WEALTHSPIRE ADVISORS

WHITEPAPER | February 2018

The Cryptocurrency Question

Dmitriy Katsnelson, Deputy Chief Investment Officer

The Cryptocurrency Question

Dmitriy Katsnelson, Deputy Chief Investment Officer

The most common financial question that we have been asked over the last six months or so relates to Bitcoin[1] (or any number of other cryptocurrencies). *Is it real? How is it valued? Should we invest in it? Can it keep going up in price?* The answers to these questions are not easily answered, are complex, and are dynamic over time.

To start, *Crypto* comes from the Greek *Kruptos*, which means "hidden." Because of the complexity of the subject matter, we would prefer to hide from making an opinion on cryptocurrencies in general. However, they (and the technology surrounding them) are increasingly relevant in our world and worthy of some further discussion. Since it is difficult to pin down all the salient arguments surrounding blockchain and cryptocurrencies in this forum, what follows is a high-level review.

THE ORIGIN STORY

The first iteration of what is now called cryptocurrency was developed around 2008, near the height of the financial crisis. The founder(s) of Bitcoin wanted to create a secure digital currency[2] that was not controlled by any central bank, government, or hegemon. Because it was not centrally controlled, it would be incorruptible (no QE, no repatriation, etc.). It would act as a currency in that it serves as a means of exchange, store of value, and unit of account.

WHAT IS BLOCKCHAIN?

Any conversations surrounding cryptocurrencies must start with blockchain. In its simplest definition, blockchain is a digitized and decentralized public database or ledger.

- "Digitized": It is not physical or tangible as it all resides in computer code and on computers across the world.
- "Decentralized public database": It's probably easier to imagine the opposite, which is a centralized private database. This is the backbone of pretty much every system that stores information today. Your bank keeps all transactions of its users in a private database that only it can access. Facebook has all of your personal information sitting in its own database, that is also centralized and private. A decentralized public database means everyone has access to the information and it's not under the control of one, centralized power.

The Olympics provide a good analogy. Every major country sends television crews and reporters to document the happenings and post medal counts at the end of the day. No one country or television station owns the information, and each is responsible for maintaining a record in its own database. It is not the most efficient route, but it works, and if there are discrepancies, they can cross reference each other's counts to get the right result. It is public and decentralized.

WHAT IS A CRYPTOCURRENCY AND HOW IS IT USED?

Cryptocurrency uses the blockchain structure as a mechanism to track and compensate users for facilitating transactions. To illustrate how this process plays out, let's contrast it with a traditional financial transaction.

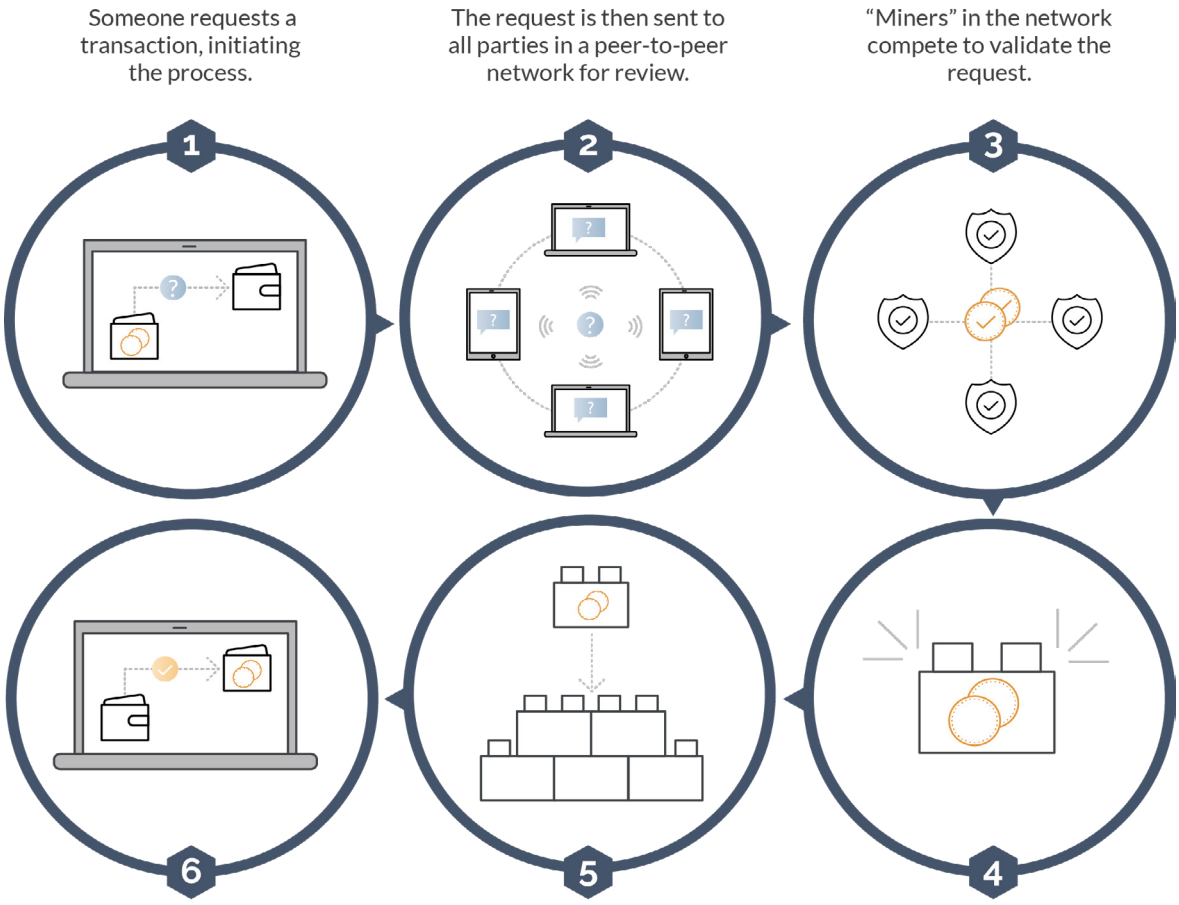
In a traditional paradigm, I want to buy a Go Team USA shirt for $20 using a debit card at retailer XYZ. The card company is responsible for making sure I have enough money in my account to cover the transaction, verify the transaction, keep a record of it, and is also responsible for keeping all of my and XYZ's account information private. In exchange for convenience and for the work of reconciling the transaction, they collect a percentage of the transaction value.

Now let's say I want to buy that same shirt with cryptocurrency, and for the sake of argument, let's call that currency OLYcoins. Instead of notifying a centralized intermediary, i.e. debit card company, a note is sent to the entire network of OLYcoin users saying that I want to send 20 OLYcoins to retailer XYZ. Anyone who can do the work ("miners") to verify the transaction ("mining") gets compensated the same way that a card company does for doing very similar work. That transaction is logged and then verified by other users. My account will have a debit and the retailer will have a credit of OLYcoins that was confirmed and reconciled by multiple people, not just one card company. The chart below is a good visual of the process:

The verification process ("mining") works more like a lottery than a first-come-first serve queue. The miners must solve a complex cryptographic problem to win the right to reconcile a transaction (remember that this is how they get paid). This is to make sure that no one party is verifying all of the transactions. This information and activity is encrypted with multiple layers, protecting each transaction and each user at every step (miners cannot know who the actual senders and receivers are).

When enough transactions occur, they get logged into the public ledger (this is adding blocks to the blockchain) which subsequently becomes the latest iteration of the chain and the basis for every subsequent transaction.

The Blockchain Process



Rinse and repeat. The process is obviously less efficient than the traditional debit card approach since it requires thousands (if not millions) of parallel databases running across the globe. This also requires a significant amount of energy to sustain, which we will touch on at the end. In other words, blockchain is purposefully creating an inefficient process to remove a centralized agent from the equation.

WHERE DOES THE CURRENCY COME FROM?

Unfortunately, this is not the same for every cryptocurrency. In the case of Bitcoin and similar protocols, new coins come into being only when a miner verifies a transaction. In other words, in the beginning, there were no coins. The first coin was issued upon the reconciliation of the first transaction. That process has continued since, with coin awards adjusting over time. This is the only mechanism for creating new coins under this protocol. Other protocols exist, such as ones that are facilitated by ICOs (Initial Coin Offerings), but they fall outside the scope of this missive.

APPLICATIONS

Blockchain technology applications are countless and are being explored by a variety of public and private sector users. What should be understood is that the computer code behind blockchain is "open-source". No one owns blockchain in the same way that no one owns the internet or internet protocols such as HTTP. So, although applications may arise that generate lots of dollars for those successful in commercialization, it will not be from someone selling the blockchain code itself.

ARE CRYPTOCURRENCIES WORTH ANYTHING?

In a vacuum (assuming no outside forces like regulation, taxation, government intervention, etc.), there are several proposed ways of pricing cryptocurrencies. We say this a bit tongue-in-cheek since we do not believe cryptocurrencies will be able to operate unchecked. Here are a few examples of pricing strategy:

- **Value it like a commodity** - What is the cost of mining plus profit margin? For cryptocurrencies, it is the cost of setting up a mining facility (hardware, electricity, overhead, margins, etc.). Similarly, a gold miner must take into consideration the cost of the land, equipment, people, energy, financing, etc. before opening a mine. It does not mean the commodity will trade anywhere near that cost, but it at least shows the price necessary for a miner to continue operations. Without miners, there is no ongoing transaction verification, so it's a worthwhile exercise.
- **Value it like a currency** - This valuation comes from a broader macro-economic standpoint and uses the equation of exchange and the quantity of money theory[3]. This is again completely theoretical and requires one to assume the quantity of cryptocurrency that the world requires (i.e. underworld, persons in countries without banking or supportive ownership laws, etc.).
- **Value based on medium of exchange** - This pricing focuses specifically on remittance transactions[4]. The argument is that cryptocurrencies can do it cheaper than traditional channels. Here, one calculates the addressable market of money transfers through systems like SWIFT, CHIPS, and Fed wire, and calculates what happens if cryptocurrencies can take on part of the volume, and subsequently collect associated fees.

We are not subscribing to any of the above but wanted to provide a bit of color on how folks believe the currencies should act when viewed purely from a theoretical perspective.

BIG QUESTIONS

- **Regulatory** - There are many ways regulations could come into play, from taxation, to illegality, to oversight, to confiscation (to those that do not believe the US government is capable of confiscation, look at Executive Order 6102, where in 1933 US citizens were forced to exchange their gold for $20.67 per oz.). Central banks can also launch their own cryptocurrencies, an idea that has been discussed domestically and abroad. It is unlikely that governments will have zero reaction to the market novation. Every country is at a different stage in how it is approaching cryptocurrency, but in aggregate the oversite is weak[5].
- **Barrier to entry** - There are now roughly 1,500 different cryptocurrencies traded on more than 8,000 markets. The aggregate market cap is around $600 billion dollars. The code to create your own is free. This is one of the big questions out there, since anyone can (and many do) create their own currencies every week. Although everyone is still looking at bitcoin as the de-facto behemoth, it now makes up only 33% of cryptocurrency value vs. 80% a year ago.

- **Security** - This is not a question of the blockchain itself, but of the many custodians/exchanges that have popped up as facilitators of cryptocurrency activity. There have been countless small, and several very large, exchange heists in the past few years including:
  - $530 million from Coincheck (2018)
  - $480 million from Mt. Gox (2014)
  - $155 million from Parity Wallet (2017)
- **Not all cryptocurrencies are the same** - Some newly launched cryptocurrencies operate under sets of rules that create potential for manipulation. For some nascent currencies, concentrated actors control a significant amount of computing power or ownership, creating questions about code and system oversite. Even with coins like bitcoin, the concentration of miners in countries with differing rules of law (China accounts for nearly 70% of cryptocurrency mining capacity) is a concern.
- **Sustainability** - The sub-group of cryptocurrencies that depends on proof-of-work to facilitate transactions is a large consumer of energy. In exchange for decentralization, these systems require a significant amount of computing power, which at this point is making a sizable dent in global power demand. According to digiconomist.net, one bitcoin transaction uses more power than 100,000 Visa transactions. In aggregate, bitcoin mining alone is estimated to consume more electricity than Nigeria or Hong Kong. As the difficulty of transaction reconciliation rises, the amount of power will as well.

SUMMARY

In summary, we are not dismissing cryptocurrencies as just another fad. We just do not have enough clarity around the above questions to rationally allocate to the nascent idea. As we mentioned in our last quarterly letter, there are components of this craze that are very much bubble-like. In some cases, even using the make-believe vacuum valuation methods, current prices appear unsustainable.

For the average person in a developed country that has a robust rule of law, cryptocurrencies seem like a solution searching for a problem. Yet, for nations where the rule of law varies depending on the day and property rules are illusory, cryptocurrencies have created another avenue beyond hoarding precious metals or USD bills in a mattress. The issue lies in the fact that those methods still have the support of global governments, are tangible, and cannot be easily replaced without overcoming significant economic hurdles.

The evolution of blockchain and cryptocurrencies is one that we continue to monitor, but until there is clarity around the most salient questions, it will continue to be something we review from afar.

Footnotes

1 The standard is upper case B for the protocol and lower case for currency.

2 Digital money and cryptographic protocols are not new. DigiCash had anonymous transactions behind a cryptographic protocol going back to the late 1980s and early 1990s, before the internet was what it is today.

3 MV=PQ: where M = money supply, V = velocity of money, P = price level, Q = economic output. PQ = nominal GDP.

4 Remittance is a transfer of money by migrant workers back home. Global remittances neared $600 billion in 2016 according to the World Bank.

5 Country by country cryptocurrency oversite summaries may be found here - https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html