Technical Report STR 2022-1 • Oct. 2022

SAPIENCE •ORG
Thinktank for disruptive and intelligent computing

On the Utility Value of Currencies

Amnon H. Eden, Yaron Katzir
Sapience.org

Categories: Computational finance, thermodynamics, computer science

Keywords: Entropy, Bitcoin, abstract machines, utility value

Abstract

Notions of value of currencies such as Bitcoin and the US Dollar presuppose that the exact value of each coin equals its exchange rate or price at each point in time, ie, the price of one coin is only ever defined in terms of another. Alternative notions of value are also defined in relative terms (e.g., the price of gold, or 'purchasing value'). Consequently, financial analyses focus on questions about the future: will price go up or down? We rarely agree on the answer to, What is the actual value of Bitcoin? Or ask, inter alia, What is the actual value of the US Dollar?

This paper examines an alternative understanding based on the assumption that currencies have *utility values*: at each point in time, the utility value of a currency is a physical, absolute, independent property, which can be measured just like the temperature and entropy of a gas. We define an abstract machine which models the currency's wallets and the movement of coins between them, and postulate that utility values can be computed from the currency's abstract machine, using data about the currency itself and nothing else. Figuratively speaking, utility values define 'price' without prices.

In support of this theory we use entropy and entropy-like functions to estimate the utility values of three currencies: Bitcoin, Ethereum, and Cardano. We also show that, not only do our price estimates correlate closely with market caps (94% correlation), but the utility values obtained also closely approximate ($\Delta = 0.23$) the spot exchange rates between these currencies as recorded by trading platforms for each day in between mid-2018 and mid-2022. Figuratively speaking, we calculate the prices of these coins without prices.

Sapience.org is a thinktank dedicated to the study of disruptive and intelligent computing. Its charter is to identify, extrapolate, and anticipate disruptive, long-lasting, and possibly unintended consequences of progressively intelligent computation on economy and society; and to syndicate focus reports and mitigation strategies.

1. Introduction

All things are numbers
-- Pythagoras

The price of Bitcoin, which rose from a fraction of a penny to over USD50K, raises fundamental questions about the value of currencies. For example, we know the price of Bitcoin at every point in time, but Is Bitcoin undervalued or overvalued? What is Bitcoin's actual value? And, inter alia, what is the actual value of a US dollar?

Existing financial theories of currencies take the value of a coin to mean its latest price, i.e., its exchange rate with relation to another currency. For example, in Sep 2022 one USD is valued as 0.87 British Pounds. Similarly, based on Bitcoins exchange rate we say that the currency's market cap is about USD0.5B. Others estimate each coin's 'purchasing power' relative to its historic value, for example by defining what 100 USD could buy in 1950. Value can also be attached relative to a specific set of essential commodities, for example by measuring the expenses of the median family.

Alternatively we could measure value using the notion of 'gold standard'. It is based on the observation that the value of gold has remained stable while currencies have undergone inflation, and occasionally deflation. However, any notion of value based on "equals to x grams of gold" is founded on the scarcity of gold. Scarcity which may one day diminish significantly, as the history of the value of aluminium has taught us (Diamandis 2021). Consider also the following thought experiments: What if one day, all the gold in the world has vanished? What if cheap means of producing gold are found? Will currencies instantly lose all their value? Precious metals do not offer us a scientific yardstick for the value of coins.

What of inter-currency exchange rates? Spot exchange rates merely reflect the supply/demand conditions. Those can be very volatile, as crypto markets show. Clearly the daily, weekly, and even monthly fluctuations offer no satisfactory, objective notion of value. Besides, seeing as no currency is itself founded on a scientific notion of value, spot exchange rates do not solve our problem.

Consequently, analysts focus on trends, asking: "Will the price of Bitcoin go up or down?", and "Will the GBP weaken or strengthen as a result of Brexit/The War on Ukraine? However, questions about future prices are notoriously complex and can rarely be answered with any confidence.

Thus, the questions "What is the actual value of Bitcoin?" or, inter alia, "What is the real value of the GBP?" seem meaningless to ask outside context. In con-

clusion, currencies are assumed to have no inherent, scientifically measurable, absolute notion of value.

We present an alternative understanding of the notion of the value of a currency, which can be summarised as follows:

1. At any point in time, each currency has a *utility value*, a number which can be measured from the currency itself, and which depends exclusively on the coins and wallets in the same currency and nothing else.
2. The ratio between the utility values of two coins closely approximates their actual exchange rates as recorded by the market.
3. Currencies can be represented as abstract machines which process transactions.
4. The utility value of currencies can be calculated from their representation as abstract machine. Crucially, the calculation does not involve price history.
5. Utility values can be approximated closely by entropy functions, polynomials, and statistical functions which measure the distribution of coins among the wallets.

In other words, each currency has a *utility value*, a physical property that can be measured just like the temperature and pressure of a gas are measured: values that are absolute and independent of the observer or measuring devices. If an alien visited earth, they would reach the same results simply by observing the currency. Unlike price predictions, utility values are calculated without any price history whatsoever. In other words, while each day the spot price of one Bitcoin is determined by a drop/rise relative to yesterday's price, we estimate each day's exchange rate, or *utility ratio*, without any such information.

Our analysis shows that, at least for three cryptocurrencies, that a notion of a utility value of a currency can be precisely defined such that the exchange rates between these currencies can be approximated with relative accuracy ($\Delta = 0.23$) using mathematical functions over coins and their distribution among wallets. We also show that utility values, and the respective exchange rates can be calculated from these numbers which are publically (and freely) available.

What if utility values exist? What if they can be precisely determined? For one, questions such as "is Bitcoin under/overvalued right now" can be answered with relative confidence. Crucially, the answers do *not* require us to predict the future, which remains uncertain as ever. We know if Bitcoin's price reflects its true value *right now* because utility values make no assumptions about the future. Similar questions can also be asked and answered not only about cryptocurrencies but also about the US dollar, Euro, British Pound, and every other currency, and answered conclusively.

Information about utility values may also have implications for monetary policy. For example, the Federal Reserve could calculate exactly how printing x dollars will affect the utility value of the US dollar in precise terms.

Another significant insight arises from utility functions that are based on entropy measures such as those analysed below, which is: The closer the currency is to a uniform distribution, the higher is its utility value. In other words, as coins are distributed more evenly, their exchange rates go up, and vice versa. A variety of other consequences can be conjured at this point. Those remain outside the scope of this paper.

Open questions

This paper does not purport to resolve fundamental questions about utility values and many questions remain open, such as: Do utility values even exist, and if so, can they be calculated accurately? What are the utility values of the US dollar? Of the British Pound? Do they yield close approximations to the exchange rates between traditional currencies? What is the relation between entropy, energy, and currencies? How does "printing money" affect the utility value exactly? How is the (un-/usable) heat generated by such work measured? Is it related to fees and/or latency? What can be learned from applying the law of conservation of information to currencies? How does the entropy of currencies evolve with time? What are the computational properties of a currency?

We hope that these questions will be examined and answered in the future.

2. Currencies

We introduce the following notation which couches our discussion in currencies and market prices in accurate terms.

C, C_1, C_2	Currencies	Eg: USD, EUR, GBP, BTC, ETH

We restrict our discussion in "pure" currencies: money that has no inherent value other as a means of trade. For example, gold is not a currency for our purposes.

$¢, ¢_1, ¢_2$	Coins	Eg: \$1.00, €1.00, £1.00, 1₿, 1Ξ

The native unit of a currency. We distinguish between the native unit ('coin') vs. the smallest unit ('atom').

a, a_1, a_2	Atoms	Eg: \$0.01, €0.01, 1 satoshi (bitcoin), 1 wei (Ethereum)

Atoms are the smallest (indivisible) unit of a currency. For example, the smallest unit of the US Dollar is the cent, defined as 1/100 of the dollar. For example, the satoshi is the smallest unit of Bitcoin, defined as $1/10^8$ of the native unit.

$\#¢, \#¢_1, \#¢_2$	Number of coins in circulation	Eg, in 2022, $\#USD$ is about 5.5 trillion, $\#GBP$ is about 4.7 billion, and $\#₿$ about 19 million
$\#a, \#a_1, \#a_2$	Number of atoms in circulation	Eg, the number of atoms in the US dollar is 100x the number of dollars in circulation.
$\#w, \#w_1, \#w_2$	Number of wallets	Eg, in 24 May 2022, there were about 35M non-empty ([1]) wallets on the Bitcoin blockchain and 48M on Ethereum.
$(C_1 \div C_2)_t$	Spot exchange rate from the first currency to the second at time t	Eg: The price of one bitcoin in USD on the last day of 2021 is written: $(BTC \div USD)_{31Dec2021} = 46{,}355$

Wallets represent locations where money is stored. With Bitcoin, a wallet maps to the set of addresses on the same elliptic curve, normally associated with one user. With traditional currencies, a wallet could be realised as a bank account, a pocket, a safe, or other means of storing money.

The exchange rate notation represents the de-facto exchange rate between two currencies at point in time t. For example, at the end of the last day of 2022 one Bitcoin was recorded as equivalent to 46,355 US Dollars.

([1]) To remove noise we restrict our attention to wallets with non-negligible balance.

The market cap of one currency is defined by the product of the total number of coins and the coin's exchange rate with another coin (say, US dollar), i.e.

$$MarketCap(C_1, C_2)_t = \#¢_t \cdot (C_1 \div C_2)_t$$

Where $\#¢_t$ is the number of coins in circulation of currency C_1 at time t. For example, the market cap of Bitcoin in USD was about 876B on 31 Dec 2021.

This notation demonstrates what market caps are not: an absolute measure of value. For example, if the market cap of Bitcoin has grown when measured in US dollars does not necessarily imply that Bitcoin's value has grown during that time, given that the US dollar is regularly devalued by inflation. Utility values are hypothesized to provide an absolute notion of value.

To conclude the description we also account for the changes in a given currency over time: C_t denotes a pure currency C at any given point in time $t = 0,1,2 \ldots \tau$, such that C_0 represents the currency on its first launch and C_{t+1} represents the outcome of the transactions that were completed between t and $t + 1$. On occasion the parameter t may be implied such that C represents the currency at a specific point in time.

3. Information

What we mean by information is a difference which makes a difference
(Bateson 1972)

What is money? "There are £20.00 in my pocket, £126.42 in my bank account, and £2,000 in my safe." Whether I have four five-pound bills or one bill of twenty pounds in my pocket makes no difference. Whether the bank records my balance is written on a paper ledger or a blockchain is irrelevant. When it regards to money all that matters is, how much? Whether represented as physical coins, as a bank balance, or as an address on the blockchain, whether in one denomination or another, money is a sum total, a value, a number, nothing else. In other words, money is information.

So what is information? A deeper philosophical investigation invites this question. Hinting upon the answer, Norman Wiener is quoted as saying,

> *"Information [is] a name for the content of what is exchanged with the outer world as we adjust to it, and make our adjustment felt upon it."*
> *(Wiener 1954)*

This description explains well our understanding of money.

Deeper questions into the precise ontological nature of information — its *metaphysics* if you insist on asking *what* — receive wildly different answers from different physicists, mathematicians, and computer scientists at different points in time (Floridi 2004). It appears that the precise ontological status of information is as contested as the question how to measure information. Quoting the same brilliant mathematician, the answer requires rethinking scientific metaphysics:

> *"Information is information, not matter or energy. No materialism which does not admit this can survive at the present day" (Wiener 1961)*

Considering each currency as a whole, the British pound for example is a set of coins of a known total size (about 94 billion in 2022). Some coins were minted in specific denominations (mostly £10 and £20), some coins were issued digitally by the Bank of England. Some coins are held in pockets, some in banks, some in the dungeons of Sheol, and some have remained with the Bank of England. At each point in time, the British pound can therefore be thought of as a set of wallets, each with a given balance. Transactions are simply movements of coins between wallets: when Jones pays Smith x GBP, the balance in Jones' wallet shrinks by x GBP and grows in Smith's wallet by x GBP. The effect of each transaction is fully represented by the new balance of the wallets involved. More abstractly, each transaction is 'computed' by the currency, and represented mathematically as the transition from one set of wallets and balances (the currency before the transaction) to another (the currency after the transaction).

To summarise, everything there is to know about money: where it is stored, how much of it is there at each point, which value each coin and bill represent, and how much of it moves from one wallet to another, can be fully understood in terms of information storage and processing.

In the same vein we may describe currencies using abstract machines from automata theory in theoretical computer science. A currency can be thought of as a computer or an abstract machine — an *automaton* (Sipser 1997) — processing transactions and calculating balance in each wallet. While such radical simplification may seem removed from the role of money in society, we show below that this abstraction is sufficient for the purpose of our analysis.

We define the notation and vocabulary that shall be used formulating our abstract machine, starting from the notions of wallets and transactions. Since all wallets have an identity (i.e., each wallet is only equal to itself), we use an unbounded set of unique symbols from which new wallets can be drawn.

Definition. A wallet w is an element drawn from an unbounded set of unique symbols. Every wallet is associated with a natural number $\underline{w}$ called the balance of w. A transaction x is a triplet $x = \langle |x|, w_{out}, w_{in} \rangle$ such that $|x| \in Z^+$ (natural number or zero); w_{out} and w_{in} are wallets.

4. Computation

Every physical system registers information, and just by evolving in time, by doing its thing, it changes that information, transforms that information, or, if you like, processes that information.
-- Seth Lloyd

This section lays out the notation underlying our analysis and describes how currencies can be modelled as automata. The purpose of this automaton is to mathematically define the evolution process of currencies, day by day, transaction by transaction.

Abstract machines, such as *finite automata* and *push-down automata* (Sipser 1997), are mathematical models of computation. Each automaton defines a set of possible states, an alphabet of possible inputs, and a transition function which maps the input and a 'current' state to another state. Computational processes are thus defined in terms of transitions between the states of the machine according to its input. We use this formal vocabulary to model currencies as automata that pro. The states in our model are abstractions of currencies, representing the wallets and their balances, and provide a snapshot of the currency at a particular point in time.

Definition. A state is a pair of sets $S = \langle \mathcal{W}, \overline{\mathcal{W}} \rangle$ each of a given finite size $\#w$ such that $\mathcal{W}$ is a set of wallets and $\overline{\mathcal{W}}$ is the set of their respective balances, written

$$\mathcal{W} = \{w_1, \dots w_{\#w}\}$$
$$\overline{\mathcal{W}} = \{\overline{w_1}, \dots \overline{w_{\#w}}\}$$

The null state is designated $s_0 = \langle \phi, \phi \rangle$, where ϕ stands for the empty set. We also denote $\#a$ the sum of balances, also referred to as atoms in circulation, ie

$$\#a = \sum_{i=1}^{\#w} \overline{w_i}$$

Definition. An automaton $\mathcal{A}$ is a triple $\mathcal{A} = \langle \mathcal{S}, \Sigma, \delta \rangle$ where $\mathcal{S}$ is the set of possible states, Σ is the input alphabet which consists of possible transactions, and δ is a transition function mapping states and input to states, ie

$$\delta : \mathcal{S} \times \Sigma \longrightarrow \mathcal{S}$$

The transition function δ is defined as follows. Given state $S = \langle \mathcal{W}_1, \overline{\mathcal{W}_1} \rangle$ and an input transaction $x = \langle \overline{x}, w_{out}, w_{in} \rangle$ such that $w_{out}, w_{in} \in \mathcal{W}_1$ and $\overline{x} < \overline{w_{out}}$, then the state resulting from $\delta(S_1, x)$ is $\langle \mathcal{W}_1, \overline{\mathcal{W}_2} \rangle$ such that

$$\overline{\mathcal{W}_2} = \{\overline{w_1}, \ldots (\overline{w_{out}} - \overline{x}), \ldots (\overline{w_{in}} + \overline{x}), \ldots \overline{w_{\#w}}\}$$

We further extend our notions of transactions and transition function to account for cases of special interest for currencies.

Definition. Given state $s = \langle \mathcal{W}_1, \overline{\mathcal{W}_1} \rangle$ and an input transaction $x = \langle \overline{x}, w_{out}, w_{in} \rangle$, we define the resulting state $\delta(S, x) = \langle \mathcal{W}_2, \overline{\mathcal{W}_2} \rangle$ such that:

- $w_{in} \notin \mathcal{W}$ (w_{in} is a new symbol) is said to add a wallet and

$$\mathcal{W}_2 = \mathcal{W}_1 \cup \{w_{in}\}$$
$$\overline{\mathcal{W}_2} = \{\overline{w_1}, \ldots \overline{w_{out}} - \overline{x}, \ldots \overline{w_{\#w}}\} \cup \{\overline{w_{in}} = \overline{x}\}$$

- $\overline{x} = \overline{w_{out}}$ is said to remove a wallet, and

$$\mathcal{W}_2 = \mathcal{W}_1 \setminus \{w_{out}\}$$
$$\overline{\mathcal{W}_2} = \{\overline{w_1}, \ldots \overline{w_{in}} + \overline{x}, \ldots, \overline{w_{\#w}}\} \setminus \{\overline{w_{out}}\}$$

The transitions defined hitherto preserved the total number of atoms in circulation. In reality however coins can be added to circulation, for instance when new dollar bills are printed by the Federal Research and when cryptocoins such as Bitcoin are mined. Similarly, torn bills are removed from circulation by the Federal Reserve and on occasion Ether coins are burned. We extend our transition function to account for these as follows.

Definition. Given state $S = \langle \mathcal{W}_1, \overline{\mathcal{W}_1} \rangle$ and an input transaction $x = \langle \overline{x}, w_{out}, w_{in} \rangle$, we define the resulting state $\delta(S, x) = \langle \mathcal{W}_2, \overline{\mathcal{W}_2} \rangle$ such that:

- $w_{out} = \phi$ is called inflationary and

$$\mathcal{W}_2 = \mathcal{W}_1$$
$$\overline{\mathcal{W}_2} = \{\overline{w_1}, \ldots \overline{w_{in}} + \overline{x}, \ldots \overline{w_{\#w}}\}$$

- $w_{in} = \phi$ is called deflationary and

$$\mathcal{W}_2 = \mathcal{W}_1 \setminus \{w_{out}\}$$
$$\overline{\mathcal{W}_2} = \overline{\mathcal{W}_1} \setminus \{\overline{w_{out}}\}$$

This automaton operates by processing, at each step, state S_1 and transaction x, yielding that state S_2 such that $\delta(S_1, x) = S_2$. This step is written

$$S_1 \circ x \rightarrowtail S_2$$

We extend this notation with a sequence of transactions $X = \{x_1, \ldots x_n\}$ and represent the state resulting from processing them in sequence, ie

$$S \circ X \stackrel{\text{def}}{=} \big((S \circ x_1) \circ x_2\big) \ldots \circ x_n$$

This automaton has several obvious properties.

Lemma.
1. The balance in all wallets is always positive.
2. The number of possible states and the size of the alphabet (possible transactions) are not finite. Our automaton is therefore not finite.
3. Given any pair of states S_1, S_2, possibly including the null state, there exists a non-finite number of sequences of transactions X such that $S_1 \circ X \rightarrowtail S_2$.

The proof is elementary. ■

5. Utility Values

Having furnished a precise vocabulary of currencies and their abstractions, we may introduce the central assumptions about their relation.

Utility Hypothesis. At each point in time t, every pure currency C_t has a utility value, written $\mathcal{U}(C)$, a positive rational number whose value is determined exclusively from the currency itself, eg its wallets, balances, coins and their movements, independently from other currencies and parameters outside the currency. ([2])

The first hypothesis states that utility values are calculated from information exclusively about the currency itself, ie, its wallets and coins, nothing else. In other words, at each point in time, the utility value of a coin is calculated irrespective to exchange rates and other currencies, supply/demand figures, GDP, national deficit, economic infrastructure, trade volume, technological breakthroughs, and any other economic metric. While such external metrics determine at each point in time, the *momentary price* of a coin, as well as indirectly affect those numbers from which utility values are calculated (i.e., wallets and coins), they are not partake in the calculation. Figuratively speaking, utility values can be said to determine the 'price' of a coin without its price.

This hypothesis does not determine how utility values are calculated. Below we consider a range of candidate possible functions, and use them to assess the strength of this hypothesis. As there are no other known physical metrics of value, we measure the correlation between the utility values and market caps.

The next hypothesis however furnishes us with much more precise means of empirical testing: by comparing the prediction made by utility values to exchange rates. To define it we introduce the notion of utility ratio.

Definition. Given currency C with coin ¢ (native unit), #¢ number of coins, and utility value $\mathcal{U}(C)$, we define the utility value per coin, written $\mathcal{U}(¢)$, as

$$\mathcal{U}(¢) \stackrel{\text{def}}{=} \frac{\mathcal{U}(C)}{\#¢}$$

[2] The notation $\mathcal{U}(C)$ is used as a shorthand for $\mathcal{U}(C_t)$. On occasion the indication for time point is implicit and subscript omitted for clarity.

Definition. Given two currencies C_1, C_2 we define the utility value per coin ratio, or utility ratio, written $\mathcal{U}(C_1) \doteqdot \mathcal{U}(C_2)$, as the ratio between the Shin values per coins. That is, for $¢_1, ¢_2$ the coins of C_1, C_2 respectively,

$$\mathcal{U}(C_1) \doteqdot \mathcal{U}(C_2) \stackrel{\text{def}}{=} \frac{\mathcal{U}(¢_1)}{\mathcal{U}(¢_2)}$$

Utility Ratio Hypothesis. Given a every pair of pure currencies C_1, C_2 and distance function Δ, the difference between the utility ratios and the pair of currency's exchange rate at each point in time is at most $\Delta(C_1, C_2)$, ie

$$(C_1 \doteqdot C_2) \approx_\Delta \mathcal{U}(C_1) \doteqdot \mathcal{U}(C_2)$$

Put simply, the second hypothesis postulates that utility values can estimate the actual exchange rates. The distance function $\Delta(C_1, C_2)$ measures the expected discrepancy between the exchange rate and the prediction made by the utility ratios. In the experiments described below we measure distance simply as the average gap between the exchange rates and the utility ratios we calculated. Our preliminary results show that this gap shrinks as the currency 'grows' in the number of wallets, suggesting that as a currency grows in size its price converges to that which is predicted by its utility value. A more appropriate distance function might therefore be monotonous in the number of wallets of the smaller currency.

The next definition allows us to reason about currencies using abstract machines.

Definition. Given a point in time t and a pure currency C_t, the abstract computation of C_t is the pair $\langle S, X \rangle$, where $S = \langle \mathcal{W}, \overline{\mathcal{W}} \rangle$ is a state such that $\mathcal{W}$ and $\overline{\mathcal{W}}$ represent the sets of wallets in C_t and their balances respectively, X is the set of the transactions conducted in C until time t, $\mathcal{s}_0$ is the null state, and

$$\mathcal{s}_0 \circ X \rightarrowtail S$$

That there exists an abstract computation of every pure currency follows directly from the formulation of pure currencies in §2 and the Lemma in §4. The mapping between abstract and concrete transactions and wallets is obvious. The remainder of the proof is obtained by inductive construction of the transactions and states of the currency at time $\tau = 0, 1, 2, \ldots t$ such that X_τ stands for the set of transactions between τ and $\tau + 1$ and state S_τ results from the sequence of transitions $s_0 \circ X_0 \circ \ldots \circ X_\tau \rightarrowtail S_\tau$. ■

Our last and final hypothesis articulates the assumption that currencies are not only modelled as automata but also they are, in essence, precisely that. As articulated eloquently by Seth Lloyd:

> *Every physical system registers information, and just by evolving in time, by doing its thing, it changes that information, transforms that information, or, if you like, processes that information. [Seth Lloyd]*

Abstract Computation Hypothesis. The utility value of a currency can be calculated from its abstract computation.

The third hypothesis equates concrete currencies with the automata we defined. It postulates that the simplified computational model of currencies, whose operation computes transactions and balances, is sufficient to account for utility values. In comparison with the first hypothesis, the third one narrows down further the information necessary to calculate utility values.

Below we demonstrate that good approximations can be obtained with even less than a complete account of the currency.

6. Shin Functions

The signal is the truth. The noise is what distracts us from the truth.
-- Nate Silver

How can utility values be calculated? Below we describe some of the functions we used to test our hypotheses in search for utility values. We use the term *Shin functions* ([3]) to denote our candidates for the utility function, candidates which per the third hypothesis are mathematical functions from the elements in the abstract computation of pure currencies — wallets, balances, and transactions — to the positive rationals.

If "money is information" and pure currencies are abstract machines then it is only natural to expect entropy functions to be the first Shin functions to test.

The term entropy was originally introduced to classical thermodynamics by Rudolf Clausius. Since then the term has evolved to describe different measures of information, order and chaos, dissipative and usable energy etc. in different fields of study, in particular information theory, algorithmic complexity, dynamic systems, and quantum mechanics. Today, the term entropy carries a different

([3]) 'Shin' originates for the Semitic word for value, *shovi*, whose first letter is the Aramaic Shin, written ש

meaning depending on how much information is available and how much of it is unknown. Below we consider two definitions which served our purposes most. In the next section we describe the results of testing the predictions made by the entropy functions defined below, as well as several variations of them. Other Shin functions tested were based on statistical measures such as variance.

Boltzmann's Entropy

The first Shin function we consider is based on the definition of entropy offered by Ludwig Boltzmann, who used it to measure the amount of information required to describe the macrostate of a system with a set number of possible microstates W with the following formula ([4]):

$$H_{Bol} = log\, W$$

Borrowing this notion of entropy leads us to measure how much information is stored in the abstract computation of a currency. More precisely, the number of bits of information necessary to give a full account of the currency which the abstract machine represents.

A most simple interpretation was found to be useful and simple to calculate: one which ignores transactions entirely. Instead, it only measures the number of bits in representing the balances of the wallets, which for each individual wallet w_i is $log\, w_i$, yielding

$$Boltzmann(C) = \sum_{i=1}^{\#w} log\, \overline{w_i}$$

Shannon's entropy

Claud Shannon introduced a different measure of information. His definition of entropy (Shannon 1948) is based on amount of surprise from the occurrence of an event, specifically: given p the probability of a certain event, $\log p$ represents the amount of surprise. In other words, the less likely an event is, the more information its occurrence provides. Shannon's entropy uses Gibb's formula to measure the amount of information in such an occurrence, ie

$$H_{Sha} = -p \cdot log\, p$$

([4]) Boltzmann's tombstone famously bears the inscription of this formula.

Thus the entropy or the total amount of information in the occurrence of $\#w$ 'events' is

$$Shannon(C) = \sum_{i=1}^{\#w} p_i \cdot log\, p_i$$

There are different ways of measuring the information in an abstract machine. Here, again, we have not found transactions to contribute significantly to the notion of utility value. In the version which proved useful, the number of wallets $\#w$ and coins $\#¢$ are known ahead, and the probability of each wallet of having a given balance is calculated iteratively, such that with the balance of each additional wallet decreases the range of possible balances of the remaining wallets. We do so by ordering the wallets in the currency by their balance such that $\overline{w_1} > \overline{w_2} > \cdots > \overline{w_{\#w}}$. By this calculation, the probability of the first wallet is

$$p_1 = \frac{\#¢ - \overline{w_1}}{\#¢}$$

and of each wallet thereafter is

$$\left\{ p_i = \frac{\overline{w_{i-1}} - \overline{w_i}}{\overline{w_{i-1}}} \right\}_{i=2}^{\#w}$$

7. Preliminary results

Reporter: What would you do if the measurements of bending starlight at the 1919 eclipse contradicted his general theory of relativity?

Einstein: Then I would feel sorry for the good Lord. The theory is correct.

Here we provide preliminary empirical results in support of our hypotheses. Data was analysed for three cryptocurrencies: Bitcoin (BTC), Ethereum (ETH), and Cardano (ADA), for the period between 1 July 2018 and 24 June 2022. We show the results obtained using data downloaded from coinmetrics.io and analysed using KNIME 4.5.2. Correlation was measured using Spearman's Rho (Spearman 1904).

The following tables include the results of four comparisons:

1. The utility ratios between the pair Bitcoin/Ethereum vs. their exchange rate (average error ratio and correlation)
2. The utility ratios between the pair Bitcoin/Cardano vs. their exchange rate (average error ratio and correlation)

3. Bitcoin's utility values vs. its market cap in USD (correlation only)
4. Ethereum's utility values vs. its market cap in USD (correlation only)

Our experiments were conducted with rudimentary means of data collection and analysis. Further analysis is required of finer resolution of data and of other currencies, past and current.

The candidate utility functions tested include the entropy measures defined above, as well as several variations thereof with other common metrics. For example, SER stands for Supply Equality Ration, a metric defined by

$$SER(C) = \frac{\sum_{w_i < \#\text{¢} \cdot 10^{-7}} (\overline{w_i})}{\sum_{w_i \in \lceil W \rceil 0.01} (\overline{w_i})}$$

where the enumerator stands for the total sum of wallets whose balance is less than ten millionth of the coins in circulation, and the denominator stands for the total sum of the top 1% of wallets ([5]).

Another metric used is A_{nd} which stands for the number of wallets that have conducted a transaction in the last n days. A smoothing function we used is single exponential smoothing of a metric M and M_n stands for the value of the metric M on the $n-$th day, such that SE180 stands for $SE_{180}^{180}(M)$, defined recursively:

$$SE_n^k(M) = \begin{cases} M_0, & n = 0 \\ \frac{2}{k+1} \times M_n \ + \ (1 - \frac{2}{k+1}) \times SE_{n-1}^k(M), & n > 0 \end{cases}$$

Last candidate function uses a measure of the statistical variance between the balances, ie

$$VAR(\mathcal{W}) = \frac{\sum_{w_i \in \mathcal{W}} (\overline{w_i} - \mu)^2}{\#w}$$

where μ stands for the mean balance.

[5]() https://coverage.coinmetrics.io/asset-metrics/SER

Shin(BTC//ETH) st. Boltzmann(C)=Avg(BolMin,BolMed)	0.701
Shin(BTC//ETH) st. Shannon(C)=-Sum(p*logp), p_i←1 - m_i/m_i-1, m←med	0.699
Shin(BTC//ETH) st. Shin(C)=Shannon * SER	0.354
Shin(BTC//ETH) st. Shin(C)=Bol-Avg / ((SE180(A30d) + SE180(A7d))/#¢)	0.246
Shin(BTC//ETH) st. Shin(C)=Boltzmann / lg#a, a←in wallets	0.493
Shin(BTC//ETH) st. Shin(C)=#w/lg(VAR)	0.524

Table 1. Average ratio of error between spot exchange rates of the pair BTC/ETH and the utility ratios of the two coins as calculated by six different Shin functions (KNIME)

Shin(BTC//ETH) st. Boltzmann(C)=Avg(BolMin,BolMed)	79.55%
Shin(BTC//ETH) st. Shannon(C)=-Sum(p*logp), p_i←1 - m_i/m_i-1, m←med	82.53%
Shin(BTC//ETH) st. Shin(C)=Shannon * SER	87.49%
Shin(BTC//ETH) st. Shin(C)=Bol-Avg / ((SE180(A30d) + SE180(A7d))/#¢)	72.62%
Shin(BTC//ETH) st. Shin(C)=Boltzmann / lg#a, a←in wallets	79.53%
Shin(BTC//ETH) st. Shin(C)=#w/lg(VAR)	80.32%

Table 2. Spearman correlation between spot exchange rates of the pair BTC/ETH and the utility ratios of the two as calculated by six different Shin functions (KNIME)

Table 3. Spot exchange rates of the pair BTC/ETH and the utility ratios of the two coins as calculated by two Shannon-based Shin functions (KNIME)

Table 4. Spot exchange rates of the pair BTC/ETH and the utility ratios of the two coins as calculated by three Boltzmann-based Shin functions (KNIME)

Estimating BTC/ADA Exchange Rate

Shin(BTC//ADA) st. Boltzmann(C)=Avg(BolMin,BolMed)	0.502
Shin(BTC//ADA) st. Shannon(C)=-Sum(p*logp), p_i←1...	0.393
Shin(BTC//ADA) st. Shin(C)=Shannon * SER	5.929
Shin(BTC//ADA) st. Shin(C)=Boltzmann / (A90d/#¢)	2.029
Shin(BTC//ADA) st. Shin(C)=Boltzmann / ((SE180(A30...	2.736

Table 5. Average ratio of error between spot exchange rates of the pair BTC/ADA and the utility ratios of the two coins as calculated by five different Shin functions (KNIME)

Shin(BTC//ADA) st. Boltzmann(C)=Avg(BolMin,BolMed)	75.96%
Shin(BTC//ADA) st. Shannon(C)=-Sum(p*logp), p_i←1 - m_i/m_i-1, m←med	88.27%
Shin(BTC//ADA) st. Shin(C)=Shannon * SER	83.42%
Shin(BTC//ADA) st. Shin(C)=Boltzmann / (A90d/#¢)	75.16%
Shin(BTC//ADA) st. Shin(C)=Boltzmann / ((SE180(A30d) + SE180(A7d))/#¢)	68.23%

Table 6. Spearman correlation between spot exchange rates of the pair BTC/ADA and the utility ratios of the two coins as calculated by five different Shin functions (KNIME)

Table 7. Spot exchange rates of the pair BTC/ADA and the utility ratios of the two coins as calculated using Shannon and Boltzmann entropies (KNIME)

Estimating Bitcoin Market Cap (USD)

Boltzmann(C)=Avg(BolMin,BolMed)	92.52%
ShannonMean(C)=-Sum(p*logp), p_i←1 - m_i/m_i-1, m←mean	89.51%
Shannon(C)=-Sum(p*logp), p_i←1 - m_i/m_i-1, m←med	78.73%
Shin(C)=ShaCombinatorial / lg(#¢)	95.75%
Shin(C)=#w/lg(VAR)	92.58%

Table 8. Spearman correlation between Market cap (USD) of Bitcoin vs. the currency's utility values as calculated by five different Shin functions (KNIME)

Table 9. Market cap (USD) of Bitcoin vs. the currency's utility value as calculated by Boltzmann and variance-based Shin functions (KNIME)

Table 10. Market cap (USD) of Bitcoin vs. the currency's utility value as calculated using estimations of the currency's Shannon entropy (KNIME)

Boltzmann(C)=Avg(BolMin,BolMed)	94.89%
ShannonMean(C)=-Sum(p*logp), p_i←1 - m_i/m_i-1, ...	84.64%
Shannon(C)=-Sum(p*logp), p_i←1 - m_i/m_i-1, m←med	90.13%
Shin(C)=ShaCombinatorial / lg(#¢)	43.93%
Shin(C)=#w/lg(VAR)	94.57%

Table 11. Spearman correlation between Market cap (USD) of Ethereum vs. the currency's utility values as calculated by five different Shin functions (KNIME)

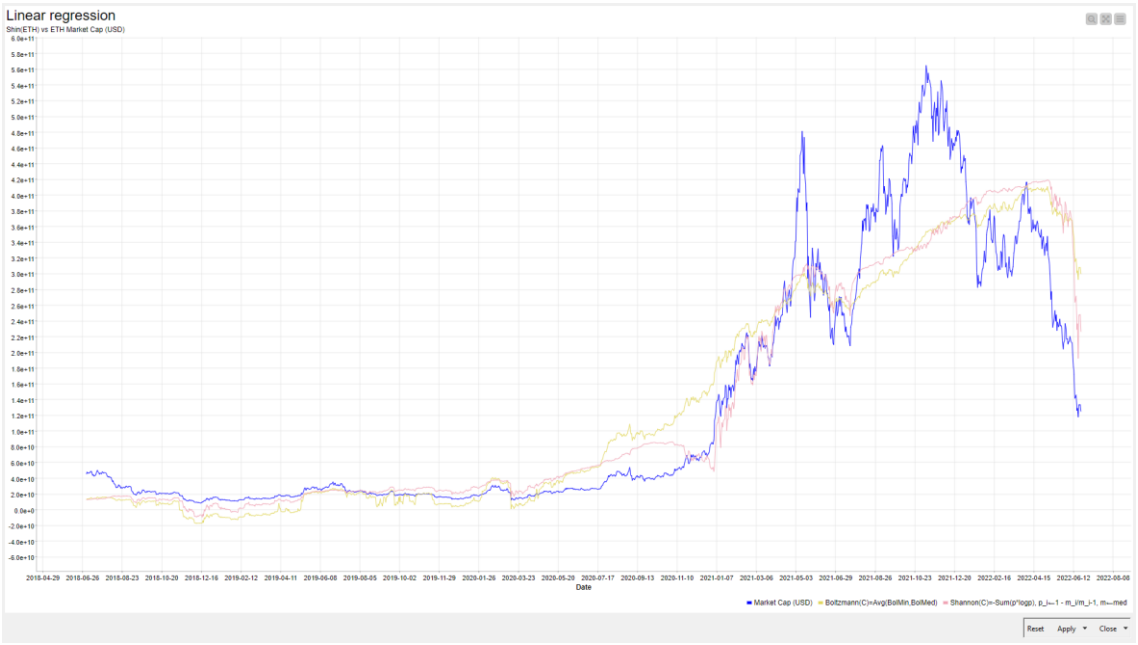

Table 12. Market cap (USD) of Ethereum vs. the currency's utility value as calculated using Boltzmann and Shannon entropy (KNIME)

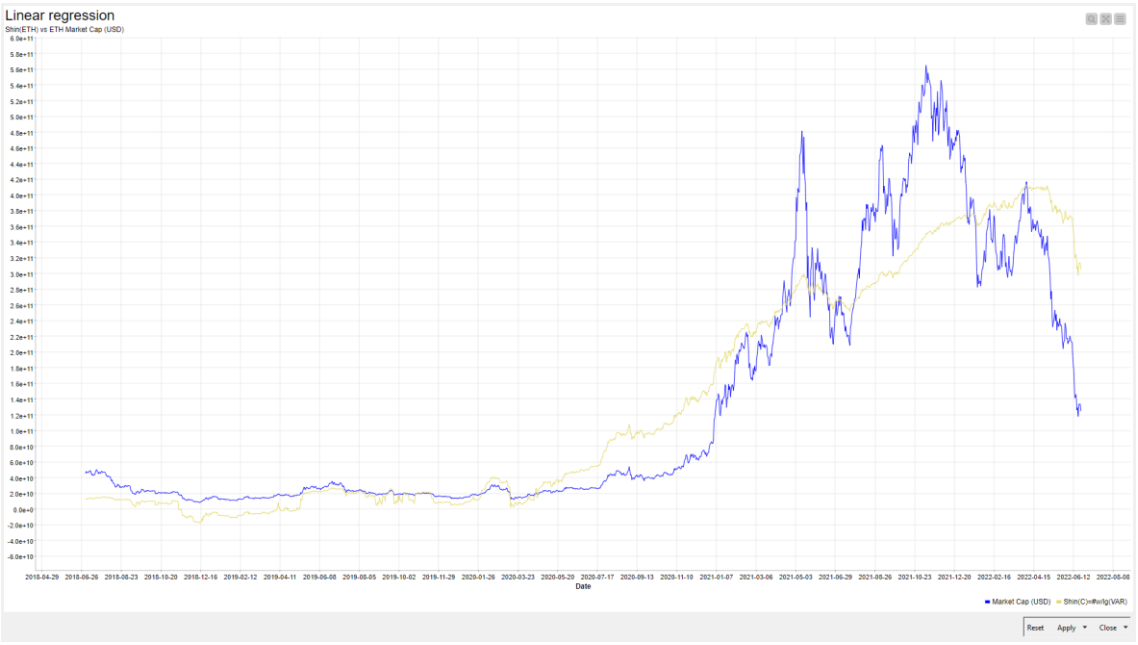

Table 13. Market cap (USD) of Ethereum vs. the currency's utility value as calculated using variance-based Shin functions (KNIME)

8. Acknowledgements

The data were downloaded from coinmetrics.io and processed using KNIME framework version 4.5.2. Out thanks go to Yoram Hirshfeld for his mathematical teachings and to Yehuda Elkana for his interdisciplinary schooling. Also we wish to thank George Karakousis for his input, to Carolyn Seet for her diligent assistance, and to Saul Eden-Draaijer and Sue Graham for their encouragement.

9. References

Bateson, Gregory. 1972. *Steps to an Ecology of Mind: Collected Essays in Anthropology, Psychiatry, Evolution, and Epistemology*. Chicago, IL: University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/S/bo3620295.html.

Diamandis, Peter H. 2021. 'The Story of Aluminum: A Lesson for Entrepreneurs'. 4 November 2021. https://www.diamandis.com/blog/story-of-aluminum-lesson-for-entrepreneurs.

Floridi, Luciano. 2004. 'Information'. In *The Blackwell Guide to the Philosophy of Computing and Information*, edited by Luciano Floridi. Malden, MA: Blackwell Pub.

Shannon, C. E. 1948. 'A Mathematical Theory of Communication'. *The Bell System Technical Journal* 27 (3): 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

Sipser, Michael. 1997. *Introduction to the Theory of Computation*. Boston: PWS Pub. Co.

Spearman, C. 1904. 'The Proof and Measurement of Association between Two Things'. *The American Journal of Psychology* 15 (1): 72–101. https://doi.org/10.2307/1412159.

Wiener, Norbert. 1954. *The Human Use of Human Beings: Cybernetics and Society*. Revised 1988. New York, N.Y: Da Capo Press.

———. 1961. *Cybernetics: Or Control and Communication in the Animal and the Machine*. 2nd ed. Cambridge, MA, USA: MIT Press.