# Computational Aspects of Cryptocurrency Valuation

Matt Gmitro

December 19, 2017

**Abstract**

I provide an economic analysis of decentralized cryptographic asset consensus protocols through case studies on Bitcoin and Ethereum. In the Bitcoin study, I build on Hayes' (2015) cost production model by projecting future inputs and their implications on the market. In the Ethereum study, I survey the transition from a proof-of-work to proof-of-stake consensus and develop a model for decline in supply. Finally, I draw lessons from NXT's alternative proof-of-stake protocol and survey the condition of Initial Coin Offering markets. Using these frameworks, I draw conclusions on the future of consensus protocols and their impacts on cryptocurrency markets.

## 1 Introduction

While cryptocurrencies have exploded in popularity, the naive investor knows little about their complex technological underpinnings. The current universe is vast, with a plurality of over 1,300 cryptocurrencies to choose from. Blockchain consensus protocols specify how nodes propose various blocks and come to an agreement on the permanent record of the chain. Consensus algorithms drive economic incentives for miners and users because they require validation to formally prove trust. Furthermore, these protocols change over time to reflect the nature of market actors and technological innovations. For example, the protocol for bitcoin changes the difficulty for adding a block to the chain in response to how much computational power is spent on the network.

There is a large base of literature covering consensus algorithms and a small but growing study of cryptocurrency valuation. I aim to marry these two areas of study by directly considering the economic impacts of changes to consensus protocols. Modifications to a consensus protocol affect the means of production and value behind a cryptocurrency by refactoring incentives and rewards for participating in the network.

In this paper, I survey the future of blockchain consensus mechanisms and consider impending market implications. Section 2 covers basic background knowledge on blockchain, proof-of-work, and proof-of-stake models. Section 3 is a case study on the economic impacts of Bitcoin protocols changing over time. Section 4 is a case study on the economic impacts of Ethereum's transition from proof-of-work to proof-of-stake. Section 5 surveys altcoin variations and the Initial Coin Offering market. Finally in section 6, I draw conclusions and propose future lines of study.

# 2 Background

## 2.1 Blockchain

Not all cryptocurrencies are created equal, but all stem from a familiar technology – blockchain. Blockchain is a distributed ledger system whereby each node in the network independently confirms transactions by adding blocks to the ledger that are cryptographically linked and secured. For a node to add a block to the ledger, it must follow a number of protocols. The node hashes a series of transactions into a Merkel Tree where the root hash is used to form a block header. The block header is a combination of the root hash, the previous block's hash, and a "nonce" to align the block with the protocol. The node which creates a block is rewarded through the issuance of new coins or transaction fees.

Different blockchains have different protocols for different uses. For example, Bitcoin uses the SHA256 cryptographic hash function while Litecoin uses the Scrypt hash function. Different hash functions require varied types of computations. One of the most important types of protocols is the protocol by which nodes form consensus. These protocols prove that the data in a block on the blockchain must be true for all users. Sections 2.2 and 2.3 cover the two main flavors of consensus protocol.

## 2.2 Proof-of-Work

The blockchain can undergo forks when multiple blocks are proposed. Thus, a newly generated block must achieve consensus approval to be added to the chain. Proof-of-Work (PoW), is a set of consensus algorithms driven by solving computational problems.

Miners compete to solve computational puzzles by generating an acceptable hash to their block. Once a block is found, it is broadcast to the network. Because the puzzles are unique, this solves the problem of agents appending to multiple branches by leading them to append to one branch [12]. The specific blockchain protocol determines the mining rate by changing the difficulty of the puzzles. There also may be a cap on the maximum number of coins in existence and changes to the mining reward.

Proof-of-Work systems require immense amounts of computational power and, in turn, electricity. Furthermore, they are prone to centralization because mining pools form to amass computing power. A popular conceptual attack is the 51% attack in which the attackers gain control over 51% of the computing power and are able to maliciously reinvent the blockchain with only their definition of acceptable blocks.

### 2.3 Proof-of-Stake

Proof-of-Stake (PoS) is a newer consensus model based on validators with economic stake in the network. In PoS, validators put up a deposit before proposing and voting on new blocks. There are two main types of algorithms for choosing a validator for each block [14]:

1. The chain-based proof-of-stake algorithm selects a validator at each time slot and bestows the right to create a block. The chains eventually converge because the algorithm specifies the previous block to the validator.

2. The Byzantine Fault Tolerance (BFT) proof-of-stake algorithm allows all validators to propose a block before a multi-round vote. Each round, every validator votes on blocks and at the end they all must agree permanently on the blocks.

PoS algorithms have several benefits. Under PoS, there is no need for mass expenses of computational power and electricity. Furthermore, PoS systems heighten the asymmetric nature of blockchain cryptography by penalizing validators who attempt to subvert the permanent record [14]. PoW also penalizes malfeasant actors, but only through the computational power they waste. PoS gives the ability for the protocol to impose harsher economic consequences by destroying a validator's stake.

At the same time, these algorithms are susceptible to many security threats. Being a validator allows for much more freedom within the protocol than simply running a processor like in PoW. Many problems have been solved in the implementation of the upcoming Ethereum PoS protocol, but some issues still remain to be solved. Saleh (2017) provides a formal proof of consensus for naive PoS protocols. His approach, however, does not account for game theoretic cartel situations that arise when a dominant group of validators can censor a minority group of validators. Zamfir (2016) proposed that "the cartel cannot censor the absence of censored validators." This implies a sophisticated PoS protocol must penalize the cartel when validators appear to be missing and in turn penalize validators who go offline.

The following case studies explore how changes in these protocols will affect market structure and value.

## 3 Case Study 1: Bitcoin

Bitcoin is the model example for PoW consensus. In bitcoin's protocol, the mining difficulty is adjusted such that a block is only mined on average every 10 minutes. There is an upper limit on the number of bitcoins at 26 million, about 80 percent of which have already been mined

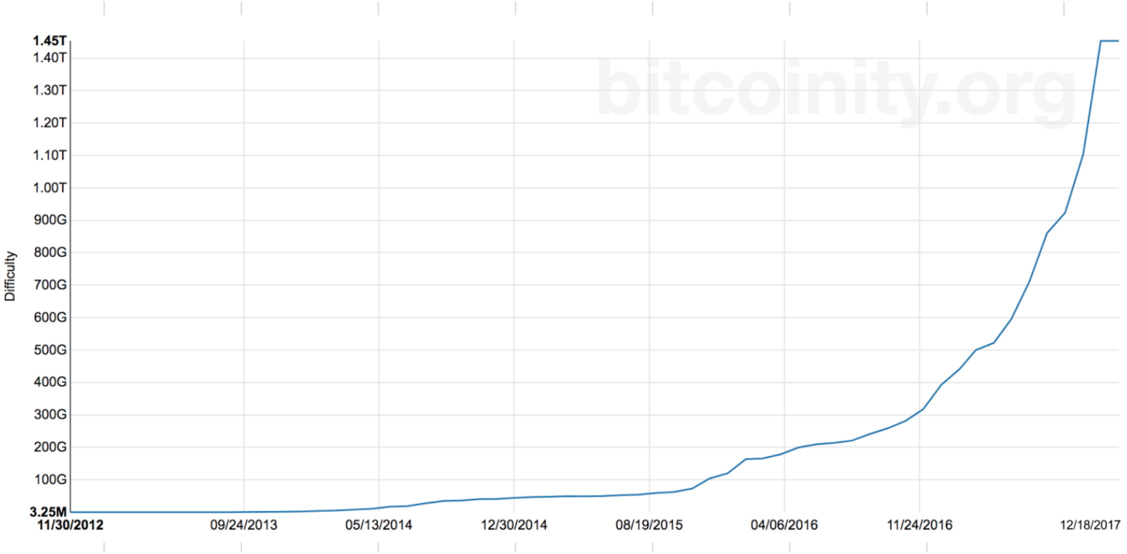
[12]. Furthermore, the reward for mining decreases as time goes on and computational power requirements increase.

Hayes (2015) provides an empirical least-sqaures regression using data from 66 cryptocurrencies to determine factors driving valuation. He found that mining difficulty and rate were highly statistically significant for variations in cryptocurrency price relative to other cryptocurrencies in the basket. Furthermore, he provides a cost production model for bitcoin:

> The cost of mining per day, $E_{day}$ can be expressed as:
>
> $$E_{day} = (\$price\ per\ kWH \cdot 24hr_{day} \cdot W\ per\ GH/s)(\rho/1000)$$
>
> Where $E_{day}$ is the dollar cost per day for a producer, $\rho$ is the hashpower employed by a producer, the \$price per kWh is the price per kilowatt-hour, and W per GH/s is the energy consumption efficiency of the producer's hardware. The marginal product of mining should theoretically equal its marginal cost in a competitive market, which should also equal its selling price. Because of this theoretical equivalence, and since cost per day is expressed in \$/day and production in BTC/day, the \$/BTC price level is simply the ratio of (cost/day) / (BTC/day). This objective price of production level, p*,
>
> $$p* = E_{day}/(BTC/day*)$$

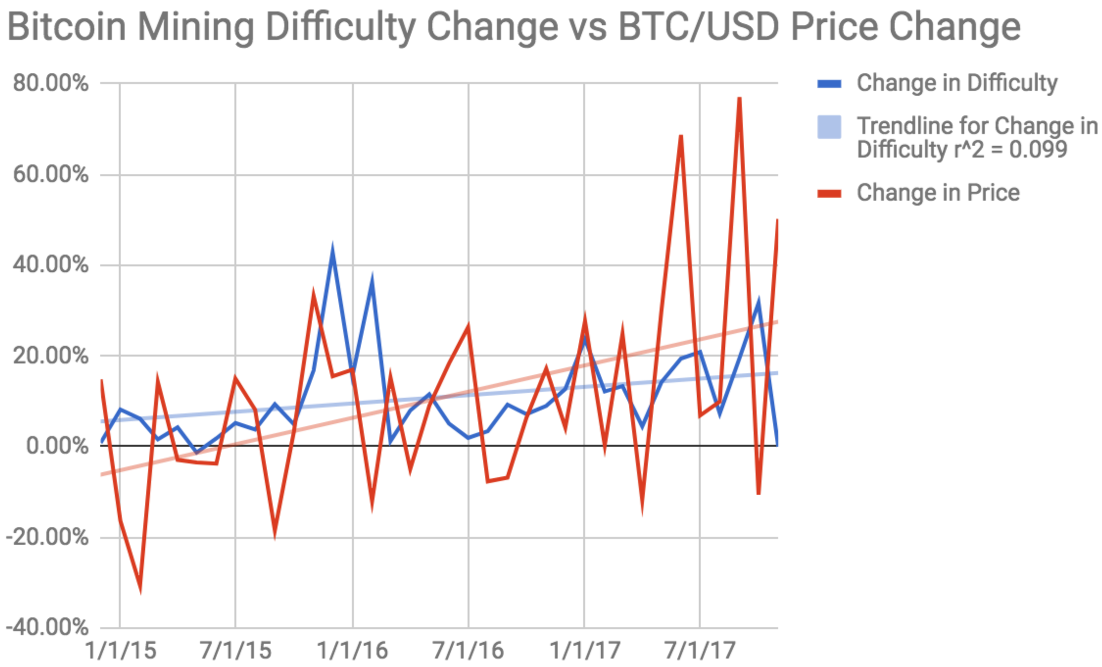
Using this model, we can observe and predict the nature of changes in mining incentives over time. The mining difficulty increases every 2,016 blocks by an amount which depends on the current global block difficulty and how many participants are actively mining on the network. Historically, difficulty increase follows an exponential pattern, doubling about every 4 months.

Historical Increase in Mining Difficulty CITE



Source: bitcoinity.org

Furthermore, we can analyze how changes in mining difficulty correlate with the price of bitcoin. Using month over month data on percentage change in difficulty and price, I obtain the following chart:



Data source: bitcoinity.org

There is a cause-and-effect loop relationship between changes in difficulty and changes in price. When prices rise, increases in mining difficulty should be higher because miners have a better incentive to deploy their resources. Alternatively, when the difficulty rises, the price increases because there is more computational power backing the coins and the miners require more handsome rewards. These properties create a feedback loop whereby speculative price gains encourage heightened mining activity and heightened mining activity catalyzes price jumps due to demand for mined coins eclipsing supply. Interestingly, the average monthly change in price (11.26%) is very close to the average monthly change in mining difficulty (10.67%).

In a competitive theoretical economy, the miners should keep increasing the marginal cost they are willing to spend until the costs are equal to the marginal reward of mining. This is because miners would keep buying equipment and ramping up electricity consumption until they are no longer making a marginal profit. Thus, as miners are forced to spend more the network should compensate them equally. However, bitcoin also has the property of halving the mining reward every 210,000 blocks. This could cause some miners to drop out due to lack of competitive resources and incentive, which would hypothetically lead to a decrease in difficulty. Empirically, this has not been the case because gains in the price of bitcoin bolstered the real reward value for miners as difficulty rose. The problem with this approach is that crowded out miners are less sophisticated than large mining operations. The difficulty continues to increase, albeit at a slower rate, as large operations scale to the computational challenge quickly.

To project increases in bitcoin mining difficulty, I use the average of monthly change in difficulty over the past three years (11.26%). We can then solve Hayes' production equations using the most up to date metrics. First, we set price per kWH to \$0.12. Then using the specifications for the most powerful current ASIC mining device, the AntMiner S9, I set W per GH/s to 0.098 and $\rho$ to 14000 GH/s. BTC/day can be calculated with the following formula:

$$BTC/day = GH/sec \cdot 1,000 \cdot 12.5\, BTCReward \cdot 24\, hrs \cdot 3600\, sec/2^{32}/Difficulty$$

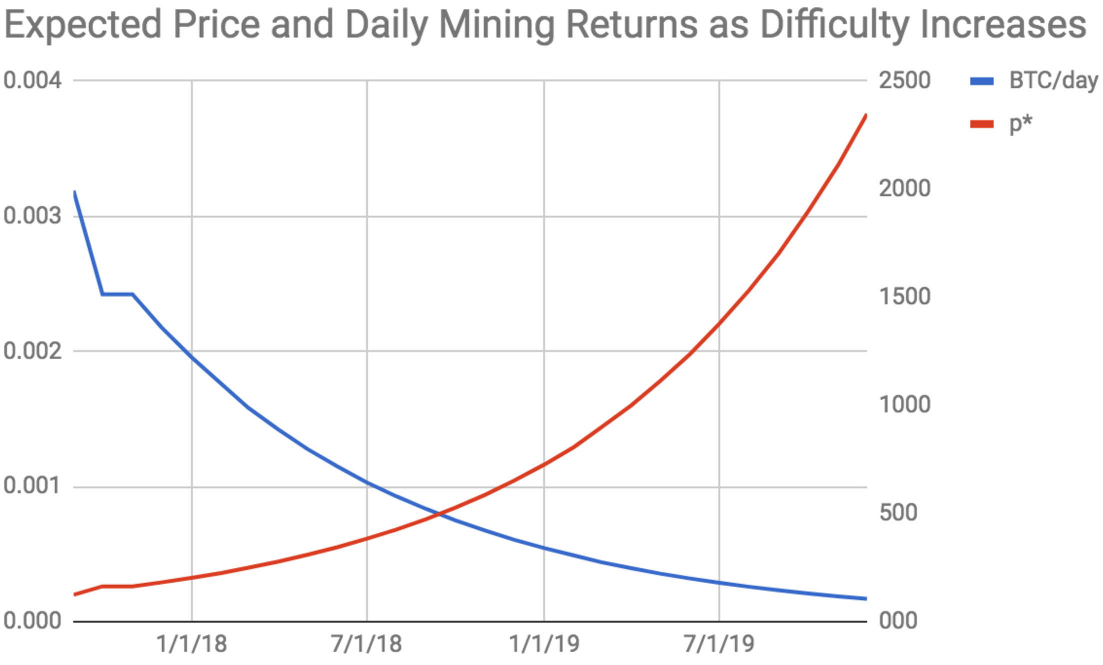
$$= 14000 \cdot 1000 \cdot 12.5 \cdot 24 \cdot 3600/2^{32}/(1,590,896,927,258/1,000,000) = 0.00221283935$$

Substituting this into Hayes' formulas, we get:

$$E_{day} = (0.12 \cdot 24 \cdot 0.098)(14000/1000) = 3.95136$$

$$p* = 3.95136/0.00221283935 = 1785.65154312$$

Using this model with our projection for increasing mining difficulty, I create the following chart:



This model does not take into account costs of mining hardware, downtime, or mining pool fees. I also do not calculate the benefit of transaction fees on mining profits.

The data suggests that bitcoin's market value (around \$18,900 as of December 18th, 2017) is much higher than the current cost of production. At the current price of bitcoin, a miner would remain highly profitable through the end of 2019 even with increases in difficulty. A miner with the best equipment in today's market is earning \$41.82 per day while spending \$3.95. This should incentivize more miners to join the network, which would increase competition and push costs up. However, getting the best mining hardware is a challenge. The AntMiner S9 is sold in periodic batches by one company. In secondary markets, the price for one of these devices is nearly triple the retail cost. This slows the rate of difficulty increase by keeping prospective miners on the sidelines.

It also explains the problem of marginal cost being less than marginal reward because some miners are limited from spending more on resources. There are also disadvantages for miners in regions with more expensive electricity. Thus, the marginal reward can increase and the marginal cost remains relatively low.

There may be various reasons why bitcoin's market value suggests such a discrepancy from the cost production model. First, bitcoin's economic value is not solely tied to the production of mining. The market is influenced by speculators, large illiquid pools of BTC, and macroeconomic circumstances. While price volatility implies high levels of speculation, there are publicly known illiquid pools of bitcoins such as the 980,000 owned by anonymous bitcoin inventor Satoshi Nakamoto. Illiquid stakes of bitcoin should influence the price to rise over the long term by limiting supply.

Second, the total supply of bitcoin is capped at 21 million. The market may be pricing in the future value of bitcoin in a world where all bitcoins are mined, pushing its current value higher than predictably justifiable. Based on the protocol, all bitcoins will be mined by 2140. When this happens, miners will not receive block rewards but continue to receive transaction fees. It is foreseeable that the price of bitcoin will increase to the point where transaction fees are feasible rewards for mining. However, miners may begin to take malicious strategies when the block reward is removed. Carlsten et al. simulated bitcoin mining strategies absent a block reward. They found multiple strategies malicious miners can utilize to undercut each other in an effort to find blocks with the biggest transaction fees [4]. The bitcoin protocol will, therefore, more than likely need to be updated as the maximum issuance is reached.

Due to tremendous uncertainty surrounding the true value of bitcoin, the price is subject to massive swings. However, analyzing the mining ecosystem provides a clear picture of the costs associated with creating bitcoin and the economic incentives behind market participants. Bergstra and Weiland type bitcoin as a money-like informational commodity because bitcoin holds a scarce good in the form of trustworthy information. Similar to pricing a commodity, the costs of production and holding provide a baseline for valuation before market considerations of supply and demand.

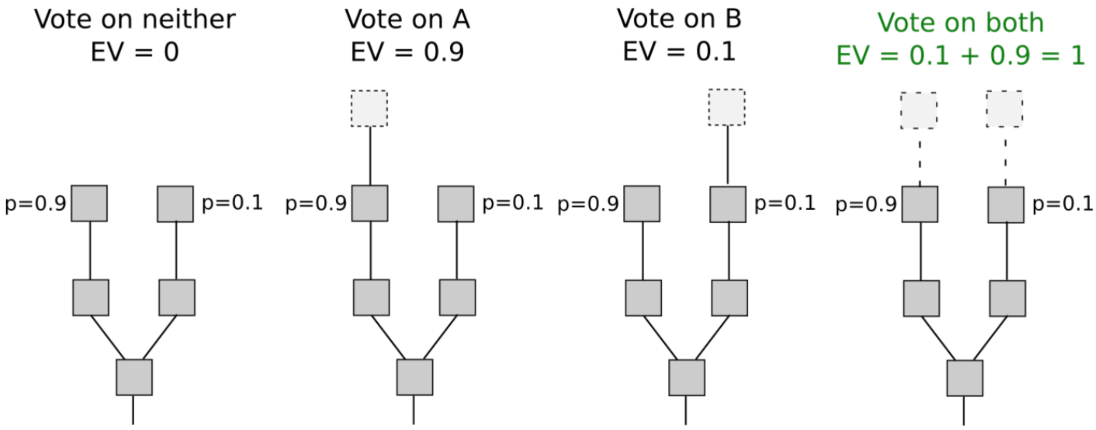
# 4 Case Study 2: Ethereum

## 4.1 Casper Overview

Ethereum's blockchain uses a virtual machine (the Ethereum Virtual Machine) to run smart contracts. When a transaction occurs, users pay or receive the cryptocurrency ether to execute the logic involved with the transaction and add it to the ledger. The beauty of the EVM is the ability to program any type of logic into what are considered Turing-complete smart contracts.

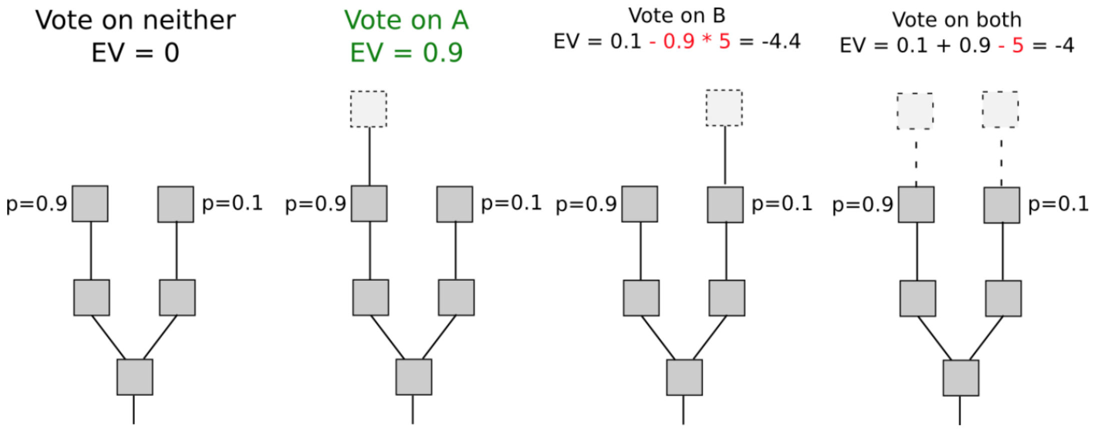
Ethereum's developers are currently planning a fundamental change from a proof-of-work to a proof-of-stake consensus protocol. This transition will impose major changes unto the network and could drastically change the scalability of Ethereum. The new PoS algorithm, called Casper, is the product of years of research into PoW alternatives.

Casper is implemented with novel ways of solving several challenges to PoS algorithms. The Nothing-at-Stake problem proposes that a malicious validator may attempt appending a block to every possible branch because there is no cost to doing so [14]. The validator's incentive is to reap the rewards from a new block either way even if they are appending to an incorrect branch.



Source: Ethereum Github Wiki

PoW algorithms solve for this because the malicious actor would have to suboptimally split their computing power. In Casper, validators put up a deposit in ether and bet on the blocks they believe will be added to the blockchain. More weight is given to validators who deposit larger sums. The value of the deposit changes with rewards and penalties. Validators vote on checkpoints along the blockchain. If two thirds of validators agree on a checkpoint, then it is considered finalized. If there are multiple chains with two thirds approval, Casper follows "slashing" protocols whereby at least one third of the total deposits from bad validators are destroyed [3]. Moreover, these protocols disincentivize validators from voting for less probable branches by penalizing for choosing the wrong branch, as depicted below.



Source: Ethereum Github Wiki

To boost efficiency, the Casper protocol uses "checkpoint trees" to validate. Every one hundred blocks added to the chain is a checkpoint. Each checkpoint c has a height h(c) that is equal to the number of blocks stretching from the checkpoint to the root. A validator votes on blocks to be added to the checkpoint tree by including a source checkpoint, a target checkpoint, and the heights of the source and target. There are two slashing conditions in the initial Casper implementation [3]:

**(1)** $h(target_1) = h(target_2)$. A validator may not publish two votes that share the same target checkpoint height.

**(2)** $h(source_1) < h(source_2) < h(target_2) < h(target_1)$. A validator must not vote within the span of its other votes. This means that the checkpoint heights of both the start and target from one vote may not fall between the checkpoint heights of the start and target from the other vote.

The initial Casper implementation will feature a hybrid-PoW-PoS consensus algorithm where miners propose blocks and validators validate them in the context of the blockchain. Eventually, the goal is to implement a pure PoS algorithm for Ethereum where validators are also bestowed the right to create and propose blocks.

## 4.2 Market Implications

Making such a fundamental change to the Ethereum network will have important economic impacts. PoW mining will eventually become unsuitable, forcing current Ethereum miners to migrate their computational power towards other cryptocurrencies that follow similar cryptography schemes. Given the implications from earlier in this paper, these alternative PoW cryptocurrencies will experience a jump in mining difficulty and price.

Ethereum itself will see the most sweeping changes. First, without PoW, there is little need to issue new coins. The developers have already declared their wish to gradually reduce and eventually end new issuance [15]. Built into Ethereum's protocol is a difficulty bomb where at a certain point the computation to mine new ether will outscale the feasibility to do so. In the past, Ethereum used hard forks to avoid this problem and maintain issuance, but Casper is a long term solution. Ether was designed as a disinflationary currency because the growth rate of the monetary base is set to decrease each year [11]. That is, the amount of ether inflation decreases every year under the current protocol. This is because while the number of ether issued each year is fixed, real exchange rates are not. Ether will appreciate relative to other currencies which are inflating.

Moving to a PoS system will drop the rate of inflation deeper into negative territory when new issuance is eliminated due to slashing bad validators' deposits in addition to the (1%) of ether that are lost every year in bad transaction [11]. The supply of ether is much greater than that of bitcoin (about 80,000,000 ethers versus 18 million bitcoins in circulation). Because validator deposits in Casper are made using ether, the available supply of ether will drop dramatically for two reasons:

First, bad validators will incur slashing penalties that will destroy those ether forever. Conflicts requiring the decimation of large swaths of deposits are doubtful, but Casper also necessitates a small penalty for merely appending to the wrong chain (as opposed to trying to append to two separate chains maliciously).

Second, deposits are meant to be large and stay locked up for a considerable amount of time. While there is no official word on the deposit size and lock up time, developers recently detailed deposit sizes of 32 ether and lock up times of 4 months to a year in the Ethereum.org 2.0 Mauve Paper. With the current price of ETH/USD around $800.00, this will require a significant amount of capital to be held illiquid for a long period of time.

Using the rate of slashing, amount deposited, and amount lost, we can build a simple model for ether supply decline at a given point in time:

$$Loss_t = Outstanding_0 + \sum Issuance_t - ((Outstanding_t \cdot 1\%/t) + Slashed_t + Deposits_t)$$

Where t denotes the number of days since the beginning of the year and variables subscripted with t denote the total amount of the variable on day t. Because of the economic incentives behind Casper, the rate of slashing should be low. When a conflict does occur, however, one third of deposited values involved at a conflict will be erased every time slashing does occur [3]. This does not take away from the immediate general supply, but from the deposit supply. The second order consequence is that more deposits will fill the void to maintain staking competitiveness. I assume the amount lost from users going offline will follow developer estimates at 1% per year [11]. The amount deposited in stakes depends on how many stake-holders appear and how profitable staking becomes.

Ether was also designed with a purpose detached from the market. It is the "fuel" to run and process smart contracts on the Ethereum blockchain. The use cases for Ethereum differ drastically from bitcoin because complex transaction systems can be built on the network. However, the current plan keeps the cost of transaction the same regardless of ether valuation. With this feature, ether's value is free to fluctuate without impacting the underlying technology.

Finally, PoS makes ether intrinsically more valuable. A stake of ether may be viewed like an expensive mining chip plus the electricity to run it. In PoW models, the mining chips get more expensive as the cryptocurrency becomes more valuable because the value of rewards and competition for them increase. In PoS, buying the resources to stake will increase the value of ether itself. Compared to the two way cause and effect feedback loop from increasing mining power and bitcoin price, the PoS system builds a self-reinforcing feedback loop where higher prices beget higher prices. Thus, Ethereum will experience both a supply glut and demand boom when moving to PoS. Furthermore, the PoS system does away with the fixed costs of mining units. This diminishes the economies of scale leading to centralization in PoW schemes because it gives no marginal advantage for larger stakers, only a proportional advantage.

The findings of this section suggest that the price of ether will begin to skyrocket with the transition into proof-of-stake protocols. The key factors for the future value of ether are how often slashing will occur, when new issuance will stop, and how much ether becomes tied up in staking. Each of these inputs decrease the supply of ether, the future question is to what extent that will happen.

# 5 Altcoin Considerations

## 5.1 Alternative Proof-of-Stake Example

Several altcoins use proof-of-stake consensus protocols that differ from Ethereum's proposed Casper model. The main difference between Casper and other proof-of-stake implementations is the security concerns Casper alleviates through the penalizing slasher system.

NXT is a cryptocurrency similar in scope to Ethereum. Its protocol uses a random system to choose a validator, giving more weight to validators with higher stakes. The penalty for a malicious validator in NXT is simply that the value of their stake becomes diminished after an attack. This does not necessarily solve the Nothing-at-Stake problem. Bad validators may also try to subvert the random seeding system by skipping the opportunity to create a block [14]. NXT has a fixed coin supply and allows stake-holders to withdraw at any time.

The design ideology behind NXT was not that NXT be used as a valuable token, but rather as an access to the NXT blockchain on which other applications can be built. This seems short-sighted because valuable applications running on NXT would confer value onto the tokens that grant access. After the recent announcement that NXT holders would get free tokens from a new cryptocurrency built on the NXT platform, the price of NXT spiked [13]. Ultimately, NXT is an example of early technological innovation around Proof-of-Stake that attempts to remain detached from speculative valuation. NXT provides a salient example of how tokens may be rewarded economic value through technologies built upon their blockchains.

## 5.2 Initial Coin Offerings

The world of initial coin offerings (ICOs) is akin to the wild west. An ICO is a method of initial issuance for cryptocurrencies or tokens. A firm proposes a new coin on a proprietary blockchain or a blockchain platform that supports contracts for tokens (like Ethereum). The firm will typically present a technical white paper and use crowdfunding to raise a sufficient amount of capital. Investors get the new token at the issuance price, betting that it will someday be valuable.

Generally speaking, these new tokens can adopt any protocol the creators choose, but typically add some function on top of the token other than as an asset. ICOs are risky because there is no guarantee the token will gain popularity and there is little regulation around the process.

Conley (2017) analyzes token valuation from various paradigms (e.g. as a currency rather than a security). While I agree with his salient analysis, the end conclusion is that an investor must differentiate between types of tokens to value them. I seek to provide an analysis of the ICO market generally.

ICOs of successful coins produce huge returns on investment at huge risk. An investor in IOTA's 2015 ICO would have a 990,741% return on investment with current market prices . However, only about 3% of the over 1300 cryptocurrencies in existence achieved over 1000% return of investment [9]. The main reason for this is that many investors fail to do due diligence on the start ups behind the ICO. Because it only takes a white paper to propose an ICO and anyone can contribute funds, the potential for ill-conceived plans or fraudulent scams receiving funding is high [18]. The market is likely to change in 2018 with the Securities and Exchange Commission becoming increasingly interested in the space. In their December 11th, 2017 commentary, the SEC describes a token with the characteristics of an equity as a security [17]. However, they also leave room for other types of cryptoassets to operate outside of the categorization. The conclusion is that ICOs which function like Initial Public Offerings will be the first to face heavy regulation.

Increased regulation and due diligence would cause the number of ICOs to decrease but the quality to increase. This would open up ICOs to be less volatile and more consistent with their purpose of funding the creation of valuable digital assets. In a world with very little volatility, ICOs seem like good bets for investors trying to make outsized returns. When volatility spikes, investors will want to search for safer havens. ICOs can be problematic in this regard because the initial fundraising can occur before the implementation of a product. This can lock up funds and reduce the probability of making any return on investment. For ICOs to be legitimately usable investment instruments, they must become formalized in a way that limits their own volatility.

## 6 Conclusion

Cryptocurrency markets are rife with uncertainty. In the press, there are incessant warnings of a bubble, and prices fluctuate with wild volatility. Technological considerations underpin the economics of cryptocurrency markets. Changes in consensus protocols, mining difficulty, and supply all affect the long term price of each asset. In order to truly understand the forces that drive value in cryptocurrencies, it is paramount to dive into their technological components. While implementations differ vastly, both Bitcoin and Ethereum deploy systems of economic incentives that imply long term value.

In Section 3, I modeled and predicted a future cost of production model for bitcoin. The model suggests that bitcoin is much more expensive than the cost of its prediction. This shows that miners will remain profitable given a certain price level despite increasing difficulty. Furthermore, I introduce the concept of a synergistic cause-and-effect relationship between mining difficulty and price change.

In Section 4, I analyze the market implications of Ethereum's proposed move from a proof-of-work to proof-of-stake protocol. I conclude that the proof-of-stake protocol is highly likely to boost Ethereum prices. I also determine the most important transition variables to be the rate of slashing, the time when new issuance will end, and the amount of ether locked up in deposits. Using these variables, I develop a model for calculating the decline in supply of Ethereum under the Casper protocol.

In Section 5.1, I survey an altcoin proof-of-stake implementation. The NXT proof-of-stake method does not exhibit the same deflationary penalizing aspects of Ethereum's Casper protocol, which opens the door for security attacks without affecting supply. Section 5.2 covers the dynamics changing the structure of the ICO market. The ICO market is in a period of change as regulation and due diligence reach more heightened levels. The ICO market needs formalization to ensure investor safety and partially limit volatility.

This paper presents a markets based analysis on the technological and economic incentives behind cryptocurrency development. Further work is needed to determine the effects of confounding variables on cryptocurrency valuation. Specifically, economic variables that affect outsized valuations need to be studied. Bitcoin cost production can be modeled with larger datasets and more precise predictions. A more fine-grained analysis of bitcoin mining equipment would detail problems of centralization. Once Ethereum transitions towards a proof-of-stake consensus model, new data will be available to project and test impacts on supply and demand. Similar case studies could also apply to many cryptocurrencies with variations in protocol.

In conclusion, the technology behind cryptocurrencies is a new set of protocols for data transfer with economic incentives baked in for miners, users, and speculators. A sophisticated investor ought to take a long term view on market structure dictated by examining the technological challenges facing cryptographic assets. I build on and propose models for the cost production of bitcoin and the supply decline of ether to predict the impacts of consensus algorithms on cryptocurrency markets.

# 7 References

Bentov, Iddo, Ariel Gabizon, and Alex Mizrahi. "Cryptocurrencies Without Proof of Work." Financial Cryptography and Data Security Lecture Notes in Computer Science (2016): 142-57. Web.

[1] Bergstra, Jan A, and Peter Weijland. “Bitcoin: a Money-like Informational Commodity.” arxiv.org/pdf/1402.4778.pdf.

[2] Buterin, Vitalik. “Understanding Serenity, Part 2: Casper.” Ethereum Blog, 28 Dec. 2015, blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/.

[3] Buterin, Vitalik, and Virgil Griffith. Casper the Friendly Finality Gadget . Ethereum Foundation, 15 Nov. 2017, arxiv.org/pdf/1710.09437.pdf.

[4] Carlsten, Miles, et al. “On the Instability of Bitcoin Without the Block Reward.” Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS16, 2016, doi:10.1145/2976749.2978408.

[5] Conley, John P. (2017) "Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings", Vanderbilt University Department of Economics Working Papers, VUECON-17-00008.

[6] “Data.bitcoinity.org (Beta version).” Bitcoinity.org, data.bitcoinity.org/.

[7] Ethereum 2.0 Mauve Paper. Ethereum Foundation.

[8] Hayes, Adam. "Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin." SSRN Electronic Journal (2015): n. pag. Web.

[9] “ICO Stats | Track ICO Performance.” ICO Stats, icostats.com/.

[10] Li, Xin, and Chong (Alex) Wang. "The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin." By Xin Li, Chong (Alex) Wang :: SSRN. Decision Support Systems, 27 Oct. 2014. Web.

[11] Lubin, Joseph. “The Issuance Model in Ethereum.” Ethereum Blog, 22 July 2014, blog.ethereum.org/2014/04/10/th
issuance-model-in-ethereum/.

[12] Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. www.cryptovest.co.uk

[13] Naseer, Hunain. “NXT Set to Burst Ahead of IGNIS Airdrop This Month? It’s a Gamble.” Cryptovest, 14 Dec. 2017, cryptovest.com/news/nxt-set-to-burst-ahead-of-ignis-airdrop-this-month-its-a-gamble/.

[14] Proof-of-Stake FAQ. github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ. Accessed 17 Dec. 2017.

[15] “Reduce ETH issuance before proof-of-Stake · Issue #186 · ethereum/EIPs.” GitHub, github.com/ethereum/EIPs/is

[16] Saleh, Fahad. “Blockchain Without Waste: Proof-of-Stake.” Working Paper, 2017, people.stern.nyu.edu/fsaleh/JMP.pdf. Accessed 17 Dec. 2017.

[17] “Statement on Cryptocurrencies and Initial Coin Offerings.” SEC, 11 Dec. 2017, www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

[18] Yadav, Mohit, Exploring Signals for Investing in an Initial Coin Offering (ICO) (September 1, 2017). Available at SSRN: https://ssrn.com/abstract=3037106

[19] Zamfir, Vlad. The History of Casper - Chapter 5. 30 Dec. 2016, medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-5-8652959cef58. Accessed 17 Dec. 2017.