplied—which is here the total number  $n_d = a^{-1}z^*(q, a, r)$  sold to the buyer in period 1–and the function c has standard properties.

 $<sup>^{21}</sup>$ If this were not the case, e.g. if characteristics each had their own separate market, then this argument would not hold. One might then need to suggest that the seller has access to financial markets with a higher risk-free rate than the buyer, to allow the seller to gain positive profits in the buyer's Case I. But the point here is that because the token is a bundled good, such an asymmetry is not required—a negative rate of return on k, ceteris paribus, does not imply negative profits for the seller.

With this in mind, the seller's full problem is

$$\max_{q,r,\hat{a}} q(\hat{a} \cdot z^*(q,r,\hat{a})) - c(\hat{a} \cdot z^*(q,r,\hat{a}),\hat{a}) - \frac{1}{1 + r_f} r z_k^*(q,r,\hat{a})$$
(3.7)

$$r \ge (1 + r_f)q\hat{a}_k,\tag{3.9}$$

$$\hat{a} \in \hat{\mathcal{A}}.\tag{3.10}$$

Denoting the Lagrange multiplier of the return constraint (3.9) by  $\lambda$ , the associated first-order conditions with respect to q and r are straightforward to derive:

$$\left(q - \frac{\partial c}{\partial n}\right) \left(\hat{a} \cdot \nabla_q z^*\right) = -\hat{a} \cdot z^* + \frac{1}{1 + r_f} r \frac{\partial z_k^*}{\partial q} + \lambda (1 + r_f) a_k, \tag{3.11}$$

$$\left(q - \frac{\partial c}{\partial n}\right)\left(a \cdot \nabla_r z^*\right) = \frac{1}{1 + r_f} \left(z_k^* + r \frac{\partial z_k^*}{\partial r}\right) - \lambda. \tag{3.12}$$

System (3.11) - (3.12) states the conditions under which an optimal selection  $(r^*, q^*)$  may be found by the seller, conditional upon a selected characteristic mix  $\hat{a} \in \hat{\mathcal{A}}$ . To proceed further, suppose first that the return constraint (3.9) is non-binding, so that  $r > (1 + r_f)qa_k$ . Then r > 0 provided q > 0 and  $\lambda = 0$ , and the buyer strictly prefers to invest  $z_k^* > 0$  for future consumption and sets  $m^* = 0$ . Note that this means the seller extracts the entire resource amount y from the buyer, and thus Walras' Law holds for the buyer's period 1 budget constraint. This implies

$$q\hat{a} \cdot \nabla_r z^* = 0, \tag{3.13}$$

$$\hat{a} \cdot \nabla_q z^* + \hat{a} \cdot z^* = 0, \tag{3.14}$$

i.e. the buyer does not vary their token expenditure with respect to q or r.

Using these relations and  $\lambda = 0$  reduces the first order conditions (3.11) - (3.12) to

$$-\frac{\partial c}{\partial n} \left( \hat{a} \cdot \nabla_q z^* \right) = \frac{1}{1 + r_f} r \frac{\partial z_k^*}{\partial q}, \tag{3.15}$$

$$\frac{1}{1+r_f} \left( z_k^* + r \frac{\partial z_k^*}{\partial r} \right) = 0. \tag{3.16}$$

Thus, if  $z^*$  is a vector of normal goods in q, i.e. if—all else equal—the buyer reduces their demand for every characteristic following an increase in the token price q, then

1. since  $\hat{a} \cdot \nabla_q z^* < 0$ , (3.15) implies that there must be increasing returns to scale in token production, i.e.  $\partial c/\partial n < 0$ , for a positive token amount to be produced, and

2. the elasticity of the buyer's second period consumption with respect to the offered rate r is zero, since equation (3.16) implies

$$\left. \frac{\mathrm{d}}{\mathrm{d}r} r z_k^* = \left. \frac{\mathrm{d}}{\mathrm{d}r} x^* \right|_{q=q^*, r=r^*} = 0.$$

For a digital good such as a cryptocurrency token, there are compelling reasons why it might be assumed that the marginal cost of production goes to zero as the number of tokens produced increases, if token creation proceeds with (virtually) no additional variable costs once sunk costs have been paid.<sup>22</sup> It is difficult, however, to imagine a situation where marginal costs become negative. In addition, although it is possible that one or more characteristics constitute an externality to the buyer, and hence that for such characteristics the demand response to an increase in price is positive (equivalently, a decrease in the token price reduces demand for that characteristic), it is unrealistic to assume that such an *inferior characteristic* (or characteristics) would overwhelm the demand responses of the other characteristics.

For these reasons we shall continue to focus in this simple environment upon a seller providing characteristics that generate positive utility flows for the buyer, and relegate the question of optimal allocation when a subset of characteristics may be treated as externalities to future research.

Thus, in what follows we suppose that return constraint (3.9) binds, so that  $\lambda > 0$  and  $r = (1 + r_f)q\hat{a}_k$ . At this combination of q and r the buyer is indifferent between selecting  $z_k$  or m, or some combination thereof, as the storage of wealth to enable second period consumption x. Moreover, the level of consumption selected,  $x^*$ , is (given q) constant along the locus defined by  $z_k$  and m acting as perfect substitutes,

$$x^* = (1 + r_f)(q\hat{a}_k z_k + m). \tag{3.17}$$

See Appendix 4 for the straightforward derivation of (3.17).

Let the locus of  $(\bar{z}_k, \bar{m})$  denote the points satisfying (3.17). Note that there is no price or interest rate response from  $\bar{z}_k$  since the buyer is indifferent between  $\bar{z}_k$  and m, and hence there is no utility improvement in changing either in response to changes in q (or r). Then Walras' Law implies

<sup>&</sup>lt;sup>22</sup>On the other hand, Bitcoin has shown that consensus mechanisms such as Proof-of-Work may by contrast introduce decreasing returns to scale, as e.g. greater and greater electricity requirements must be met for further token increases. Alternative consensus mechanisms such as Proof-of-Stake may preserve the increasing returns to scale cost structure.

$$\sum_{i \neq k} \hat{a}_i \left( q \frac{\partial z_i^*}{\partial q} + z_i^* \right) + \hat{a}_k \bar{z}_k \bigg|_{r = (1 + r_f)q\hat{a}_k} = 0.$$
(3.18)

With the binding constraint (3.9) and the implication of Walras' Law (3.18) the first-order conditions may be simplified to a single relationship relating the marginal cost of production to the buyer's demand response from the token price q:

$$-\frac{\partial c}{\partial n} \sum_{i \neq k} \hat{a}_i \frac{\partial z_i^*}{\partial q} = \hat{a}_k \bar{z}_k, \tag{3.19}$$

or

$$\frac{\partial c}{\partial n} = \frac{\hat{a}_k \bar{z}_k}{-\sum_{i \neq k} \hat{a}_i \frac{\partial z_i^*}{\partial q}}.$$
(3.20)

This expression states that the marginal cost of producing a token must equal the ratio of the weighted security characteristic demand to the weighted demand response to the token price q. Further insight into (3.20) can be found by appealing to the buyer's problem—equation (3.2), reproduced here, stated that the marginal rate of substitution between non-security characteristics and the security role was proportional to the ratio of characteristics:

$$\beta \frac{\partial u_2/\partial x}{\partial u_1/\partial z_i} = \frac{1}{r} \frac{\hat{a}_k}{\hat{a}_i}, \ i \neq k.$$

Substituting this into (3.20) yields

$$\frac{\partial c}{\partial n} = -\beta \frac{\mathrm{d}u_2/\mathrm{d}x}{\mathrm{d}u_1/\mathrm{d}q} r \bar{z}_k, \tag{3.21}$$

where  $du_1/dq := \sum_{i \neq k} \frac{\partial u_1}{\partial z_i^*} \frac{\partial z_i^*}{\partial q}$  and for symmetry we adopt the notation  $du_2/dx$  to replace  $\partial u_2/\partial x$ .

Suppose for the moment that  $x^* > r\bar{z}_k$ , i.e. that  $m^* > 0$ . The seller can guarantee revenue equalling the buyer's entire first period resource amount y by increasing r ever-so-slightly above  $(1+r_f)q\hat{a}_k$ , so that the buyer selects  $m^* = \bar{m} = 0$  and  $x^* = rz_k = r\bar{z}_k$ . Although technically in the  $r > (1+r_f)q\hat{a}_k$  regime we spent some time arguing was unrealistic, this selection nevertheless preserves relation (3.21): we can extend the  $(\bar{z}_k, \bar{m}) = (x^*/r, 0)$  selection into the  $r = (1+r_f)q\hat{a}_k$  regime, since the buyer has no incentive to deviate. This outcome is fairly general and can be extended in many directions. For example, if the interest rate r were stochastic with support  $S := [(1+r_f)q\hat{a}_k, \infty)$  and Lebesque measure  $\mu$  over S, and there existed a set  $R := \{r \in \text{int}(S) \mid \Pr(r) > 0\}$ , then the buyer would strictly prefer selection  $(\bar{z}_k, \bar{m}) = (x^*/r, 0)$  when the measure  $\mu(R) > 0$  and would weakly prefer the selection as  $\mu(R) \to 0$ .<sup>23</sup>

<sup>&</sup>lt;sup>23</sup>Put still another way, the buyer could have beliefs over the seller that place non-zero measure on the

Thus, we can restate (3.21) as

$$\frac{\partial c}{\partial n} = -\beta \frac{\mathrm{d}u_2/\,\mathrm{d}x}{\mathrm{d}u_1/\,\mathrm{d}q} x^*.$$

Since characteristics  $z_i$  are assumed to act as normal goods we know that  $du_1/dq$  is negative, and so we may finally write

$$\frac{\partial c}{\partial n} = \beta \frac{\mathrm{d}u_2/\mathrm{d}x}{|\mathrm{d}u_1/\mathrm{d}q|} x^*. \tag{3.22}$$

Equation (3.22) is the fundamental relation governing token design for a monopolist seller faced with an aggregate demand  $z^*$ , when the interest rate offered for the security role k is  $r = (1 + r_f)q\hat{a}_k$ . Because the seller extracts the entire surplus y from the buyer, the relation states that the optimal token price is the one which balances the first period utility loss of the buyer from an infinitesimally higher q (which lowers token demand) against the discounted second period utility gain from a consequent infinitesimally higher r. Each side of the relation is denominated in units of buyer utility, with as usual the discount factor  $\beta$  facilitating the comparison between utility in period 1 and that in period 2.

### 4 Conclusion

The hedonic pricing approach presented here has outlined one potential method to value a bundled good such as a cryptocurrency token, with an eye toward connecting the value as a consumer benefit to the value as a seller's revenue driver. Both buyer and seller have the most conservative of objectives in this approach—the buyer maximizes utility (of the token as something providing direct utility, i.e. useful as something-in-itself, as well as providing indirect utility, i.e. as a transfer across time) while the seller maximizes economic profit (from the token as a product-in-itself, as well as a mechanism to transfer wealth from the future).

Once this foundation has been laid, however, there is no reason why the environment cannot be expanded to encompass different objectives of both the buyer and the seller. For example, once a token valuation approach has been adopted, the seller can design a token to *elicit* buyer behavior that may or may not further economic profit, but may instead incentivize objectives such as responsible investment or environmentally conscious consumption. While not guaranteed, it may be that such design approaches allow opportunities for incentivizing to occur *before* ignoring external effects becomes a global, social

possibility that the seller chooses  $r > (1 + r_f)q\hat{a}_k$ , and the argument goes through as the measure goes to zero.

externality, as has occurred (for example) with the overuse of plastic and its concomitant disposal problem.

Similarly, throughout this analysis has been the implicit reliance upon the 'incorruptibility' of the cryptocurrency token, based as it is upon an immutable, auditable ledger technology such as blockchain, so that what the seller states are the characteristics present in the token is trusted. In an extended model with many idiosyncratic buyers this trust would in principle allow buyer-to-buyer incentive mechanisms to form—a savvy seller would in turn design the token to be used in this fashion to again support one or more objectives, including but not limited to economic profit. Naturally this again requires as a point of departure a way to assign value to this token's 'consumer-to-consumer' aspect, similar to the way goods—such as automobiles—are produced taking into account potential secondary resale markets from their outset.

Using a hedonic pricing methodology helps to fill the conceptual (and empirical) gap in our understanding of cryptocurrency valuation by allowing a straightforward assessment of both the scale and scope of the seller's intentions when creating a token. Although there is a paucity of data—or techniques—available to estimate characteristics, applying existing empirical methodologies from traditional hedonic pricing models may help to define areas where future research is needed most. At the very least, understanding the data provenance, requirements, and availability, and not simply relying upon cryptocurrency exchange time series data, would appear to be one of the most urgent areas for further study.

Finally, the existence of an equilibrium environment (as coarsely outlined in the present study) that can be examined from the different perspectives that the token itself provides via its characteristics (security, utility, etc.) can help regulators and designers agree on how existing and future cryptocurrency tokens should be placed into a 'taxonomy' that allows an even, transparent and clearly defined application of legislation. After all, it is to the benefit of both regulators and designers that they should each understand the rules of the game before embarking upon their respective activities. Weighing the relative valuations of e.g. a token's utility aspect with its security aspect, as the present study affords, may help regulators apply legislation designed for securities and other assets in a clear-cut manner to those tokens that possess dominant security values. At the same time, tokens with dominant utility values may then be subject to legislation that nurtures an ecosystem where e.g. blockchain interaction or incentivization mechanisms are the main objectives of the token, fostering rather than stifling innovation. If these and other valuation methodologies become commonplace, a fruitful (and stable) development of the cryptocurrency token ecosystem becomes significantly more likely.

# **Appendix**

### Derivation of relation (3.17)

Consider the buyer's problem when  $r = (1 + r_f)q\hat{a}_k$ , i.e. when the buyer is indifferent between using m or  $z_k$  to store wealth for second period consumption—the problem can be suggestively written as

$$\max_{z,x,m} u_1(z_{\sim k}) + \beta u_2(x)$$
such that
$$y \ge q \sum_{i \ne k} \hat{a}_i z_i + (q \hat{a}_k z_k + m),$$

$$(1 + r_f)(q \hat{a}_k z_k + m) \ge x.$$

Thus, the buyer's problem in this case implies consumption (and hence utility) levels that are exactly equivalent to the problem

$$\max_{z,x,m} u_1(z_{\sim k}) + \beta u_2(x)$$
  
such that  
$$y \ge q \sum_{i \ne k} \hat{a}_i z_i + \frac{1}{1 + r_f} x.$$

In particular, second period consumption  $x^* = x^*(q)$  (suppressing dependence upon  $\hat{a}$ ) is fixed once q is given, and the locus of points  $(z_k, m)$  satisfy  $x^*(q) = (1 + r_f)q\hat{a}_kz_k + m$ , with  $z_k \in [0, x^*/(q\hat{a}_k)]$  and  $m \in [0, x^*]$ .

### References

- Barata, J. C. A., & Hussein, M. S. (2011). The moore-penrose pseudoinverse. a tutorial review of the theory. doi:10.1007/s13538-011-0052-z. arXiv: http://arxiv.org/abs/1110.6882v1 [math-ph]
- Ben-Israel, A., & Greville, T. N. E. (2003). Generalized inverses. Springer New York.
- Berentsen, A., & Schar, F. (2018). A Short Introduction to the World of Cryptocurrencies. Review. St. Louis Federal Reserve Quarterly Research Journals, 100(1), 1–16. doi:10. 20955/r.2018.1-16
- Bogart, S. (2018). The Trend That Is Increasing The Urgency Of Owning Bitcoin And Ethereum. Retrieved October 17, 2018, from https://www.forbes.com/sites/spencerbogart/2017/10/08/the-trend-that-is-increasing-the-urgency-of-owning-bitcoin-and-ethereum/
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2), 213–238. doi:10. 1257/jep.29.2.213
- Conley, J. P. (2017). Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings (Department of Economics Working Paper No. 17-00008). Vanderbilt University. Retrieved from https://ideas.repec.org/p/van/wpaper/vuecon-sub-17-00007.html
- Epple, D. (1987). Hedonic prices and implicit markets: Estimating demand and supply functions for differentiated products. *Journal of Political Economy*, 95(1), 59–80. doi:10.1086/261441
- Hargrave, J., Sahdev, N. K., & Feldmeier, O. (2018). How Value is Created in Tokenized Assets. SSRN Electronic Journal. doi:10.2139/ssrn.3146191
- Hinman, W. (2018). Digital asset transactions: When Howey met Gary (Plastic). Retrieved from https://www.sec.gov/news/speech/speech-hinman-061418
- Houthakker, H. S. (1952). Compensated changes in quantities and qualities consumed. The Review of Economic Studies, 19(3), 155–164. doi:10.2307/2296018
- Lachance, N. (2016). Not Just Bitcoin: Why The Blockchain Is A Seductive Technology To Many Industries. *National Public Radio Online*. Retrieved from https://www.npr.org/sections/alltechconsidered/2016/05/04/476597296/not-just-bitcoin-why-blockchain-is-a-seductive-technology-to-many-industries
- Lancaster, K. J. (1966). A new approach to consumer theory. Journal of Political Economy, 74(2), 132-157. doi:10.1086/259131
- Leonhard, R. (2017). Corporate Governance on Ethereum's Blockchain. West Virginia University College of Law. doi:10.2139/ssrn.2977522

- Marr, B. (2016). How Blockchain Technology Could Change The World. Forbes. Retrieved from https://www.forbes.com/sites/bernardmarr/2016/05/27/how-blockchain-technology-could-change-the-world/#6609318c725b
- Mas-Colell, A., Whinston, M. D., & Green, J. R. (1995). *Microeconomic theory*. Oxford University Press.
- Rosen, S. (1974). Hedonic Prices and Implicit Markets: Product Differentiation in Pure Competition. *Journal of Political Economy*, 82(1), 34–55. doi:10.1086/260169