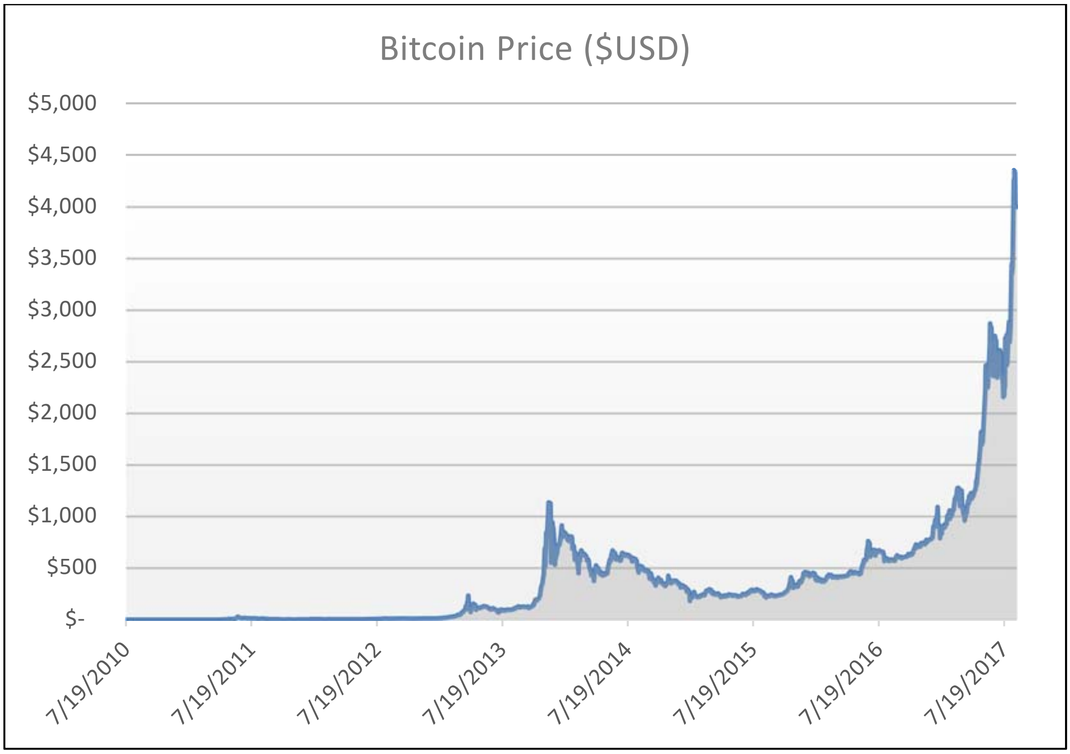
Lynx
Investment Advisory

Bitcoin Cryptocurrency

This whitepaper aims to introduce readers to Bitcoin cryptocurrencies through an exploration of: how the major elements of the Bitcoin system function, a comparison with existing currencies, and the prospects for cryptocurrency development and adoption.

Bitcoin was theorized in a research paper published October 2008 by Satoshi Nakamoto. The author's name proved to be a pseudonym, and the creator's identity remains a mystery to this day. Bitcoin uses digital encryption to enable secure global transactions via the internet. Fiat currencies such as US dollars, Euros, or Yen, are issued by national governments or their central banks and declared a legal medium of exchange, but are not redeemable for gold or silver. In contrast, Bitcoin is not issued by a central authority and has no central point of control. Bitcoin has been one of the best performing assets over the past few years, doubling many times over. These rapid price increases and increased media attention has spurred public interest in Bitcoin.



[1]

The infrastructure of the cryptocurrency systems consists of several pieces which work together to enable the system to function. These include a blockchain, wallets, transactions, and the presence of mining.

A blockchain is a ledger of all transactions since the creation of the currency which is entirely public and viewable on the web. The blockchain lists the time, amount of the transaction, sender, and recipient by their wallet address, a string of numbers and letters. E.g. one wallet address for

[1] BTC/USD price via Bloomberg

Wikipedia New York City is "1PC9aZC4hNX2rmmrt7uHTfYAS3hRbph4UN". In this way, the ledger publicizes all transactions between addresses, but the addresses are not immediately identifiable by real name or other personal details. One individual or organization can create unlimited addresses linked to the same wallet as a way of anonymizing their activities.

Wallet software and websites allow one to transact in cryptocurrency and hold the private key, or password, needed to send coins. Sending coins is irreversible in the same manner as physical cash transactions. If a wallet is lost, such as through the destruction of a computer containing the only private key, the coins are 'lost' in the same way physical cash can be lost or destroyed.

Mining is the process by which the blockchain is updated and Bitcoins are created. Mining involves setting up computers to solve difficult math problems for which the answer is time consuming to compute, but easy for the other network participants to verify as correct. Once a miner solves a problem, and the answer is verified by the network, new Bitcoins are created and deposited in the miner's wallet. Over time, the difficulty of the problems increases, and the amount rewarded is halved. Initially, it was feasible to mine Bitcoins on a personal home computer. As the difficulty has increased mining is only economically viable using purpose built computers. Due to the large electricity consumption these computers require, Bitcoin mining businesses operate in places with inexpensive or government subsidized electricity, mainly northern China. The total number of Bitcoins that can be created is currently limited to just under twenty-one million. This limit can change only with the consensus of greater than fifty percent of the network, which is extremely unlikely given it would devalue existing Bitcoin holdings. In this respect, Bitcoin resembles gold more so than fiat currency which governments can create at-will to an unlimited extent.

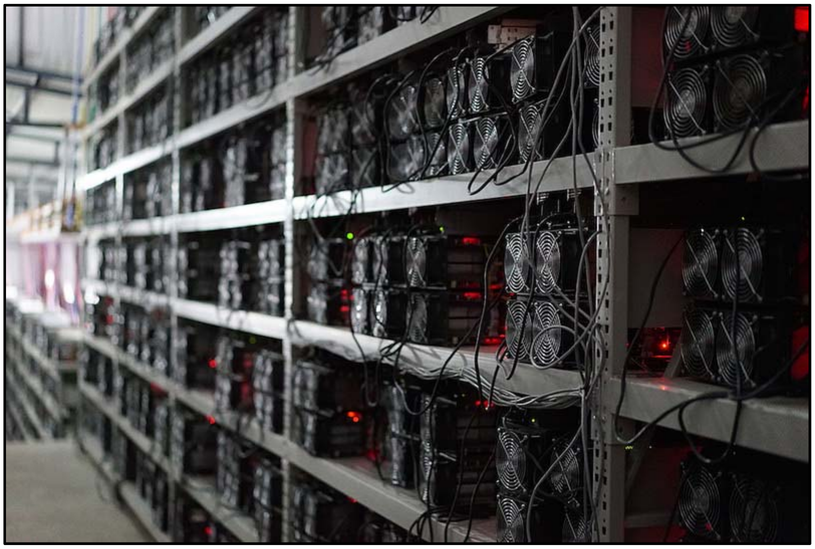


Figure 1: Computers in a Chinese Bitcoin mine

China mines more Bitcoins than any other nation partly due to the abundance of inexpensive hydroelectricity.[2]

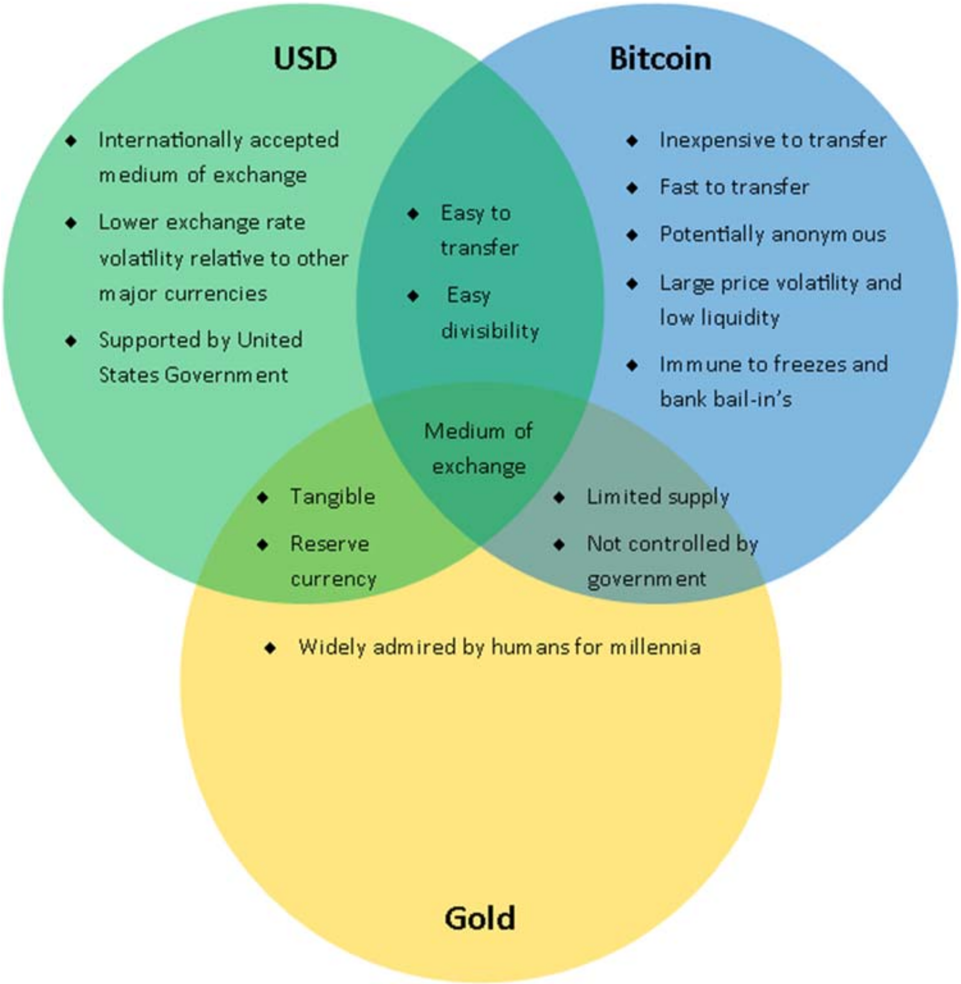
A large part of the appeal of cryptocurrencies is the possibility to offer a medium of exchange and financial transactions free from government control and restrictions. Chinese nationals who wish to transfer money abroad are limited by capital controls from exchanging large amounts of Renminbi

[2] CoinDesk: My Life Inside a Remote Chinese Bitcoin Mine

for US dollars or other foreign currency. Bitcoin provides a way to skirt these capital controls and transfer unlimited funds worldwide in minutes, which are then exchanged for foreign currency.

In hyperinflationary economies people have sought ways to protect their purchasing power using mediums of exchange other than the national currency. In 2017, Venezuelans have embraced Bitcoin to purchase daily necessities and protect their savings from hyperinflation.[3] In addition to circumventing capital controls and protecting against hyperinflation, a currency free from government seizure is attractive to those who wish to avoid suffering from bank bail-ins. A bail-in occurs when an insolvent bank is recapitalized using the funds of depositors rather than taxpayers. Depositors lose a portion of their deposits such as occurred in 2013 in Cyprus.[4]

Given the inability of governments to control transactions and determine who is behind a wallet address, Bitcoin has been employed in the sale of illegal drugs. The most notorious example was the 'Silk Road' online marketplace which generated over one billion dollars in sales before being shut down by the FBI in October 2013.[5]


USD
Bitcoin
Gold
◆ Internationally accepted medium of exchange
◆ Lower exchange rate volatility relative to other major currencies
◆ Supported by United States Government
◆ Easy to transfer
◆ Easy divisibility
◆ Inexpensive to transfer
◆ Fast to transfer
◆ Potentially anonymous
◆ Large price volatility and low liquidity
◆ Immune to freezes and bank bail-in's
Medium of exchange
◆ Tangible
◆ Reserve currency
◆ Limited supply
◆ Not controlled by government
◆ Widely admired by humans for millennia

[3] Bloomberg News: Venezuelans Are Seeking a Haven in Crypto Coins as Crisis Rages
[4] Bloomberg News: Fleeing the Euro for Bitcoins
[5] WIRED Magazine: The Untold Story of Silk Road

Several steps are necessary if Bitcoin's proponents wish to improve its reputation among the public and gain legitimacy and approval from regulators, major financial institutions, and governments. A report from the British Treasury department noted the lack of a regulatory framework and the resulting reluctance of traditional banks to work with cryptocurrency related businesses as a barrier to digital currency firms.[6] Many businesses and individuals have launched initial coin offerings of new currencies linked to their software or crowdfunding projects. The US SEC has issued a warning regarding the potential for fraud related to these largely unregulated initial coin offerings.[7]

Steps to register and regulate cryptocurrency exchanges in a similar manner to existing foreign currency exchanges would improve their credibility and legitimacy. The increased price transparency and liquidity of regulated exchanges would likely lower Bitcoin's high price volatility. Major companies including Starbucks, Expedia, Dell, Microsoft, and Dish Network have begun accepting Bitcoin payments. Currently, these Bitcoin transactions involve the businesses converting Bitcoin to US dollars immediately upon receipt. Governments around the world are making strides to register and regulate Bitcoin related businesses. Whether Bitcoin can stand independently as a viable major currency, rather than simply a transfer method with immediate conversion, thus replacing global fiat currencies remains to be seen.

At this juncture, our team is following and researching developments related to Bitcoin and blockchain technology, but remains uncommitted in terms of investment as the future regulatory landscape of these technologies is far from certain.

[6] HM Treasury: Digital currencies

[7] SEC.GOV: Investor Bulletin: Initial Coin Offerings