HORIZON KINETICS

Cryptocurrency Global Open Floor Idea Exchange – Real Questions from Real People
(December 2017 - An Ongoing Series)

Global Open Floor Idea Exchange – Real Questions from Real People
In recent months, we have received a wide spectrum of questions, feedback and ideas from people around the world, some of whom were previously unknown to us, and of course from clients as well. The former often arrive at our general email address info@horizonkinetics.com. Many of these correspondents have questions about a topic that they haven't asked before, or have heard answered incorrectly, or don't even have the technical knowledge to ask explicitly but would be pleased to hear it asked and answered. We enjoy this sort of correspondence. These questions address issues that challenge us all, and are valuable to share about the increasingly controversial topics of cryptocurrencies and investment diversification, valuation and risk. We will periodically publish these Q&As and we thank our interlocutors for their permission to share these exchanges with our clients, partners and readers.

Series of Q&A with a Financial Advisor at a Bulge Bracket Brokerage Bank based in New York, NY:

Question #1*: You seem to be relatively neutral on the various forks, which is somewhat atypical as many folks seem to be very passionate in their opinions of BTC versus BCH, and now BTG to a lesser extent. Is that for the sake of being objective on the call or do you have a particular preference, as the long-term implications seem like they might lead us to very different places?*

Answer: Okay, so the first thing to understand is that people are passionate in their opinions because they view these forks as competing technologies. At the moment, they are different protocols, but they forget that this is all open source code. So, if and when one protocol becomes distinctly superior to the others, the others will use those elements of superior protocol to improve their own. There is no long-term competitive advantage to be had by any fork insofar as superior protocol is concerned. Anybody is totally free to copy anything from everyone.

At the end of the day, they're all going to have comparable protocols. Since they have comparable protocols, they're going to have comparable value because their value is going to be based on the fact that they all have the same monetary policy. I don't think there are any significant differences among them. For those who are willing to wait a while, it might not be a bad idea to buy each fork that is created and reconstruct the bitcoin that existed with each fork. If you had bought a bitcoin originally, and you received the forks and held them, that's what your position should really look like because it's unclear what's going to happen day by day. At the end of the day, all the forks should have a comparable value.

Question #2*: Are you concerned that the forks reduce hash power and each blockchain is theoretically less secure and more susceptible to attack?*

Answer: The short answer is no, I'm not concerned, because the hash power is not finite. The hash power in the very short term is close to finite in that it takes a certain amount of time to create new mining equipment. But new mining equipment is being created, as are new miners. In the world of ASIC mining, which stands for Application-Specific Integrated Circuits, we're reaching certain physical

limitations with respect to how fast they can be, but we're not reaching those limitations in GPU, which is Graphics Processing Units.

In any event, more equipment is on the way and within a few months each currency will have more purchasing power and more nodes. When new mining equipment is installed—we know something about this—you don't just put new nodes on a network. Even before installation, we sometimes have to wait 90 days to get equipment. And even when you receive the equipment, you have to find suitable locations to host it. It then has be set up and tested, which takes some time. For new currency forks, you don't create the requisite amount of hash power to mine it in 24 hours, because the equipment for that new currency hasn't been manufactured yet. Demand exists first, and the equipment follows in fairly short order.

Question #3: *Do you have any concerns about the ability to attack each blockchain, particularly after a hard fork which splits the miners? Are you concerned about the ability of the National Security Agency (NSA) to mess with it? Most people seem more concerned about computational power, but it seems to me that the NSA could fairly easily break the blockchain since they have access to a virtually unlimited amount of fiat currency. They can simply buy coins slowly over time and then sell all at once to drive a lot of volatility. Miners would likely switch to a more predictably profitable currency, which would allow them to combine it with a 51% attack.*

Answer: If I could take the liberty of condensing the question into a single sentence, the question is really asking: Will the National Security Agency or some other government actor with access to a lot of processing power declare a cyberwar against one or more cryptocurrencies with the idea that they would like to invalidate the concept of cryptocurrency and preserve fiat?

There are two answers to that question. First, even if all the governments in the world were to unite, they wouldn't have anything like the number of people who can invent new cryptographic protocols. They could attack a given cryptocurrency for several days if they theoretically had enough processing power, but they'd be declaring war against the world of cryptography, which is made up of millions of people. So, there would be counteracts.

The U.S. government has a limited number of specialists in this realm, while the globe has an incalculably greater number. As powerful as the U.S. government is, it would be like Bermuda going to war with NATO. There would be unlimited retaliation. I don't think the U.S. government wants to invite that.

The riposte might be that somebody, in their anger, might attack the Social Security Administration, the Medicaid system, or the electric grid. I don't know why anyone would want to risk that kind of retaliation. I don't believe the U.S. government has enough resources to be able to protect against every conceivable counterattack. They have no idea who these people are. Some of them who are into cryptocurrency might even work for a national security agency.

If you're going to set off a cycle of retaliation, you better be absolutely sure that everybody in the agency is perfectly reliable. If one human being is not reliable or finds this attack objectionable, who knows what information they might release to the world of crypto? It would be an incredibly dangerous and irresponsible thing to do. At the end of the day, even if they could do it, it wouldn't be successful, because there are already well in excess of 1,300 cryptocurrencies, and there could easily be 13,000 or 130,000, and the governments will never have the resources to be able to control them all.

It's the same problem that governments encounter in any effort to control something the populace wants. There is no case of a government controlling its currency successfully. There are instances in which governments adopt exchange controls to keep money in the country and they exact severe penalties for disobeying government regulations. Nevertheless, the black market always wins. Even today, in North Korea there's a black market in North Korean won vis-à-vis U.S. dollars. You can see it on the internet. Is there any government on the planet that's willing to be more ruthless than the government of North Korea? If there is, I'm not aware of it, and it can't even control its own North Korean won. So, how can the U.S. government control cryptocurrencies?

By the way, the internet is only one way to transmit cryptocurrencies. Theoretically, they can be transmitted through microdots. Or, there could be an alternate net that is known to only a few and that could be secured. There could be tiny storage devices the size of a pin that pass from hand to hand. At the end of the day, the algorithms are just algorithms. What are they going to do? Do you think they can look at every computer on the planet for algorithms they don't like? I think it's quite beyond their resources.

Question #4*: I'm not sure I follow the logic behind valuing cryptocurrencies. I have heard a lot of comparisons between the market value of gold/precious metals and cryptocurrencies. I think the argument there is it gives us an order of magnitude (priced in fiat) of the demand for a store of value. I'm not sure I follow why all the fiat currency might be the potential value for all the cryptocurrencies. At the end of the day, the U.S. government is in a perfect situation where it has assets (tax revenue) denominated in the same currency as its liabilities (treasury bonds and entitlements). It seems to me that the portion of the U.S. economy (and similarly for other countries) would always stay in fiat so you wouldn't reduce that amount of value that could go to cryptocurrencies.*

Answer: There are two main questions here. The first is that you can't compare the value of the assets that the U.S. government might command with the value of the currency as if it were a stock, because it has nothing to do with it. To prove that, consider any of the studies that have been done, especially the one in a book by Elroy Dimson called *Triumph of the Optimists: 101 Years of Global Investment Returns*, and you'll see that, given enough time, just about every fiat currency loses its value. A typical fiat currency—and I'm doing this based on my experience, so you can question this—a typical fiat currency loses most of its value within three decades.

The Italian government, for example, had a lot of assets, and it certainly had the ability to tax the population; nevertheless, from the end of the Second World War to the final establishment of the euro as a replacement for the lira, the lira lost most of its value. The lira's value had nothing to do with the assets of the government; rather, its value had to do with its purchasing power, which has to do with the number of units of lira outstanding. The greater the rate of inflation, the more the currency falls in value.

The Federal Reserve states that its goal is to have about 2% inflation. I believe that the inflation rate since the Federal Reserve was established in 1913—and despite that we had a depression during which we had deflation—is something like 2.16%. So, in 104 years, the U.S. dollar has lost 97% of its purchasing power. That's a fact that no one can deny. There are even some who would say it has lost a bit more than that. But does it really matter if you lose 97% of your value, 99% of your value, or even 100% of your value? Those differences really lie in the fact that there are different ways of measuring inflation. We'll be debating forever about which is the proper way to measure inflation, but the fact remains that

the currency lost its purchasing power, despite the immense growth of U.S. government assets and its ability to collect tax revenue being astoundingly greater than it was in 1913.

Those facts should put to rest any idea that the currency is backed by something. Currency is backed by nothing. It's not a store of value in the conventional sense of the word. It doesn't earn anything. It's not like a corporation that has earnings. The U.S. government might have a lot of tax revenue but you don't get to share in it just because you happen to have a dollar in your wallet. You're not entitled to anything other than the dollar as legal tender. The government keeps creating more units of currency, and the more units it creates, the faster it loses its value.

The idea behind bitcoin is that it won't lose its value, because there's a finite limit on the number of units that will be created and we know what that limit is. In the case of bitcoin that number is 21 million and currently there are just over 16.7 million. It is known that in the year 2140 there will be 21 million bitcoin and the market has already discounted that knowledge and absorbed whatever the issuance is going to be. But in the case of fiat currency we have no idea what the issuance will be.

Consider the difference between the U.S. dollar and bitcoin in terms of bitcoin having no government behind it and no authority to collect tax revenue, as opposed to the U.S. dollar, which not only has both, but also has land and many types of other assets. Those differences would be real factors if the dollar actually paid you. Those assets and authorities would be a factor in government bonds if you're interested in getting a certain rate of interest, but they have nothing to do with the value of the simple currency.

If bitcoin is a better store of value, then it should have more value than the fiat currencies of the world—you have to add up the value of all the fiat currencies in the world. The question to consider is whether you would prefer having a currency that loses value or one that doesn't lose value. But somehow the paradigm is set up to ask whether you would rather have a currency with government backing, tax revenue, and assets behind it, or one that has none of those attributes. The critical word in that question is "behind," because you don't get to share in the benefit of those features in any circumstances whatsoever. A dollar doesn't entitle you to a share of the U.S. government revenues and, therefore, its only value is based on how many units it has outstanding. So, the comparison is units outstanding vis-à-vis units outstanding, not assets versus lack of assets.

Question #5: *Are you worried about how easy it is to create new cryptocurrencies and how might that affect the value in the future?*

Answer: Bitcoin has the first mover advantage. For the people who created it, it was a labor of love—which means the programmers did not work in exchange for compensation—and now it has the lowest inflation rate and the highest market value. That low inflation rate provides the miners with a fairly large incentive compared to mining a new currency that has to have a much high inflation rate to offer the same incentive. Ethereum, for example, has a much higher inflation rate than bitcoin. There's no reason Ethereum couldn't make its inflation rate lower than bitcoin's but, if it did, it would have a lot less revenue with which to compensate the miners. Less revenue would be a problem, because it would attract fewer miners, and it is the miners who support the blockchain and, through their numbers, provide the blockchain's security. The more miners there are running the distributed ledger, the more difficult it is to hack the system.

The new cryptocurrencies try to have technical faculties that bitcoin doesn't have, which should induce people to use it, and it does. But, as a store of value, they pretty much uniformly have far higher inflation rates than bitcoin, which hurts their value. If you go out enough decimal places, you can see that every ten minutes twelve and a half bitcoin are issued, and with that the bitcoin inflation rate falls, because it's approaching its cap at 21 million bitcoin.

Question #6: *Have you heard of Bitwise's Hold 10 crypto index fund? I met the two young guys who started it, and they're smart guys. I tried to explain to them the danger of using a passive strategy on a horribly inefficient market like cryptocurrencies, but they are launching it anyway. I wonder if you see any risk of passive strategies causing problems in the cryptocurrency markets. It seems to me that a strategy like HOLD 10 will be highly susceptible to manipulation by institutional investors who will exploit the weaknesses in its indexing methodology. Is there any concern that certain types of behavior will draw unnecessary attention from regulators?*

Answer: Since there are several questions here, I'll break them up.

Passive strategies: indexation of certain cryptocurrencies

The first problem with a passive strategy is that you have to make a lot of decisions. How do you weight the various currencies in the index? Do you weight them by market capitalization, or will it be float adjusted? That brings us into certain physical limitations about having a passive strategy at all, because if there's enough money in it to make it worth manipulating, then adequate float becomes an issue. How much float is there?

You can see at any given second how many bitcoin exist, but you don't know what the float is or even how to define it. You don't know how much bit rot there is, meaning how much bitcoin is on the blockchain for which the owners have either lost their private keys or that is no long accessible for any number of other reasons? You don't know how much bitcoin is in the hands of long-term holders who have no interest in selling whatsoever. Since you can't know these parameters, you have to go with market capitalization. But if you go with market capitalization based weighting scheme, that's very dangerous, because if there's a large enough inflow into the fund, you might not be able to buy enough bitcoin at a reasonable price.

It's not a question of someone exploiting the index, but that the index might not even be able to do what it wants to do. If it has a tiny flow, it's irrelevant; if it has a very large flow, it might not even be able to implement what it wants to do. An example of that in stocks is Nippon Telegraph & Telephone (NTT). In the late stages of the Japanese bull market of the late 1980s and early 1990s, NTT became public, but most of its shares were owned by the government. Its index weight was based on its market capitalization, not float, so there was no way to physically buy enough shares to actually get you to the right weighting, given the amount of money that was indexed. It physically couldn't be done. Therefore, NTT had a very high valuation. But even the high valuation wasn't necessarily the biggest problem; the biggest problem was that it was impossible to physically implement indexation in Japan, which is one of the reasons they chose the float method. Eventually, the float method dominated all indexation, which ultimately created other problems.

In the world of crypto, I don't see how you can figure out what the float actually is, because you'd have to know something about the entirety of the blockchain that the blockchain intentionally makes unknowable. You're not supposed to be able to look at the blockchain and identify the players. There's

no equivalent in the blockchain of a 13F that the SEC makes you file. And if there were, maybe we wouldn't be interested in bitcoin anyway.

Attention from regulators?

At the end of the day, every cryptocurrency will be regulated; there's no doubt about it. As a matter of fact, very soon futures on bitcoin will be available. The CME and the CBOE will offer bitcoin futures that are self-regulatory organizations defined as such by the laws of the United States so, in that sense, they already will be regulated. Position limits and many other controls will be implemented. The problem of the regulations is not that they will be too severe or that they will somehow disrupt the bitcoin market; because cryptocurrencies evolve so rapidly, and it's all open-source code.

Either a proposed regulation is not severe enough, in which case it will be ineffective, or it's too severe, in which case people will evade it by making up a completely new cryptocurrency, which is very easy to do. From the government's point of view, the situation is evolving so rapidly that it's not entirely clear what to do about it. This points to a larger problem. It's not that bitcoin in and of itself is a civilizational change or that cryptocurrency in general is a civilizational change. The civilizational change is that, historically, the hierarchy had more knowledge than the people. For centuries—for millennia really—the majority of people were illiterate, and even those who were literate weren't very knowledgeable. Only a handful of people in the hierarchy could legitimately claim the authority to tell people what to do and, therefore, they made the rules. Today, that relationship is reversed: the people in the hierarchy know much less than the people who are actually making things happen.

For example, let's say there was a problem with the New York City water supply. The mayor of New York City is not a hydrologist, nor is the governor of the state of New York, nor is the president of the United States. Even the people who work for the Environmental Protection Agency and other agencies are not hydrologists. They likely know so little about hydrology that it's not even clear they would make a good choice as to who would be a qualified person to take care of the problem. They don't have the expertise to deal with the bulk of the technological problems that we have in civilization.

The prevailing belief has been that whatever the conflict in human existence, only a handful of people in the hierarchy can resolve it. That belief came to dominate politics in the early 19th century with the imposition of the Napoleonic Code—the French civil code, which had a strong influence on the laws of many countries in Europe and beyond. The idea was to have statutes that purport to resolve every conflict in society. That approach has evolved to the point that if you look at the Treaty of Lisbon, which governs the European community, comprised of a constitution that, let alone regulations, is two huge piles of paper, each one taller than the average human being. It is so much paper that it takes several very strong people to carry it into a room. If you tried to read it, it would take you years and, by the time you reached the end, you'd forget what's in the beginning.

The idea of having a preset system of rules to govern every human activity is not workable when human activity is so infinitely variable. The Soviet Union proved that, as did Nazi Germany, Communist China, and others. But, for some reason, there are still those who don't accept it as proof. A much more sensible system is the English Common Law system, in which the rule evolves from a particular incident. If a dispute arises in society, a resolution to that conflict is crafted. In that way, a generalization emerges from the particular rather starting with a generalization and applying it to every particular instance. That approach is unique to the English-speaking world, but even in that realm, it's unfamiliar to the average person.

Many of the laws of Britain were never passed by Parliament; rather, they were the result of case law, of court proceedings over the course of a thousand years. The same is true for much of U.S. law. If it were a simple matter of thinking up a statute and applying it, it wouldn't be as complex as it is. But the trouble is that the people thinking up the statutes don't have the ability to foresee every possible development, and that's where trouble arises.

Given all that, I'm not worried about the regulators running ahead of the circumstances. It's much more likely that the evolution of society will run a lot faster than the regulators can work, which is why they're rendered largely impotent. In the crypto world, this is what's been happening, and it will happen in every other aspect of society. They can't regulate because they can't keep pace with the technological changes, and they shouldn't be expected to do so. How is a small group of people, specialized as they are in one little branch of finance, going to outthink hundreds of millions, maybe billions of people? It's preposterous on its face. Therefore, I don't worry about things like that, and I don't think anybody else should either. I think the reality is that the technological innovation runs much faster than the regulators can run, which should be self-evident to anybody who wants to look at it.