FINE 434: FinTech

Lecture 17

Professor Fahad Saleh

McGill University - Desautels

Assume security of Bitcoin

Does that make Bitcoin more viable?

Are there other economic concerns?

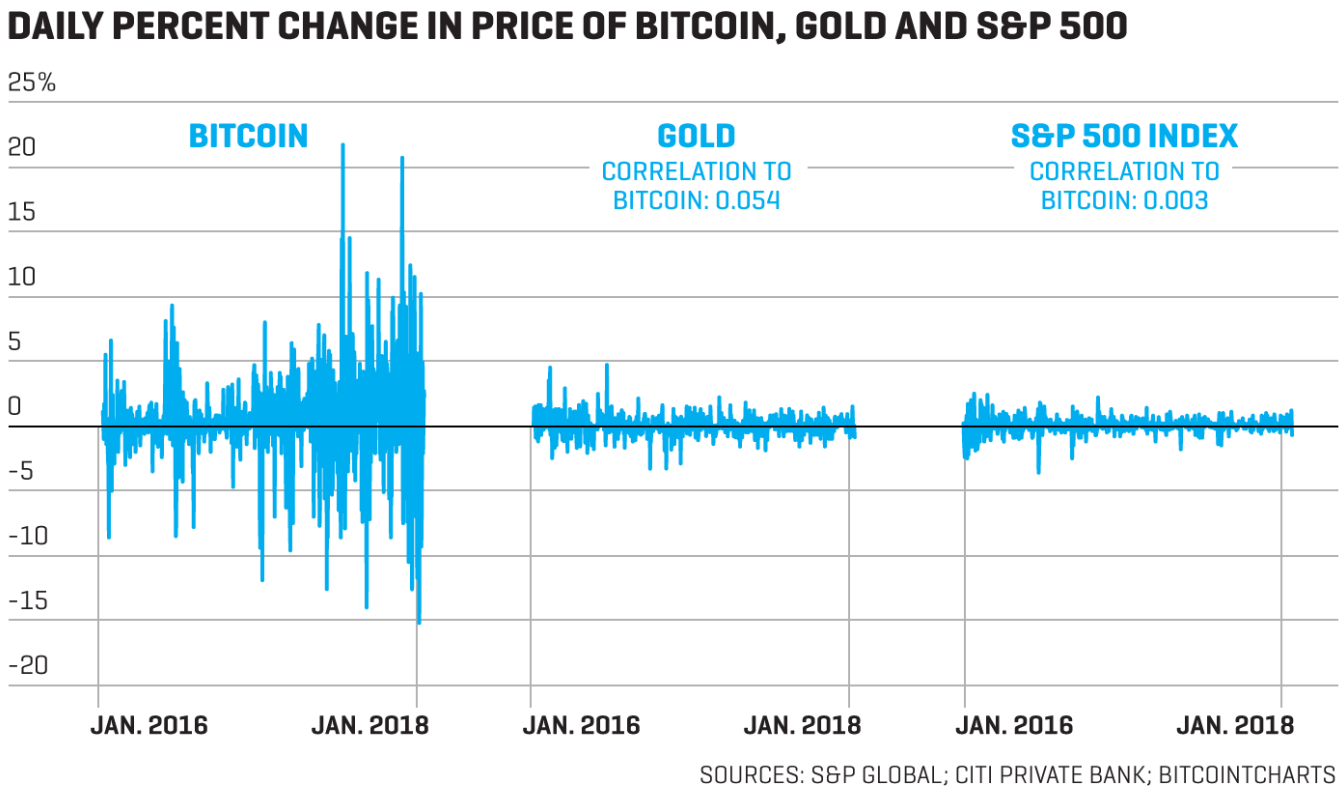
NBER WORKING PAPER SERIES

IS BITCOIN A REAL CURRENCY? AN ECONOMIC APPRAISAL

David Yermack

"Bitcoin has achieved only scant consumer transaction volume, with an average well below one daily transaction for the few merchants who accept it. Its volatility is greatly higher than the volatilities of widely used currencies, imposing large short-term risk upon users... Bitcoin appears to behave more like a speculative investment than a currency."

Volatility



Does BTC's volatility arise from infancy or underlying structure?

Supply and Demand

What makes BTC volatile?

Supply and Demand

What makes BTC volatile?

Demand
The Unity Property

Supply
A Passive Monetary Policy

Bitcoin as Decentralized Money: Prices, Mining, and Network Security

Emiliano S. Pagnotta[‡]

"unity exacerbates bitcoin price volatility"

The Unity Property

"verifiers are incentivized by the same asset that consumers use for transfers, a property that we label as **unity**."

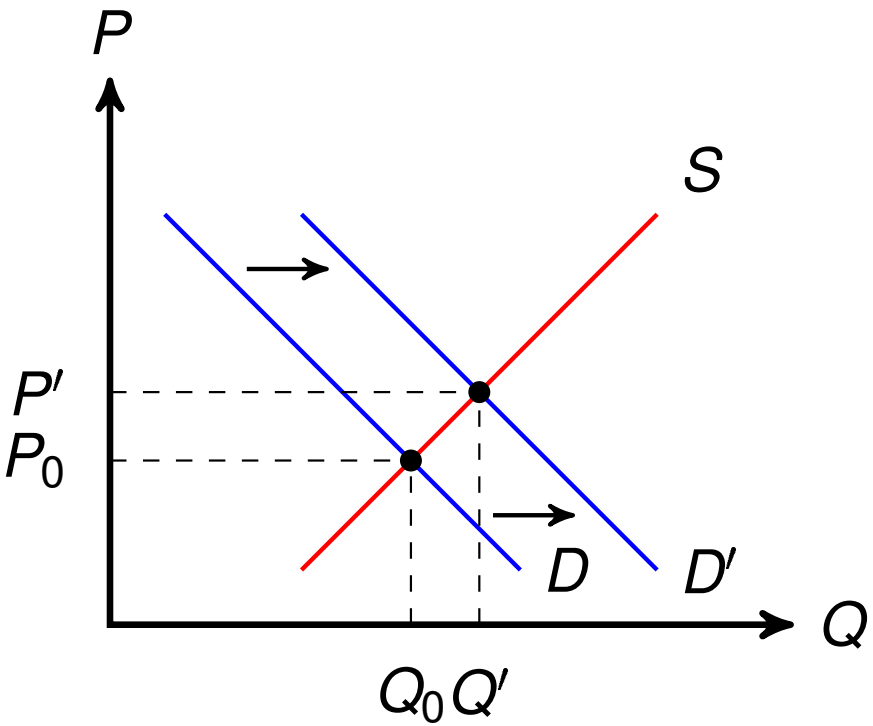
Network	Peer-to-peer	Multiple Verifiers	Free Entry Verifiers	Asset	Unity
Stock Exchanges, DTCC	n	n	n	Public equity	n
Bitcoin	y	y	y	bitcoin	y
Cryptocurrencies	y	y	y	Litecoin, Monero, Dash	y
Ethereum	y	y	y	ether	y
Ethereum	y	y	y	ERC-20 tokens	n
Ripple	n	y	n	XRP	n

Feedback Loop

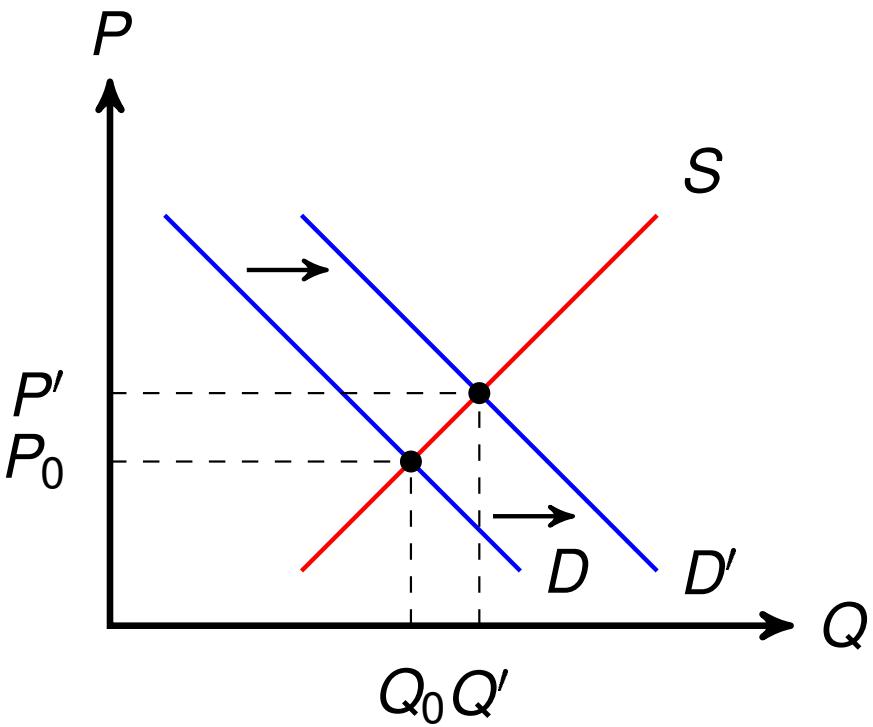
"an increase in the price generates a positive hash rate supply reaction and, thus, an increase in network security that feeds back the upward pressure on the price."

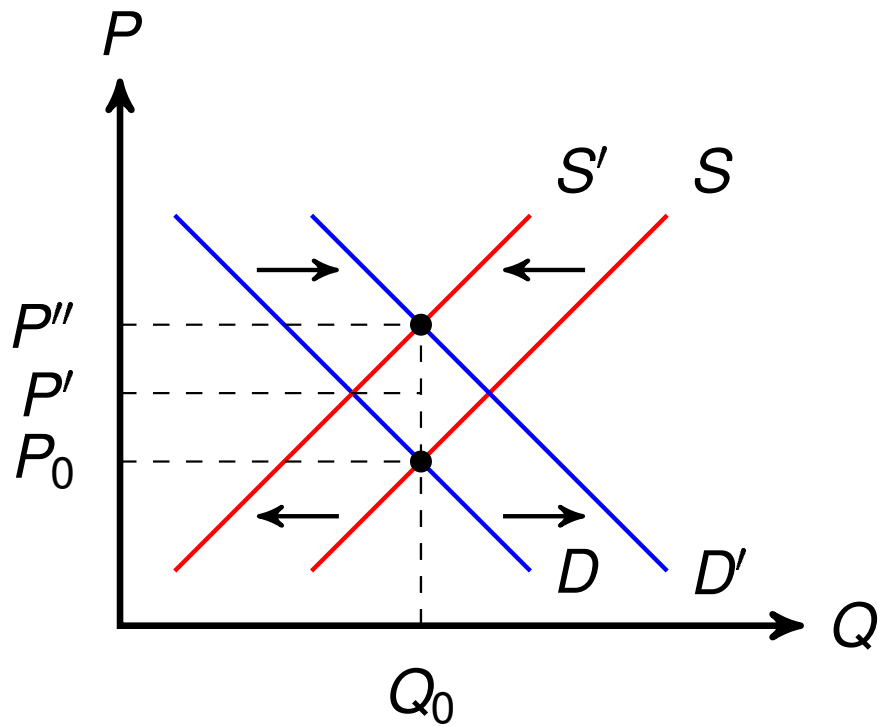
- Assumption: Consumers value security
- A price increase leads to increased mining activity
- Increased mining activity implies higher security
- Higher security further increases price

Proof-of-Work (PoW)



Proof-of-Work (PoW)





Difficulty Adjustment

What is Bitcoin's Difficulty Target and Adjustment?

Contents [Show]

Bitcoin's difficulty target is a 256-bit number that is adjusted every 2016 blocks (~2 weeks) based on the time it took to mine the previous 2016 blocks. The difficulty algorithm attempts to produce a block roughly every ten minutes and is proportionately modified by Bitcoin clients every two weeks to the amount of time higher or lower than it took to mine the previous 2016 blocks.

Difficulty Adjustment

What is Bitcoin's Difficulty Target and Adjustment?

Contents [Show]

Bitcoin's difficulty target is a 256-bit number that is adjusted every 2016 blocks (~2 weeks) based on the time it took to mine the previous 2016 blocks. The difficulty algorithm attempts to produce a block roughly every ten minutes and is proportionately modified by Bitcoin clients every two weeks to the amount of time higher or lower than it took to mine the previous 2016 blocks.

... what are the monetary implications?

Monetary Policy

New coins are produced only when a new block is mined

Targeting block times amounts to targeting monetary policy

e.g., 12.5 BTC per block and 10 minutes per block means 12.5 new BTC per 10 minutes irrespective of broader economic conditions

High Volatility

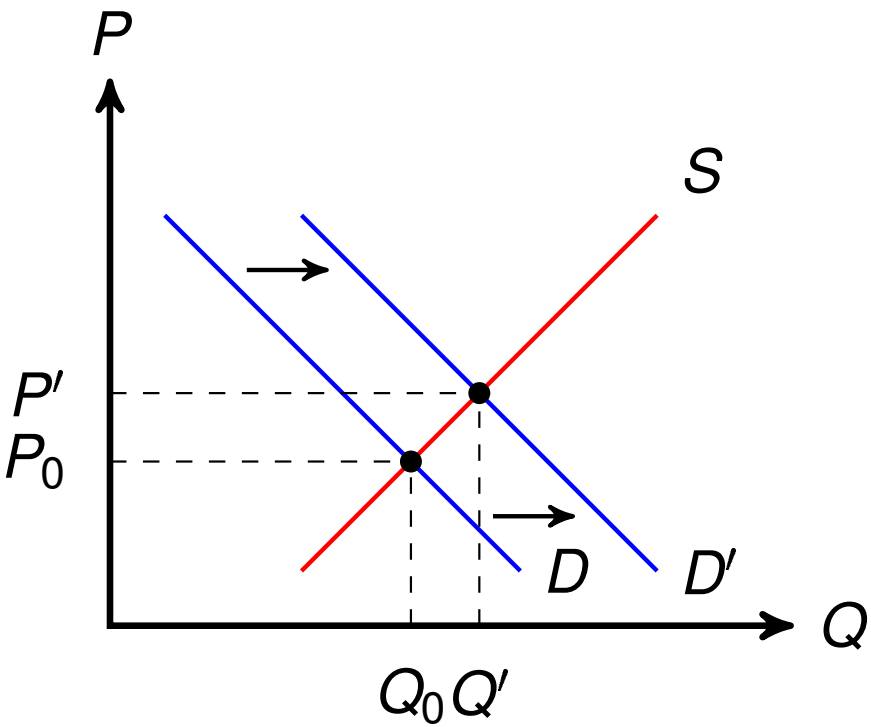
An Increase in Demand pushes up prices

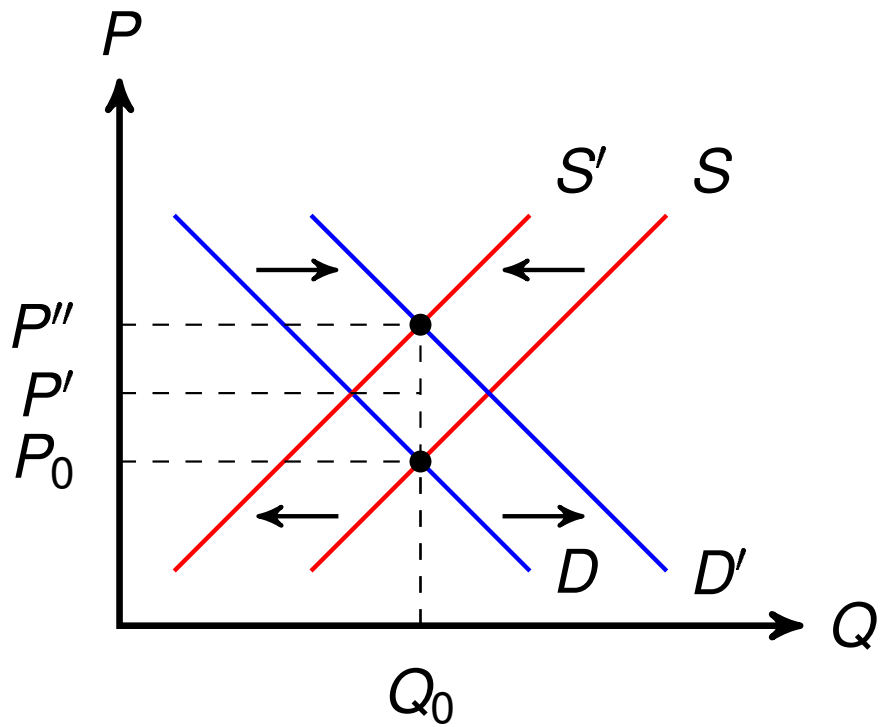
Higher prices should induce more mining and therefore more supply

The BTC protocol, however, increases difficulty of block discovery which discourages mining and keeps the rate of block discovery approximately constant

Prices, therefore, rise by more than without this adjustment

Take Two





Volatility and Welfare in a Crypto Economy*

Fahad Saleh†

McGill University, Desautels

December 22, 2018

Abstract

Proof-of-Work (PoW) blockchains possess at least two undesirable characteristics: exceptional price volatility and welfare impairment. Exceptional price volatility arises because PoW implements a passive monetary policy that fails to modulate cryptocurrency demand shocks. Welfare impairment arises because PoW compensates those updating the blockchain through seigniorage while facilitating free-entry among them. This paper theoretically formalizes the aforementioned points and also examines an alternative blockchain mechanism, Proof-of-Burn (PoB), that induces arbitrarily low volatility with arbitrarily enhanced welfare. PoB implements an active monetary policy that modulates cryptocurrency demand shocks. Further, PoB employs a similar incentive structure as PoW but induces welfare gains by supporting cryptocurrency prices with blockchain updating expenses. This paper demonstrates that PoB maintains desirable PoW-characteristics such as free-entry and a deflationary monetary policy but does so without inducing undesirable PoW-characteristics such as exceptional volatility and welfare losses.