A fair-value model for bitcoin and the mining parity

The Digital Investor
Executive summary

In this Digital Investor, we propose two models to value crypto-currencies. The first is a comprehensive valuation model that provides a fair-value estimate of bitcoin in US dollars. This model is built around four concepts describing the key characteristics of blockchains (network and immutability) and of crypto-currencies (monetary policy and currency type). According to our estimate, bitcoin fair value is currently USD 10,900.

According to our estimates, the most sensitive variables in valuing crypto-currencies are the number of users (demand) and monetary policy (supply) as measured by the network parameter n and the scarcity factor s. The immutability and Gresham parameters, on the other hand, have a lower price elasticity. It is worth noting, however, that as the calibrated hash rate H(d,t) is a large number, its level impacts price level.

The second model compares the exchange rates of crypto-currencies within the crypto-currency space. It is based on a no-arbitrage condition, mining parity. According to it, miners should expect the same profit when mining comparable crypto-currencies in terms of consensus algorithms. Empirical evidence strongly supports the existence of mining parity.
1. Valuation

“Price is what you pay; value is what you get,” said Warren Buffett, the most famous value investor and a crypto-currency sceptic. While it is easy to know the price of everything, it is tricky to estimate the value of things. In the FX space, for instance, Purchasing Power Parity (PPP) and Uncovered Interest Rate Parity (UIP), two models based on sound concepts, do not provide reliable estimates. Despite their poor track records, these models shape and form the basis of investors’ understanding of the FX market, as they help explain where currency value comes from in a fiat money world where none of the currencies has intrinsic value.

According to the existing valuation models, the value of bitcoin network is between zero and 100 trillions US dollars. This range is so vast that it does not provide any insight.

There are several difficulties in valuing crypto-currencies. First, there are no cash-flows associated with crypto-currencies, eliminating the use of any type of discounted-cash-flow model. Second, crypto-currencies are abstract and intangible, unlike commodities. Consequently, they do not have any industrial use, are not a source of energy, and do not shine. Unlike commodities, they do not have intrinsic value. Third, crypto-currencies are not comparable to traditional currencies, as they are not legal tender of any country and do not have economies to back them. These difficulties imply that the PPP model does not apply. As there is no financial system around crypto-currencies, there is no yield curve either, making the UIP model not applicable either.

By any means, crypto-currencies are different from traditional asset classes, but what are they? Coin Metrics’ State of the Network issue 37 and issue 40 provide a comprehensive synthesis of the current models. Though many models provide good instincts, they often answer questions in silos. We propose a broader framework with a comprehensive approach. In this edition of Digital Investor, we attempt to provide this comprehensive model for crypto-currencies.

2. A comprehensive model for crypto-currencies

The valuation model we propose is articulated around four terms that capture the essence of native crypto-currency value: network, immutability, monetary policy, and currency type. The first two terms describe the underlying blockchain or the demand for a secure storage, and the last two characterise the crypto-currency, i.e., the supply of a certain type of currency. Only a combination of a robust blockchain and a well-designed currency wrapped in an appropriate set of rules (tokenomics) has value.

Expressed as an equation, our model is as follows

\[ p_c(t) = u(t) \cdot (d(t) / c(t))^{n} \]

where \( p_c(t) \) is the dollar price of the crypto-currency, \( u(t) \) the number of crypto-currencies in circulation, and \( p(t)C(t) \) the market capitalisation.

The first term is the network value. \( U(t) \) is the number of users and \( n \) is the network parameter that captures the positive externalities associated with the users. The number of users indicates the magnitude of adoption. According to Hyman Minsky, “Everyone can create money; the problem is to get it accepted”. In our context, this quote means that the larger the adoption, the higher the value attached to the crypto-currency.
The valuation model we propose is articulated around four terms that capture the essence of native cryptocurrency value: network, immutability, monetary policy, and currency type.

The first two terms describe the underlying blockchain or the demand for a secure storage, and the last two characterise the cryptocurrency, i.e., the supply of a certain type of currency.

Only a combination of a robust blockchain and a well-designed currency wrapped in an appropriate set of rules (tokenomics) has value.

The second term is the immutability value. $H(d,t)$ is the calibrated network hash rate and $i$ the immutability parameter; the second term measures network security. The higher $i$, the more important is immutability as a characteristic and the higher the value associated with it. $H$ is the calibrated network hash rate variable defined as $d^22^{32}$ with $d$ being the difficulty. As $1/H(d,t)$ is the probability the next hash mines a block, the larger $H(d,t)$, the higher the security of the blockchain. Finally, the immutability parameter $i$ measures the price elasticity of security.

$H(d,t)$ is an important variable, as it captures the essence of a blockchain database: its security. When users use a blockchain, they are using the block space, which is scarce. As a result, the piece of information stored in a block, a transaction such as a value transfer, a smart contract, or a transfer of information (signed message), has value. Why would anyone pay a price simply to store information when there are plenty of cheaper alternatives? The explanation is because of two crucial aspects—censorship resistance and immutability. Immutability is a synonym for proof-of-existence; it provides the same guarantees as a bank money transfer, a written contract, or a notarial act in the physical world, without the need to trust any third party.

Notice that $H(d,t)$ is also proportional to the cost of running the network. Whether in a proof-of-work or proof-of-stake blockchain, $H$ provides an indication of the aggregate investment at risk to secure the system and is thus an indication of transfer finality and settlement. The higher $H$, the more likely a transaction is final, as the cost of altering the state change of the blockchain increases.

The last two terms characterise the crypto-currency attached to the blockchain. The third term describes the monetary policy. $C(t)/C$ is an index measuring the proportion of circulating supply $C(t)$ to total supply $C$, and $s$ is the scarcity parameter. This term is a simple description of the monetary policy that fits crypto-currencies that have rigid supply schedules and a maximum number of currencies. It is easy to imagine supply schedules that offer some elasticity while still offering a high degree of discipline. The monetary policy used here is a particular case of the broader idea of monetary policy discipline.

Finally, the fourth term describes the currency type. The ratio $C(t)/T(t)$ measures the proportion of transaction $T(t)$ to the current supply $C(t)$, and $g$ is the Gresham parameter. This ratio captures whether the crypto-currency is more a medium of exchange or a store of value; it is a way to put a figure on the eternal debate about whether bitcoin is a store of value or a medium of exchange. The lower the ratio, the more transactions are observed relative to the supply of money, suggesting that crypto-currency has a high turnover and, thus, is considered by users to be primarily a medium of exchange. A higher ratio indicates low turnover and a high degree of holding.

To this ratio we attach a parameter $g$ for Gresham, as this ratio reflects also the idea behind Gresham’s Law that states that “bad money drives out good”. The good money that is more valuable in the eye of the user gradually disappears from circulation as it is held. This practice translates into a low turnover (a high ratio), as that money is mainly a store of value. Bad money circulates more, as people try to get rid of it. As a result, that money is a medium of exchange characterised by a high turnover (low ratio).

Before turning to empirical results, it is worth noting that our model is designed for crypto-currencies. Platform and utility crypto-currencies probably need another specification.

---

1 Difficulty is a measure of how difficult it is to mine a block. It is adjusted every 2016th block to keep an average mining time of 10 minutes in the case of bitcoin. To translate the difficulty level in hashes, it needs to be multiplied by $2^{32}$.
2 Anybody can send a transaction as long as her/his address balance is greater than the amount s/he wishes to send.
3 Changing information in a block is incredibly difficult. It is a function of $H$ and of the number of blocks mined after the block that is to be changed. The higher $H$ and the longer the blockchain, the higher is immutability.
3. Empirical results

To estimate our model, we run an OLS regression on the logarithmic transformation of our model. (Note that for reading ease, variables previously written in capital letters are noted in small letters when expressed in logarithms. Interested readers are invited to examine the Appendix to see how we arrived at the econometric model.) After rearrangement, the econometric model becomes

$$p_t + c_t = b_0 \left(1 - \frac{c_t}{c_t}ight) + b_1 u_t + b_2 h_t + b_4 (t_t - c_t)$$

where $p(t)$ is the market capitalisation, $m(t)$ the modified monetary policy, and $t(t)-c(t)$ the Gresham’s turnover. Figure 1 presents the bitcoin (BTC) regression estimates. All parameters are significant and show the correct signs. From these estimates, we retrieve the original parameters $s$, $n$, $i$, and $g$. Each is presented in Figure 1.

The specification of the model is such that the parameters measure the price elasticity of the variables. For instance, the network parameter $n=1.26$ means that for a 1% increase in the number of users, price increases by 1.26%. According to our estimates, the most sensitive variables are the number of users (demand) and monetary policy (supply) as measured by the network parameter $n$ and the scarcity factor $s$, respectively. The immutability and the Gresham parameters, on the other hand, have lower price elasticity. It is worth noting that as the calibrated hash rate $H(t)$ is a large number, its level impacts price level.

---

4 We are grateful to Sivaji Sabbavarapu for helping us specify and estimate the econometric model.

5 To estimate the number of users, we use the number of addresses that have at least 0.001 BTC. For the transaction variable, we use the value of transactions in native currency.
Figure 2 illustrates the evolution of BTC price and fair-value estimates. At the time of this writing, bitcoin fair value is at USD 10,900, suggesting that at its current price bitcoin is close to fair-value. In the wake of halving, the fair value has declined, as indicated by the light green line in Figure 2. The decline is due to the two downward difficulty adjustments that followed halving, in line with the price forecasts we published in the May Digital Investor.

Notice that, as with all models, estimates need to be taken with humility. Nevertheless, we think this model provides a framework for analysing price movements from a fundamental angle and gives an anchor to investors.

Estimates for other crypto-currencies such as Litecoin (LTC), Bitcoin Cash (BCH), and Bitcoin Satoshi Vision (BSV) are not conclusive. Parameters are mostly significant but show incorrect signs. For instance, BCH’s network parameter \( n = -0.90 \) suggests that value declines as the number of users increases. For LTC, the scarcity parameter \( s = -1.09 \) is negative, meaning that the scarcer the currency, the less value it has.

We think these results reflect weaknesses in the ecosystems supporting the crypto-currencies. Comparing bitcoin and other proof-of-work currencies, trust in bitcoin is the strongest among the pack for several reasons. Bitcoin has survived against all odds, while BCH and BSV have been challenged in stormy weather and are both identified with controversial personalities. LTC has limited development. In contrast, bitcoin has become more decentralised. Developers have received grants from different organisations including academic institutes such as MIT and firms such as Square, Inc. Development of bitcoin has remained robust over the years. One can safely assume that bitcoin is the most decentralised proof-of-work cryptocurrency. This robustness attracts miners and, in turn, more security, and more security translates into more trust.

These qualitative judgements are not captured in any of the four terms that make up our model. In econometric terms, there is an omitted variable bias. The bias results in the model attributing the effect of the missing variables to the variables that were included.
4. Mining parity

Accepting that our model provides reliable estimates of BTC fair value, the market price is very often, perhaps almost always, out of equilibrium. Investors know that this observation is valid for traditional asset classes as well. In the FX market, for instance, the spot price deviates significantly and for a long time from its PPP value.

Acknowledging these observations, fair-value models provide insightful signals for long-term investors and for large price discrepancies. In the short term, however, their use is limited. Therefore, we propose a no-arbitrage condition built on mining activity: the mining parity approach. In spirit, it is similar to the notion of mint parity used in metallic systems such as the gold standard to compare the price of two currencies.

Three coins, Bitcoin (BTC), Bitcoin Cash (BCH), and Bitcoin Satoshi Vision (BSV), are directly comparable as they use the same mining algorithm. Miners can switch between them with little difficulty. The relative ease of switching between these coins forms the basis for analyzing whether some coins are more attractive than others.

The first assumption is that miners are rational. In a competitive market, each coin is expected to result in the same return. Otherwise, arbitrage is possible between the coins. This no-arbitrage condition is the mining parity.

The expected USD profitability of mining the next BTC block is expressed as follows:

\[
E^{BTC}_{t}(\text{Profitability}^{USD}_{t+1}) = P_{t}(\text{Block}^{BTC}_{t+1}) E_{t}(\text{Block reward}^{BTC}_{t + 1}) E_{t}(\text{BTCUSD}_{t+1}) - \text{Cost}^{USD}_{t + 1}
\]

The equation illustrates that the expected profitability in USD in time \( t \) to mine the next block at time \( t+1 \) is equal to the probability of mining the block multiplied by the block reward (mining reward and fee) expressed in USD minus the cost of mining in USD (e.g., hardware and energy). This generic equation holds for BTC, BCH, and BSV.

Mining parity states that

\[
E^{BTC}_{t}(\text{Profitability}^{USD}_{t+1}) = E^{BCH}_{t}(\text{Profitability}^{USD}_{t+1})
\]

as miners are indifferent in choosing to mine BTC or BCH. Given that the equipment and overhead costs are the same, rearranging the terms, we get the following mining parity for BTCBCH (i.e., the price of BTC expressed in BCH).

According to the mining parity condition, the BTCBCH exchange rate should be equal to the ratio of the probability of mining the next block of each coin, multiplied by the respective rewards.

\[
E_{t}(\text{BTCBCH}_{t+1}) = \frac{P_{t}(\text{Block}^{BCH}_{t+1}) E_{t}(\text{Block reward}^{BCH}_{t + 1})}{P_{t}(\text{Block}^{BTC}_{t+1}) E_{t}(\text{Block reward}^{BTC}_{t + 1})}
\]

According to the mining parity condition, the BTCBCH exchange rate should be equal to the ratio of the probability of mining the next block of each coin, multiplied by the respective rewards.

\(^4\) According to mint parity, if a coin is backed by 10 grams of gold and another coin by 5 grams, the first coin is twice as valuable as the second.
While there is no evidence of miners switching between coins to maximise their expected returns, mining parity seems to hold, as Figures 3 and 4 suggest.

**Figure 3: BTCBCH and the mining parity**

![BTCBCH and the mining parity graph](image)

Source: SEBA, Coinmetrics
Historical data are not a reliable indicator for future performance

**Figure 4: BTCBSV and the mining parity**

![BTCBSV and the mining parity graph](image)

Source: SEBA, Coinmetrics
Historical data are not a reliable indicator for future performance
Conclusion
In this edition of Digital Investor, we have presented two crypto-currency models. The first model is an attempt to provide a comprehensive approach to valuing crypto-currencies. In the second model, we used a no-arbitrage condition, mining parity, to compare the price of two crypto-currencies.

The results of both models are encouraging. They show that we can value crypto-currencies and that their behaviours against each other are not random. We believe that these models can help investors gauge the attractiveness of crypto-currencies and make better investment decisions.

5. Appendix

For memory, the model is

$$P_t C_t = U_t H\left(\frac{C_t}{C_{t-1}}\right)^{\gamma}$$

To estimate our model, we run an OLS regression on the logarithmic transform of the model. Note that for the ease of reading, variables previously written in capital letters are noted in small letters when expressed in logarithms. After rearranging the terms, the model expressed in logarithms look as follows

$$p_t = -sc + nu_t + ih_t + (s + g - 1)c_t - gt_t$$

As parameters s and g are related to each other, the model is rewritten to make the constraint explicit:

$$p_t = b_0 + b_1u_t + b_2h_t + b_3c_t + b_4t$$

s.t. $$b_3 = -\frac{b_0}{c} - b_4 - 1$$

After substituting for the constraint and rearranging the terms, we have:

$$p_t + c_t = b_0 \left(1 - \frac{c_t}{c_{t-1}}\right) + b_1u_t + b_2h_t + b_4(t - c_t)$$

where $$p'(t)$$ is the market capitalisation, m(t) the modified monetary policy, and $$t(t) - c(t)$$ Gresham’s turnover.