5-7-2019

Establishing Cryptocurrency Equilibria Through Game Theory

Carey Caginalp

Gunduz Caginalp

Establishing Cryptocurrency Equilibria Through Game Theory

Comments

This article was originally published in *AIMS Mathematics*, volume 4, issue 3, in 2019. https://doi.org/10.3934/math.2019.3.420

Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 4(3): 420–436.
DOI:10.3934/math.2019.3.420
Received: 02 March 2019
Accepted: 25 March 2019
Published: 07 May 2019

Research article

Establishing cryptocurrency equilibria through game theory

Carey Caginalp[1,2,*] **and Gunduz Caginalp**[1]

[1] University of Pittsburgh, Mathematics Department, 301 Thackeray Hall, Pittsburgh, PA, USA
[2] Chapman University, Economic Science Institute, 1 University Drive, Orange, CA, USA

* **Correspondence:** Email: carey_caginalp@alumni.brown.edu.

Abstract: We utilize optimization methods to determine equilibria of cryptocurrencies. A core group, the wealthy, fears the loss of assets that can be seized by a government. Volatility may be influenced by speculators. The wealthy must divide their assets between the home currency and the cryptocurrency, while the government decides the probability of seizing a fraction the assets of this group. We establish conditions for existence and uniqueness of Nash equilibria. Also examined is the separate timescale problem in which the government policy cannot be reversed, while the wealthy can adjust their allocation in reaction to the government's designation of probability.

Keywords: mathematical finance; game theory; cryptocurrency; optimization
Mathematics Subject Classification: 91A05, 91A80, 91B26, 91B30, 91B50

1. Introduction

Cryptocurrencies have evolved into a new speculative asset form that differs from others in that most represent no intrinsic value; they cannot be redeemed by a financial institution for any amount [1]. The roller-coaster ride of Bitcoin prices* from \$6,000 to \$20,000 back to \$6,000, with bounces in between, all during the period from October 2017 to July 2018, was shadowed by other major cryptocurrencies [17]. This has been accompanied by the general feeling in government, business and academia that the speculative fever is of concern only to those who own the cryptocurrencies. There is some justification for this perspective as the total market capitalization of all cryptocurrencies is now only about \$131 billion, so that large moves in the cryptocurrency price are not likely to have a significant impact on the world's stock and bond markets. However, this impact will present a significant risk to the world's markets if the market capitalization of the cryptocurrencies increases significantly. During the dramatic round trip of Bitcoin between \$6,000 to \$20,000, the market capitalization of all cryptocurrencies nearly doubled in six months. Moreover,

*In March 2019, Bitcoin hovered near \$3,800.

10,000 Bitcoins were used to purchase two pizzas in the first transaction in 2010 [32]. If people gradually become more comfortable with cryptocurrencies, as they did with internet shopping, it is likely that the market capitalization could grow to a few percent of the $75 trillion Gross World Product (GWP) as the fraction of the world's savings that is under threat by government seizure, high inflation, etc., is certainly at least this fraction (as discussed further below). At this point, large price changes in cryptocurrencies would likely have an impact on the broader markets.

It is thus important to understand the factors behind the market capitalization and price of cryptocurrencies. With all other assets there is some theoretical methodology to determine the value, which is at least a first step estimating the trading price. For example, the value of a stock is assessed by measures such as the expected dividend stream and other measures (see Graham [21, 22], Luenberger [27], Bodie et al. [4], and Wolpert et. al. [39]). Even beyond these calculations, a shareholder is *de facto* part owner of a corporation, and shareholders can – and do – collectively exercise their rights assured by law. By contrast, a typical cryptocurrency does not assure the owner of any rights. Furthermore, there is no corporate governance at all. The "miners and developers" – whose names are usually not disclosed – get together and decide essentially on the supply (e.g., by introducing a related cryptocurrency that they term a "fork"). Unlike corporate actions in which shareholders can demand a vote, e.g., for directors via a proxy battle, it is not even clear which, if any, nation's laws apply. Thus, the absence of an intrinsic value of a cryptocurrency means that the usual traditional finance methods, such as those introduced by Graham ([21, 22]), are inapplicable.

Our analysis begins with a game theoretic examination of the motivations of three groups that are the key players. For a core group, the basic need for a cryptocurrency arises from the inadequacy of the home currency and banking system [33]. There are also a significant number of people who are not able to obtain a credit card or even open a bank account in the US, for example [38]. In many countries, owning large amounts of the currency can present a significant risk. There is the possibility of expropriation by the government, sometimes in the guise of a corruption probe. The government could institute policies in which inflation is very high, e.g., the extreme example in Venezuela [20] where hyperinflation decimated any individual savings. Onerous taxes can be placed by the government on the wealthy. Thus a group of people in the world have rational reasons to replace their country's currency with one that is outside the control of their government or financial institutions, even if it presents some risk. Once it is transferred to cryptocurrency, they would have the option of buying a more reliable currency or asset in another country. We denote this group by $\mathcal{W}$ (the "wealthy"). Returning to the point made above, there is a substantial amount of the world's wealth (including individual's whose assets are not large) that is in this situation. Many of these people, however, are not yet comfortable with or knowledgeable about cryptocurrencies. As they feel more comfortable, a greater fraction of this wealth may move into cryptocurrencies, inflating the market capitalization, perhaps to a few percent of the world's GWP.

The second group, $\mathcal{D}$, represents a government that is totalitarian, at least with respect to monetary policy, so that its citizens are not free to transfer their wealth into other, more reliable national currencies. There is a probability, p, that the government can initiate policies that will deprive citizens of a fraction k of their wealth, e.g., by printing money. This possibility is noted by the wealthy, $\mathcal{W}$, who must make a decision on the fraction of their assets, denoted $1 - x$ held in the home currency and the remainder, x, in cryptocurrency, which presents risks of its own due to the volatility. The government, $\mathcal{D}$, exhibits risk aversion as with any financial entity. After all, its existence is dependent on obtaining funds from its citizens. A third group, $\mathcal{S}$, consists of the speculators† whose sole reason to trade is to profit from the transaction at the expense of the less knowledgeable group, $\mathcal{W}$. In a typical situation, the member of $\mathcal{W}$ is trading for the first or second time – having made their money in another endeavor – while the speculators are professionals who have made thousands of trades, and make their living at the expense of novice traders. The speculators effectively determine the volatility (see Appendix). Note, however, that our analysis would be similar if the volatility were an exogenous variable that is set arbitrarily. While $\mathcal{D}$ can set the probability, p, with which the assets can be seized, group $\mathcal{W}$ can decide what fraction, x, to convert into the cryptocurrency.

We model this situation to find equilibria in two different ways. The first is to find the Nash equilibrium [13, 18, 28, 29, 35] which is defined as the point (p^*, x^*) such that neither party can improve its fortunes by unilateral action. The underlying assumption is that both parties, $\mathcal{W}$ and $\mathcal{D}$, are aware of the situation faced by the other, so that they can simultaneously self-optimize while assuming that the other party does likewise.

In a later section, we utilize the more realistic assumption that while $\mathcal{W}$ can make immediate changes (e.g., one day), $\mathcal{D}$ must make a decision that is irrevocable during a longer time (e.g., one year) as policies (e.g., creating inflation, imposing onerous taxes) are implemented. But in doing so, $\mathcal{D}$ must be aware that $\mathcal{W}$ will self-optimize in its choice of x, knowing p. Thus, both parties are aware of the different time scales involved in anticipating the other party's decision.

The methods we present in this paper are aimed at determining the demand using optimization. The investors of the cryptocurrency do not have any clear idea how much is the right amount to pay per unit of the cryptocurrency, so that the demand will determine the trading price as discussed in Appendix A and [9]. In a setting in which there is one cryptocurrency with a fixed supply, the price will be determined as

$$\text{Equilibrium Trading Price} = \frac{\text{Demand in Dollars}}{\text{Number of Units}}. \tag{1.1}$$

Analogous methodology can be utilized for multiple cryptocurrencies.

One might be led to examining cryptocurrencies in the context of monetary policy, but the terminology "currency" is the main similarity between the cryptocurrencies and the US Dollar, Euro, Yen, etc. The differences are profound‡. Major currencies are established by governments within a well-defined process that is governed by law. The identities of those who are responsible for monetary policy are known. The citizens of the country can influence the representatives who appoint the monetary officials. Finally, if the citizens feel that the direction of monetary policy is not in their interest, they can elect new representatives. There have been many currencies throughout the world, and it is no accident that the most viable currencies have been those of the countries with the most respect for the law and the voices of their citizens.

Thus, the theory of monetary policy will be of limited use in the understanding today's cryptocurrencies. The aspect of our analysis that is closest to monetary policy involves the actions of the government, $\mathcal{D}$, which must make a decision on issues such as generating inflation (see, e.g., [2, 3]). Of course, the government in our analysis is one that is very different from the major democratic governments that have the more reliable currencies.

†In commodities such as gold and oil, there are producers and industrial users who must trade. In cryptocurrencies, there are no end users other than $\mathcal{W}$ who are trade infrequently, unlike industrial users for gold, for example, who are perpetually trading.

‡This point is probably clear to anyone who bought Bitcoin at \$20,000 and sold it at \$6,000 several months later.

Since the widespread use of cryptocurrencies is a fairly new phenomenon, the literature is also recent. Many papers have focussed on the blockchain technology and its potential for increased speed and safety of transactions. The introduction of JP Morgan's JPM Coin (see Appendix A) is an example of utilization of this technology without any new economic issues, since JPM Coin would be redeemable in US Dollars. The economics of cryptocurrencies have been discussed in terms of legal issues [24], valuation [15], security issues [5, 16] and stability [7, 23, 26, 30] and feasibility [12]. Experiments have also been used to study cryptocurrencies and related issues [14, 19].

Our analysis can be viewed in the more general setting of an asset that is easily traded and out of the reach of the state and other entities. However, the popularity of cryptocurrencies may indicate that there are not so many of these. Traditionally, gold has been used as a haven, but it is not always easy to prevent theft. Nevertheless, followers have often noted spikes in gold when there is political uncertainty in the highly populated and less developed countries. Also, the demand for gold depends upon other factors such as industrial use.

2. The utility functions of the groups

The general framework for this section will be to write the utility functions of the three groups, modeled on portfolio theory [27], [4] whereby one seeks allocate resources to maximize return while minimizing risk. The general form for a basic utility function is $U = m - d^2\sigma^2$ where m and σ^2 are the expectation and variance of the outcome, while the parameter d^2 quantifies the risk aversion.

The speculators, $\mathcal{S}$, are assumed to have an influence on the volatility and risk. Even if they had no influence on the volatility, they are likely to profit at the expense of $\mathcal{W}$, who are likely to be novices (as discussed above). Hence, the role of $\mathcal{S}$ is secondary (and discussed in the Appendix) as they create an expected loss and a variance for $\mathcal{W}$.

Focusing now on the groups, $\mathcal{W}$ and $\mathcal{D}$, we assume that $\mathcal{W}$ has a choice between the home currency, F, and a cryptocurrency, Y. Any money held in F faces the risk that a fixed fraction $k \in [0, 1]$ will be seized by $\mathcal{D}$ with probability p. Thus, the outcome will be $(1 - x)(1 - k)$ with probability p and 1 with probability $1 - p$. Letting m_F and σ_F^2 denote the mean and variance of the investment in F, one finds,

$$\begin{aligned} m_F &= (1-k)\,p + 1\cdot(1-p) = 1 - kp, \\ \sigma_F^2 &= k^2 p\,(1-p)\,. \end{aligned} \tag{2.1}$$

For the investment in Y, we let m_Y and σ_Y^2 denote the mean and variance that may be determined by the speculators (see Appendices B and C).

The utility function for $\mathcal{W}$ with the fraction $x \in [0, 1]$ of its assets in Y and the remainder in F can then be expressed as

$$\begin{aligned} U_W &= m - d^2\sigma^2 \qquad (2.2) \\ &= x m_Y + (1-x)\, m_F \\ &- d^2\left\{x^2\sigma_Y^2 + (1-x)^2\sigma_F^2 + 2x(1-x)\,Cov\,[Y,F]\right\}. \end{aligned}$$

We will assume that the correlation between the two assets, Y and F, is zero, but the analysis can easily be carried out if there is a correlation.

The utility function for $\mathcal{D}$ can be expressed in terms of the amount that it seizes, i.e.,

$$U_D = (1-x)\,kp. \tag{2.3}$$

This can be augmented with a term (as in portfolio theory) that expresses the risk aversion. In particular, one has

$$U_D = (1-x)\,kp - d_D^2 p^2, \tag{2.4}$$

where d_D^2 represents the risk aversion of $\mathcal{D}$.

3. Nash equilibria

We assume the utility functions described in Section 3, using the risk aversion form of U_D above (2.4) . Thus, we need to find (p^*, x^*) such that

$$\begin{aligned} \partial_x U_W(p^*, x^*) &= 0, \;\; \partial_p U_D(p^*, x^*) = 0, \\ \partial_{xx} U_W(p^*, x^*) &\leq 0, \;\; \partial_{pp} U_D(p^*, x^*) \leq 0\,. \end{aligned}$$

i.e., (p^*, x^*) satisfies the definition of a Nash equilibrium (see e.g., [18, 28]). Briefly, the definition ensures that at (p^*, x^*) neither party can unilaterally improve its situation. We compute

$$0 = \partial_p U_D(p,x) = (1-x)\,k - 2d_D^2 p, \tag{3.1}$$

$$\begin{aligned} 0 &= \partial_x U_W(p,x) = m_Y - m_F + 2d^2\sigma_F^2 - 2d^2\left(\sigma_Y^2 + \sigma_F^2\right)x \\ &= m_Y - 1 + kp + 2d^2k^2p\,(1-p) - 2d^2\left(\sigma_Y^2 + k^2p\,(1-p)\right)x. \end{aligned} \tag{3.2}$$

Denote the solution of (3.1) by $x_1(p)$ and that of (3.2) by $x_2(p)$, so that

$$x_1(p) = 1 - \frac{2d_D^2 p}{k} \tag{3.3}$$

$$\begin{aligned} x_2(p) &= \frac{\sigma_F^2 + \left(2d^2\right)^{-1}(m_Y - m_F)}{\sigma_F^2 + \sigma_Y^2} \\ &= \frac{k^2p\,(1-p) + \left(2d^2\right)^{-1}(m_Y - 1 + kp)}{k^2p\,(1-p) + \sigma_Y^2}. \end{aligned} \tag{3.4}$$

The intersection of $x_1(p)$ and $x_2(p)$ determine a Nash equilibrium. We first establish sufficient conditions for at most one equilibrium, and then prove that under broad conditions, there exists a Nash equilibrium. Some of these curves for sample values of the parameters are illustrated in Figure 1.

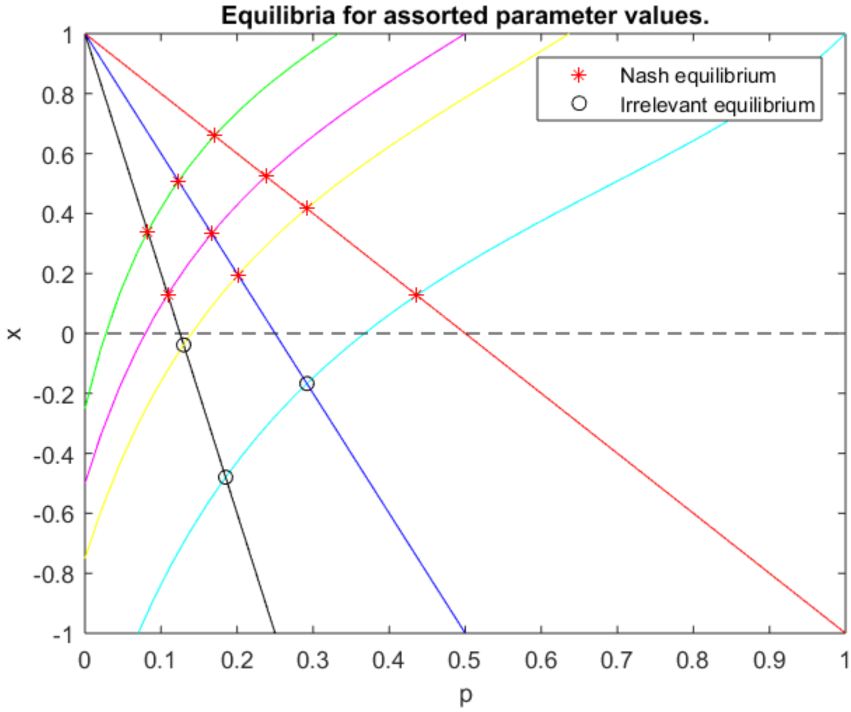

Figure 1. Selected curves modeling the fraction x of wealth to be placed into cryptocurrency from the perspectives of groups $\mathcal{D}$ and $\mathcal{W}$. The linear curves represent the optimization for $\mathcal{D}$ and the others for $\mathcal{W}$. We plot the curves for values of $a := 2\frac{d_D^2}{k} = 8, 4, 2$ against fraction under seizure k and expected loss/trading cost on cryptocurrency $b := 1 - m_Y$ given by $(k, b) = (.5, .7), (.55, .85), (.6, .9), (.75, .95)$ (starting from the upper left curve) with volatility $c := \sigma_Y^2 = 0.1$ and group $\mathcal{W}$'s risk tolerance $d = 1$ both held constant in both sets of curves. When there is an intersection in the range $(p^*, x^*) \in (0, 1)^2$, we have a Nash equilibrium. It is possible to have other intersections outside of this box, but such "equilibria" are irrelevant and their behavior will lead to boundary cases such as $p = 0$ or $p = 1$.

Theorem 1. *For $p \in [0, 1/2]$ one has $x_2'(p) \geq 0$ for all values of the parameters, so there can be at most one value of p such that $x_1(p) = x_2(p)$, and thus at most one Nash equilibrium for $p \in [0, 1/2]$.*

Proof. For convenience set $f(p) = k^2 p(1-p)$, $c_1 = \left(2d^2\right)^{-1}(1 - m_Y)$, $c_2 = \left(2d^2\right)^{-1} k$ and $c_3 = \sigma_Y^2$ so that

$$x_2(p) = \frac{f(p) + c_2 p - c_1}{f(p) + c_3}$$

and

$$x_2'(p) = \frac{c_2 k^2 p^2 + c_2 c_3 + (c_1 + c_3) k^2 (1 - 2p)}{[f(p) + c_3]^2}. \tag{3.5}$$

Clearly, for $p \in [0, 1/2]$ all terms are positive and the conclusion follows. □

Theorem 2. *If the parameters d, k and m_Y satisfy*

$$c_1 + c_3 \leq c_2 \text{ i.e., } \left(1 + 2d^2\right)(1 - m_Y) \leq k \tag{3.6}$$

then $x_2'(p) \geq 0$ *for all* $p \in [0,1]$. *Thus there can be at most one Nash equilibrium under these conditions.*

Proof. For $p \in [0,1/2]$ the result has been established. For $p \in [1/2,1]$ the numerator of (3.5) is

$$c_2k^2p^2 + c_2c_3 + c_2k^2(1-2p) = c_2c_3 + c_2k^2(1-p)^2 > 0,$$

and the result follows. □

Having determined sufficient conditions for uniqueness, we now focus on establishing existence of Nash equilibrium. Note first that the $p-$intercept of $x_1(p)$ can be on either side of $x = 1$ depending on the slope $-2d_D^2/k$. In particular, we let $p_c := k\left(2d_D^2\right)^{-1}$ and consider the two cases separately.

Theorem 3. (*a*) *If* $p_c := k\left(2d_D^2\right)^{-1} < 1$ *and*

$$k^2p_c(1-p_c) + \left(2d^2\right)^{-1}(m_Y - 1 + p_ck) > 0, \tag{3.7}$$

then one has a Nash equilibrium, i.e., there exists $(p^*, x^*) \in [0,1]\times[0,1]$ *such that* $x_1(p^*) = x_2(p^*) = x^*$.

(*b*) *If* $p_c := k\left(2d_D^2\right)^{-1} \geq 1$ *and*

$$\frac{\left(2d^2\right)^{-1}(m_Y - 1 + k)}{\sigma_Y^2} + \frac{2d_D^2}{k} \geq 1$$

then one has again a Nash equilibrium.

If in addition, equation (3.6) *holds, then the Nash equilibrium* (p^*, x^*) *is unique.*

Proof. Recall that $m_Y \leq 1$. Thus, we have the inequality,

$$1 = x_1(0) > 0 \geq x_2(0) = (m_Y - 1)/\left(2d^2\sigma_Y^2\right).$$

We use the Intermediate Value Theorem to establish an intersection between $x_1(p)$ and $x_2(p)$ in the unit square in (p,x) space.

Case (a). Suppose $p_c := k\left(2d_D^2\right)^{-1} < 1$. Then

$$x_2(p_c) = \frac{k^2p_c(1-p_c) + \left(2d^2\right)^{-1}(m_Y - 1 + p_ck)}{k^2p_c(1-p_c) + \sigma_Y^2}$$

so that by (3.7) one has $x_2(p_c) \geq 0 = x_1(p_c)$. Thus there exists an intersection of $x_1(p)$ and $x_2(p)$ at $(p^*, x^*) \in [0,0]\times[p_c, x(p_c)] \in [0,1]\times[0,1]$.

Case (b). Suppose $p_c := k\left(2d_D^2\right)^{-1} > 1$. Then $x_1(1) > 0$, and $x_1(p) \in [0,1]$ for $p \in [0,1]$. Thus, an intersection of $x_1(p)$ and $x_2(p)$ for $p \in [0,1]$ must occur on the unit square provided that $x_2(1) \geq x_1(1)$. Then the required condition is

$$\begin{aligned} x_2(1) &= \frac{\left(2d^2\right)^{-1}(m_Y - 1 + k)}{\sigma_Y^2} \\ &\geq 1 - \frac{2d_D^2}{k} = x_1(1). \end{aligned}$$

□

Remark 4. *The Nash equilibrium may not be unique if the condition above, i.e.,*

$$\left(1 + 2d^2\right)(1 - m_Y) \leq k$$

of Theorem 3 is violated. An example for two Nash equilibria can be constructed with the parameters:

$$k = 0.7,\ m_Y = 0.8,\ d = 2,\ d_D = 0.355,\ \sigma_Y^2 = 0.1.$$

The two equilibria are given approximately by $(p^*, x^*) = (0.88, 0.68)$ *and* $(0.96, 0.65)$*, as displayed in Figure 2.*

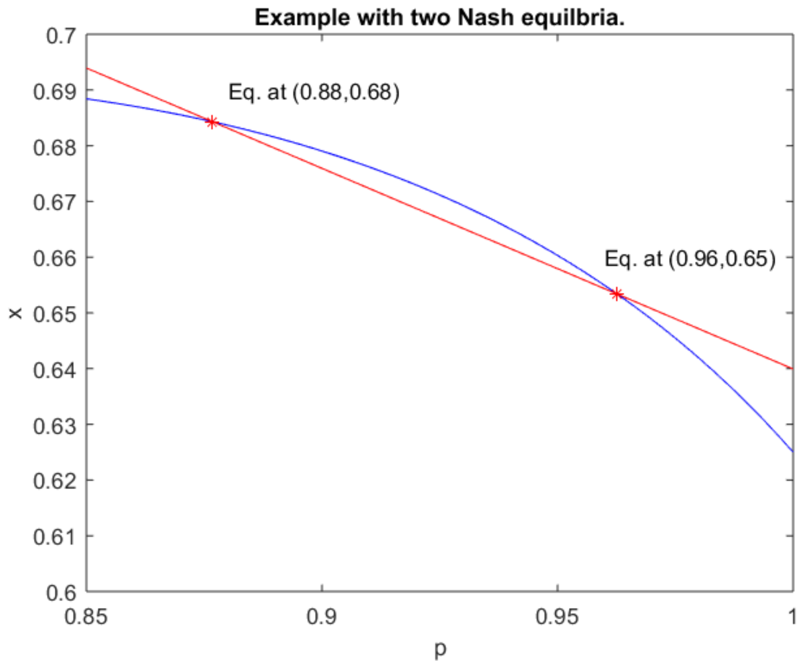

Figure 2. Under certain combinations of parameters, for example $k = 0.7, b = 0.8, d = 2, d_D = .355$, and $\sigma_Y^2 = 0.1$, we can have two Nash equilibria. The eventual steady-state of the solution would depend on where the initial conditions lie with respect to these two points.

4. Equilibrium with disparate time scales

We consider the situation in which the wealthy, $\mathcal{W}$, can decide on an allocation x immediately, (e.g., within one day), and adjust to the probability, p, while $\mathcal{D}$ must set p that cannot be changed for a long time e.g., one year. Thus, $\mathcal{D}$ lacks the opportunity to react to the value of x. Both parties are aware of the position of the other group. Hence, $\mathcal{D}$ knows that once he sets p, group $\mathcal{W}$ will set $x = \hat{x}(p)$ in a way that optimizes U_W, and that $\mathcal{W}$ does not need to be concerned with any readjustment of p in reaction to their choice of x. Thus, $\mathcal{D}$ must examine U_W (based on the publicly available information on the volatility of Y) and decide on a value of p that will optimize $U_D(p, \hat{x}(p))$. Within this setting the utility of $\mathcal{D}$ need not be strictly convex in order for an interior maximum (i.e. such that $0 < p < 1$ and $0 < x < 1$). Thus, we consider the case in which $\mathcal{D}$ has utility that is proportional to the amount it takes, without any risk aversion, which can be included with a bit more calculation.

We define the quantity

$$A := 2d^2\sigma_Y^2 + 1 - m_Y \tag{4.1}$$

which arises naturally in the calculations and is a measure of the risk and expected loss from Y. Thus a higher value of A means Y is less attractive to the wealthy.

Theorem 5. *Suppose that the utility functions, U_W and U_D, given by*

$$\begin{aligned} U_D &= (1-x)\,kp \\ U_W &= m - d^2\sigma^2 \\ &= xm_Y + (1-x)\,m_F - d^2\left\{x^2\sigma_Y^2 + (1-x)^2\,\sigma_F^2 + 2x(1-x)\,Cov\,[Y,F]\right\}. \end{aligned}$$

are known to both parties. Assume that $\mathcal{D}$ sets p irrevocably to maximize U_D, while $\mathcal{W}$ chooses x to maximize U_W based on a knowledge of p. For $0 \leq A < k$ the optimal choice of x given p is

$$\hat{x}(p) := \frac{m_Y - m_F}{2d^2\left(\sigma_Y^2 + \sigma_F^2\right)} + \frac{\sigma_F^2}{\sigma_Y^2 + \sigma_F^2} \tag{4.2}$$

with m_Y and σ_F^2 given by (2.1)*, and the optimal value of p is given by*

$$p^* := \frac{\sigma_Y^2}{k(k-A)}\left(\sqrt{1 + \frac{A}{\sigma_Y^2}(k-A)} - 1\right). \tag{4.3}$$

Thus the optimal point is $(p,x) = (p^*, \hat{x}(p^*))$. The value of maximum, $x^* = \hat{x}(p)$ is 0 *if the right hand side of* (4.2) *is negative, and* 1 *if the right hand side exceeds* 1.

Remark 6. *Note that given p the optimal fraction of assets in the cryptocurrency is a sum of the relative variance of the home currency, i.e., σ_F^2 as a fraction of $\sigma_Y^2 + \sigma_F^2$ plus the difference in expected loss from the home currency, i.e., $1 - m_F$ minus the expected loss from the cryptocurrency, $1 - m_Y$ scaled by a risk aversion factor. Thus the fraction invested in the cryptocurrency increases as the expected loss and the variance of the home currency increases, and conversely.*

Remark 7. *Note that one obtains an interior maximum with a linear utility function for U_D in this type of optimization, i.e., even though $\mathcal{D}$ is interested in pure maximization of its revenue.*

Proof. Using (2.2) we determine the maximum of U_W for a fixed p, so that

$$0 = \partial_x U_W(p,x) = m_Y - m_F + 2d^2\sigma_Y^2 - 2d^2\left(\sigma_Y^2 + \sigma_F^2\right)x.$$

Noting that $\partial_{xx} U_W(p,x) = -2d^2\left(\sigma_Y^2 + \sigma_F^2\right) < 0$ we see that U_D is maximized by $\hat{x}(p)$ given by (4.2) provided $\hat{x}(p) \in [0,1]$. In the following two cases the maximum is on the boundary:

$$\frac{m_Y - m_F}{2d^2} + \sigma_F^2 < 0 \;\text{ implies }\; \hat{x}(p) = 0,$$

$$\frac{m_Y - m_F}{2d^2} + \sigma_F^2 > 1 \;\text{ implies }\; \hat{x}(p) = 1.$$

Thus, $\hat{x}(p)$ interpolates between 0 and 1 by favoring Y if the relative risk of F (measured by $\sigma_F^2\left(\sigma_Y^2+\sigma_F^2\right)^{-1}$ is large in comparison with the relatively greater expected loss in Y (scaled by the sum of the variances).

In anticipation, $\mathcal{D}$ optimizes $U_D(p, x(p))$. We thus compute, with $B := \sigma_Y^2$,

$$
\begin{aligned}
0 &= \frac{2d^2}{k}\partial_p U_D(p, x(p)) = \partial_p \frac{Ap - kp^2}{B + k^2 p(1-p)} \\
&= \frac{(A-2kp)\left[B + k^2 p(1-p)\right] - \left(Ap - k^2 p\right)\left[k^2(1-2p)\right]}{\left[B + k^2 p(1-p)\right]^2}.
\end{aligned}
$$

This identity is equivalent to

$$
Q(p) := AB - 2Bkp + k^2(A-k)p^2 = 0. \tag{4.4}
$$

Note that $A > 0$ by assumption. The positive root of equation (4.4) is

$$
p^* = \frac{B}{k(k-A)}\left(\sqrt{1 + \frac{A}{B}(k-A)} - 1\right).
$$

One can verify that $p^* \in [0,1]$, and conclude that $(p^*, x^*) = (p^*, \hat{x}(p^*))$ is the optimal point. $\square$

Remark 8. *Case* $A = 0$. *By definition* (4.1) *we see that* $1 - m_Y = 0$. *Note that* $p^* = 0$ *follows from the identity above. Using the definition and the computed values of* $m_F = 1 - kp$ *and* $\sigma_F^2 = k^2 p(1-p)$ *we write*

$$
\begin{aligned}
\hat{x}(p) &= \frac{m_Y - 1 + kp}{2d^2\left(\sigma_Y^2 + k^2 p(1-p)\right)} + \frac{k^2 p(1-p)}{\sigma_Y^2 + k^2 p(1-p)} \\
\hat{x}(0) &= \frac{m_Y - 1}{2d^2\sigma_Y^2} = 0.
\end{aligned}
$$

In other words, when $A = 0$ *there is no risk and no expected loss in the cryptocurrency. Thus,* $\mathcal{D}$ *realizes that any nonzero value of p will result in* $\mathcal{W}$ *investing nothing in the home currency, F.*

Case $A = k$. *The quadratic numerator* (4.4) *is then* $Q(p) = AB - 2Bkp$ *so that one has* $p^* = 1/2$.

Case $k < A \leq 2k$. *By considering a small positive perturbation,* δ, *of A we see that* $Q\left(\frac{1}{2}\right) > 0$ *so that the positive region of* $\partial_p U_D$ *is extended toward the right as A increases.*

Case $A \geq 2k$. *Since* $p \leq 1$ *one has*

$$
Q(p) \geq B(A-2k) + k^2 p^2 (A-k) > 0,
$$

so $\partial_p U_D > 0$ *and the maximum is thus* $p^* = 1$.

5. Conclusion

We have examined the optimal strategies for the key parties (those with savings at risk, a dictatorial government and speculators) involved explicitly or implicitly in the formation of an equilibrium for cryptocurrencies. The second method involves different time scales in determining equilbrium that differs from the more common Nash equilibrium, in which all parties can readjust their positions continuously. As described in Section 4 this can be utilized for many realistic situations in which one entity such as a government optimizes by placing conditions such as taxes, tariffs, fees, etc., or policies that cannot be reversed or adjusted in a short time. In general, optimization in this form favors the group that can make immediate and continuous adjustments.

Each of the methods are based on parameters that can be estimated. For example, the variance of cryptocurrencies can be determined from the trading data. Parameters such as k (the fraction of assets seized) can be estimated from the policies of the government. An assessment of these quantities then leads to estimates of the amount of money that is likely to be used to purchase cryptocurrencies in the aggregate. Using the ideas summarized in [9] one can then also evaluate average price changes of cryptocurrencies as well as the total market capitalization of cryptocurrencies. The evolution of the latter is crucial in understanding the implications of instability of cryptocurrencies on other sectors of the world's economy.

Major governments have often appeared confused and lethargic in their response to cryptocurrency policy, even insofar as deciding whether it is important or not. There is also little understanding of the conditions under which a cryptocurrency could be either beneficial or detrimental to global society. The perspective of our paper suggests that a cryptocurrency price will vary widely depending on the demand that in turn is based on policies of countries where monetary policy and laws, in general are less developed. Together with the fact that cryptocurrencies cannot be redeemed for any asset, one cannot expect much stability. However, given a mechanism whereby a cryptocurrency is essentially backed by real assets (e.g., a structure similar to Exchange Traded Funds) one would have stability since arbitrageurs would take advantage of any discrepanicies. This could be linked of course to a single currency such as the US Dollar, but would only be a trading token in this case.

However, one can design a cryptocurrency that would essentially grow with the world's economy, unlike a commodity such as gold. A simple example would be that the cryptocurrency could be reedemable in units of the Gross World Product in terms of a basket of major currencies, so that each cryptocurrency could be redeemed for one trillionth of the GWP in Dollars, Euros and Yen. Such an instrument would offer much greater stability and could be used as a substitute currency that is independent of any government. As shown in our analysis, as the volatility risk would diminish, and those whose assets in the home currency are at risk would place more of their assets into this cryptocurrency. Thus the fraction, x, placed in the cryptocurrency would increase. In particular, the equilibrium point (p^*, x^*) would feature x^* that is larger and p^* that is smaller. This would mean that the citizens have greater economic freedom, and financially totalitarian regimes would have smaller resources. In summary, the creation of a viable cryptocurrency with intrinsic value would have less volatility, and thereby reduce the fraction of savings in the home currency that is under threat by a totalitarian government, whose existence is often contingent on raising money in this manner.

Acknowledgments

The authors thank the Economic Science Institute at Chapman University and the Hayek Foundation for their support. Discussions with Prof. Gabriele Camera are very much appreciated.

Conflict of interest

The author declares that there is no conflicts of interest in this paper.

References

1. Z. Bernard, Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator, 2017. Available from: http://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12.
2. R. J. Barro, *Rational expectations and the role of monetary policy*, Journal of Monetary economics, **2** (1976), 1–32.
3. R. J. Barro and D. B. Gordon, *A Positive Theory of Monetary Policy in a Natural Rate Model*, Journal of Political Economy, **91** (1983), 589–610.
4. Z. Bodie, A. Kane and A. J. Marcus, Essentials of Investments 9th Edition. McGraw-Hill, 2012.
5. R. M. Bratspies, Cryptocurrency and the Myth of the Trustless Transaction, 2018. Available from: https://ssrn.com/abstract=3141605 or http://dx.doi.org/10.2139/ssrn.3141605.
6. C. Brunetti, B. Büyükşahin and J. H. Harris, *Speculators, Prices, and Market Volatility*, Journal of Financial and Quantitative Analysis, **51** (2016), 1545–1574.
7. C. Caginalp, *A Dynamical Systems Approach to Cryptocurrency Stability*, arXiv preprint: 1805.03143, 2018.
8. G. Caginalp and D. Balenovich, *Asset flow and momentum: deterministic and stochastic equations*, Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, **357** (1999), 2119–2133.
9. C. Caginalp and G. Caginalp, *Opinion: Valuation, liquidity price, and stability of cryptocurrencies*, Proceedings of the National Academy of Sciences, **115** (2018), 1131–1134.
10. G. Caginalp, D. Porter and V. Smith, *Initial cash/asset ratio and asset prices: An experimental study*, Proceedings of the National Academy of Sciences, **95** (1998), 756–761.
11. G. Caginalp, D. Porter and V. Smith, *Financial bubbles: Excess cash, momentum, and incomplete information*, The Journal of Psychology and Financial Markets, **2** (2001), 80–99.
12. G. Camera, *A Perspective on Electronic Alternatives to Traditional Currencies*, Sveriges Riksbank Economic Review, **1** (2017), 126–148. Available from: https://ssrn.com/abstract=2902721.
13. C. F. Camerer, *Behavioral game theory: Experiments in strategic interaction*, Princeton University Press, 2011.
14. G. Camera and M. Casari, *The Coordination Value of Monetary Exchange: Experimental Evidence*, American Economic Journals: Microeconomics (Forthcoming), 2013. Available from: https://ssrn.com/abstract=1463350.
15. R. Clements, *Assessing the Evolution of Cryptocurrency: Demand Factors, Latent Value and Regulatory Developments*, Michigan Business and Entrepreneurial Law Review, 2018. Available from: https://ssrn.com/abstract=3117635 or http://dx.doi.org/10.2139/ssrn.3117635.

16. U. W. Chohan, The Problems of Cryptocurrency Thefts and Exchange Shutdowns, 2018. Available from:
https://ssrn.com/abstract=3131702 or http://dx.doi.org/10.2139/ssrn.3131702.
17. R. Curran, *Why Bitcoin's bubble matters*, The Wall Street Journal, 2017. Available from:
https://www.wsj.com/articles/why-bitcoins-bubble-matters-1507515361.
18. D. Fudenberg and J. Tirole, *Game theory*, MIT Press, Cambridge, Massachusetts, 1991.
19. R. Garratt and N. Wallace, *Bitcoin 1, Bitcoin 2 ....: An experiment in privately issued outside monies*, Economic Inquiry, **56** (2018), 1887–1897.
20. P. Gillespie, *'Death spiral:' 4,000% inflation in Venezuela*, CNN, 2017. Available from:
http://money.cnn.com/2017/11/22/news/economy/venezuela-currency-crash/index.html.
21. B. Graham, *The intelligent investor: A book of practical counsel*, 1965.
22. B. Graham and B. McGowan, *The intelligent investor*, Harper Collins, 2005.
23. M. Iwamura, Y. Kitamura, T. Matsumoto, et al. *Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money*, Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money (October 25, 2014), 2014.
24. S. Jafari, T. Vo-Huu, B. Jabiyev, et al. *Cryptocurrency: A Challenge to Legal System*, 2018.
25. A. M. Kane, *An eco-friendly Ecash with recycled banknotes*, arXiv preprint arXiv:1806.05711, 2018.
26. Y. Liu and A. Tsyvinski, *Risks and Returns of Cryptocurrency* No. w24877, National Bureau of Economic Research, 2018. Available from:
https://ssrn.com/abstract=3226952 or http://dx.doi.org/10.2139/ssrn.3226952.
27. D. G. Luenberger, *Investment science*, OUP Catalogue, 2013.
28. V. Mazalov, *Mathematical game theory and applications*, John Wiley and Sons, 2014.
29. P. Milgrom and J. Roberts, *Rationalizability, learning, and equilibrium in games with strategic complementarities*, Econometrica: Journal of the Econometric Society, (1990), 1255–1277.
30. M. Okur, Ö. Çatıkkaş and P. Kaya, *Long Memory in the Volatility of Selected Cryptocurrencies: Bitcoin, Ethereum and Ripple*, Preprint, 2018.
31. D. P. Porter and V. L. Smith, *Stock market bubbles in the laboratory*, Applied mathematical finance, **1** (1994), 111–128.
32. R. Price, *Someone in 2010 bought 2 pizzas with 10,000 bitcoins - which today would be worth $100 million*, 2017. Available from:
http://www.businessinsider.com/bitcoin-pizza-10000-100-million-2017-11.
33. K. Rapoza, *Struggling nations think cryptocurrencies will save them*, Forbes, 2018. Available from:
https://www.forbes.com/sites/kenrapoza/2018/02/26/struggling-nations-think-cryptocurrencies-will-save-them/#3b4605a47da6.
34. O. Romanchenko, O. Shemetkova, V. Piatanova, et al. *Approach of Estimation of the Fair Value of Assets on a Cryptocurrency Market*, The 2018 International Conference on Digital Science (pp. 245–253), Springer, Cham, 2018.

35. V. Smith, *Bargaining and market behavior: essays in experimental economics*, Cambridge University Press, 2005.
36. V. L. Smith, G. L. Suchanek and A. W. Williams, *Bubbles, crashes, and endogenous expectations in experimental spot asset markets*, Econometrica: Journal of the Econometric Society, (1988), 1119–1151.
37. O. Schlotmann, S. Ulreich and I. Zippe, *Bitcoin: Quo Vadis? a Forecast Based on Estimated Production Costs and Investor Preferences*, 2018. Available from: `https://ssrn.com/abstract=3291543` or `http://dx.doi.org/10.2139/ssrn.3291543`.
38. G. White, *The millions of Americans without bank accounts*, The Atlantic, 2017. Available from: `https://www.theatlantic.com/business/archive/2016/10/fdic-underbanked-cfpb/504881/`.
39. D. H. Wolpert, M. Harre, E. Olbrich, et al. *Hysteresis effects of changing the parameters of noncooperative games*, Phys. Rev. E, **85** (2012), 036102.
40. K. Wu, S. Wheatley and D. Sornette, *Classification of cryptocurrency coins and tokens by the dynamics of their market capitalizations*, Roy. Soc. Open Sci., **5** (2018), 180381.
41. K. Wu, *Financial Markets in Natural Experiments, Field Experiments, Lab Experiments and Real Life*, Doctoral dissertation, ETH Zurich, 2018.

A. Appendix A: Fundamental Value and Liquidity Value

There is a temptation to stipulate that the *only* valuation of an asset is the trading price, as this price reflects the preferences and values of the buyers and sellers via the intersection of the supply and demand curves. In principle there is nothing wrong with this perspective except that important phenomena are left unexplained, and significant risks are mischaracterized as rare or low risk.

One way to examine different aspects of price or value is through the laboratory experiments such as the "bubbles" experiments introduced by [36] in which an asset pays a dividend with expectation 24 cents at the end of each of 15 periods, and is then worthless. The value of this asset at the end of Period k is clearly given in dollars by

$$P_a := 3.60 - (0.24)\,k. \tag{A.1}$$

In numerous experiments, prices often started well below P_a in $(A.1)$ and soared far above this fundamental value, and eventually crashed. This persisted even in experiments in which the dividend payout had no randomness at all [31]. It seems difficult to deny that P_a is a meaningful and useful quantity, particularly since it is a quantity that the trader can be assured of receiving. For example, purchasing at a trading price early in the experiment that is often below P_a ensures the trader will gain a specific profit. If one ignores the intrinsic value, P_a, one would conclude that the risk is the same at any price, and likely incur a large loss during the course of the experiment. Also, it has been noted [8], that in these experiments, there is a third quantity with units of price per share. This is the "liquidity value," L, defined as the ratio of the sum of all cash in the experiment divided by the total of all shares. Experiments that were designed to test this concept [10, 11] showed that the liquidity value has a primary role in determining the size of the bubble. In fact the peak of the bubble was often close to L. In other words, when traders pay little attention to fundamental value, or if the fundamental value is not clear, the price drifts toward the liquidity value [8]. At the opposite extreme, for short term government bonds, the calculation of fundamental value is clear, as the owner is assured of a particular sum at a particular time a few months in the future. The trading price generally trades very close to this fundamental value since there are many arbitrageurs who exploit any deviations.

The vast majority of cryptocurrencies do not have any redemption value, they pay no dividends, and they do not endow holders with voting power over an entity with assets (as do stocks, for example). Thus, classical finance calculations involving expected dividends, book value, replacement value, etc., all yield a fundamental value of zero. One exception is JP Morgan's JPM Coin, announced in February 2019 which would be redeemable in US dollars. The redemption price would yield the guaranteed value, which would be P_a, the fundamental value, so long as the investors are confident in JP Morgan's ability to fulfil its commitment.

Ignoring fundamental or intrinsic value often leads to disastrous practical results, as investors discovered with the internet stocks in 1999, or the Japanese market in 1990, for example, when standard calculations of stock value [21, 22] showed a large discrepancy between the trading price and the fundamental value.

Similarly, in theoretical development, neglecting either the fundamental value, P_a, or the liquidity value, L, will have the same consequencefs as overlooking any other important quantity in modeling economics problems. One obtains some results that are not consistent with observations, and has no way to rectify the situation.

Although one cannot calculate a positive P_a for the typical cryptocurrency, people are paying for these units, so that they must see some value in it. The perspective that fundamental value must be the trading price, renders the equivalence a tautology. As discussed above, a consequence of this perspective is that important phenomena are left unexplained, and an even a basic understanding of the likely price evolution becomes more difficult.

Since cryptocurrencies have no fundamental value, prices will naturally drift toward the liquidity value, which will be given by the total amount of cash available for the cryptocurrency (i.e., demand) divided by the number of units [10, 11].

The absence of a non-zero fundamental value means that price will be set by the supply (which is fixed, for example, for Bitcoin) and demand in accordance with equation (1.1). Thus it is a calculation of demand that is key to understanding equilibrium price.

B. Appendix B: The roles of speculators and market-makers

1. We consider first the role of "pure" speculators who have no control of the type of trading or auction, the rules of the exchange, the enforcement of the rules, the display of orders, and the flow of information. Volatility arises endogenously due to the various trading strategies, such as trend following, and random events that motivate any of the traders. For many first time or novice traders, there is a tendency to overreact, chase a trend, or hop onto a fad. In the case of cryptocurrencies, which lack any fundamental value, any news is likely to result in an overreaction. Thus volatility can be expected to be high in the absence of any anchor. For example, Treasury bills offer a guaranteed payout, so that a small deviation from the certain payout due within a few months would be exploited by arbitrageurs and the price would be restored close to its intrinsic value. The speculators in many markets have a better understanding (compared to novice traders) of the factors that move prices within

a short time scale. Speculators are generally believed to lower volatility [6], as they use their capital to buy when prices move unjustifyably lower. Of course, when prices exhibit very low volatility, there is no financial incentive for speculators to trade. Consequently, in an idealized setting, the short-term volatility level will be established as the minimum value at which speculators find adequate profits after costs.

2. Next we consider "speculators" in less established markets in which the rule makers, market makers, news makers are all essentially the same group. In most developed markets such as the New York Stock Exchange (NYSE) and major commodity exchanges there are precise rules designed to promote fairness and ease of trading that have been developed over many years. An example is the NYSE rule that if there are two orders to purchase a stock, it is the higher one that prevails. Surprisingly to novice traders, this is not usually a feature of most markets. In many markets there are "market makers" who are entitled to buy the stock for their own account at a lower price, even though a higher bid has been placed by a retail customer or trader. The rules of each exchange endow the market makers and market specialists with the power to buy and sell on their own account. In many well-developed exchanges, there are rules agains "front-running" whereby insiders buy on their own accounts as they become aware of a set of large orders that are entering the market. Another example on major exchanges involves "not held" trades that are placed with the market makers but are not displayed. The intention here is that a large order to sell could prompt further selling by less informed traders. By contrast, in a less developed market environment, a market insider can place a large order (but above the market price) that will immediately lead to lower prices, whereupon he can deftly purchase.

Novice traders usually make numerous assumptions relating to fairness on the nature of market rules and procedures. Unfortunately, these are generally false for less developed markets that cater to inexperienced traders. The wishful thinking of new traders seeking quick riches (or escape from a currency) provides for a healthy income for those dominating these markets in terms of making the rules (if there are any at all) and using their capital to control the volatility. For many of the cryptocurrencies, for example, it is not even clear what the rules are, or where they would be enforced. Thus, in an under-developed market, a group of participants that controls the rules of trading has numerous tools at its disposal to adjust volatility. Even the hours of trading have a strong impact on volatility. For example, it is well-known that trading around the clock leads to times periods of low volume so that a few trades can move prices much more than during actively traded times. On the other hand, in an exchange in which there is a single trade each day at a specified time, the maximum minus minimum price within one week is likely to be much lower than in 24 hour trading.

3. Another feature that can influence prices is the extent to which information on orders is displayed. The "order book" displays the array of bids and asks for the asset in continuous time. Whether or not the order book is displayed depends upon the rules of the exchange. Also, on some exchanges, the market maker can choose to display only some of the orders. In laboratory experiments [11] it was shown that bubbles are tempered by the display of the complete order book.

Related to the order book are the rules under which the market maker can buy for his own account. While "front running" – the practice of buying for one's own account ahead of a large order – or "shadowing" – buying the same assets as a particular trader – are banned in some of the most developed exchanges, one cannot assume that they will be prohibited universally.

Of course, all of this assumes that there is a real market in which bids and asks are matched with some rule. In many cases purchases and sales are made through one entity that buys and sells for its own account, thereby granting itself a generous profit as the middleman. Even in large brokerages it is common for monthly statements to disclose "we make a market in this stock" that indicates the bid/ask spread is whatever the company designates as revenue for itself. From the perspective of the individual trader, the bid/ask spread, of course, adds to the cost and volatility of the transaction.

C. Appendix C

In examining the choice faced by $\mathcal{W}$ we assume that one option is to remain in the home currency, F, and the other to buy the cryptocurrency with the objective of later selling in order to buy other assets such as a more reliable currency, gold, etc.

The group $\mathcal{W}$ experiences a loss or gain on these transactions with the speculators, group $\mathcal{S}$, which itself has a non-linear utility function reflecting that fact that high volatility is good for profits up to a point after which it has a negative impact. Thus, one has the following utility function for group $\mathcal{S}$:

$$U_S = a_1 V - a_2 V^2$$

where V represents the volatility or variance, for example, and a_1, a_2 are positive constants. Hence, there will be a maximum value $V = V_m$ that maximizes the utility of the speculators. This can be viewed as a fixed quantity from the perspective of $\mathcal{W}$.

The mean, m_Y, and variance, σ_Y^2 of group $\mathcal{W}$'s investments in Y can be calculated based on V_m and the other parameters that describe the trading. In particular, we assume that there is a probability q (presumably small) that $\mathcal{W}$ will profit, and that their wealth will increase from 1 to $1 + r_1 V_m$ and a probability $1 - q$ that it will decrease from 1 to $1 - r_2 V_m$ where $r_2 > r_1 > 0$. In other words, there is a small probabilty, q, that $\mathcal{W}$ will benefit by $r_1 V_m$ (as a fraction of their original wealth) and a larger probability, $1 - q$, that they will lose a larger sum $r_2 V_m$. The loss is proportional to the volatility as the professional speculators are able to exploit the ups and downs of the trading at the expense of the inexperienced $\mathcal{W}$.

The mean and variance of the outcome are then

$$\begin{aligned} m_Y &= q\,(1 + r_1 V_m) + (1 - q)\,(1 - r_2 V_m)\,, \\ \sigma_Y^2 &= q\,(1 - q)\,(r_1 + r_2)\,V_m. \end{aligned}$$

In other words, there is large probability that $\mathcal{W}$ will take a loss on the transaction. One can consider more general probability distributions for $\mathcal{W}$'s profits and losses, but ultimately, the two quantities that are relevant for its utility function U_W are given by m_Y and σ_Y^2 that one can regard as empirical observables.

AIMS Press