An overview of why I am skeptical about cryptocurrencies

(v1.0, 5/3/18)
(Edit, 11/20/18)

James Dow
Department of Finance, Financial Planning, and Insurance
California State University, Northridge

Lately, I've ended up in a number of conversations about cryptocurrencies, taking the role of the skeptic, and so I've put together my reasons for skepticism in a more organized format. My assumption is the reader knows broadly what cryptocurrencies are and has an ECON 101 understanding of economics.

Typically, five broad reasons have been offered for cryptocurrencies, although which reason gets the most emphasis depends on who is making the case. Cryptocurrencies are either:

- A new unit of account/base money
- A new unit of exchange
- A political project
- A new type of asset
- A new source of funds for companies - ICOs

My argument is that when you take a close look at each of these areas, cryptocurrencies either don't provide a better solution than what we have now or there aren't enough people who care about that particular problem. I'll go through the items one by one.

A new unit of account/base money

Here's the really short version. In a very simple (but useful) model of inflation, the rate of inflation is positively related to the rate of money growth. High rates of inflation or deflation are bad, and uncertain rates of inflation or deflation are very bad. Economic theories differ on what the "best" inflation rate is, but numbers in the range of -2% to +2% have been offered, with +2% being the more common view today. To get price stability you need a money supply that expands at about as fast the economy grows (maybe a little faster, maybe a little slower, depending on what target you are shooting for).

For any economists reading this, yes, this is an oversimplification. There is a world of things this leaves out: stabilization policy, endogenous money, problems with predicting the demand for money and a whole host of measurement problems. That's fine, they make the skeptic's case stronger not weaker, but it's useful to address the argument typically presented, which is, Bitcoin has a fixed supply in the long run and that will prevent inflation. The problem is that Bitcoin has a fixed supply in the long run and so we will see rapid deflation in the transition to

the Bitcoin world and then moderate deflation farther in the future. The first is certainly bad, the second is likely to be bad depending on what we mean by moderate.

Of course, the fact that Bitcoin itself is fixed in supply isn't enough to even guarantee the absence of inflation. There can always be other base monies (new currencies, forks, etc) and likely a banking system that will be built on top of Bitcoin that might add "elasticity" to the money supply or increase velocity. Once you have a financial system with money created by financial institutions, you are back in the conventional world.

A new unit of exchange

People rarely buy goods with base money such as gold or deposits at the Federal Reserve. These are inconvenient for transacting and so are better used for netting between financial institutions. Because of that, a payment system is needed on top of the base money, and generally this is handled by large financial intermediaries such as banks.

You can imagine all the different ways to pay for something: you can pay with coins, with paper money, write a check, use a credit card, wave your phone over a reader. Some of these are actual transfers of money, some of these are just instructions that a transfer should be made at some other point at some other time, mostly by someone else. In practice, there are many different ways to pay for things because there is no one best way to make all transactions. The financial system is about convenience and so for cryptocurrencies to complete they will have to reproduce much of how the current system works (which includes the flaws).

Here's the most important thing. The current system works pretty well. Have you ever been in the position where you wanted to go out to lunch, could afford to out to lunch, but decided not to because you couldn't figure out how to make a payment? Not only do we not worry about it, we are almost oblivious to the issue. Cryptocurrencies as a payment system are solving a problem that isn't much of a problem. Could the system be faster and cheaper? Sure, but the gains would be modest compared with the disruptions of completely replacing the banking system. If you want to see technological improvements in the payment system that will actually matter, look to Apple Pay and the like, not to cryptocurrencies.

A word about security

The security system around the payments system (and pretty much anything associated with computers) isn't terribly good. And that's intentional. Good security is inconvenient and people, correctly or not, seem willing to trade convenience for security.

Bitcoin on its own is a mix of the very secure and the very insecure. If you keep your private key safe, you are safe. But if you lose your private key, you are in trouble in a way that you wouldn't be if you forget the password to your online bank account. And it's not very convenient. Because of the lack of convenience and other issues, a banking system has built up around cryptocurrencies in a similar way to how a banking system has developed in traditional finance.

Convenient banking systems are inherently insecure. The crypto-banking system has a pretty bad history in terms of security although there is no reason to think it won't improve to the level of the current banking system, that is, it won't be super secure but it will work OK.

Part of the problem is that the worst thing for security is fast, anonymous transactions on the internet. The most secure transactions are slow, personalized transactions because they can always be reset. The first priority for cryptocurrencies has been anonymity (or at least pseudonymity) which undermines the security.

One reply to this might be that this willingness to give up security is a bad idea and that consumers will eventually come around. But if so, the traditional banking system can change the way it does business. There are plenty of ways that banks could make banking more secure. Bitcoin banking isn't competing against the current level of security but against a (future) banking system that also puts greater value on security.

A political project

If you follow Bitcoin twitter, it readily becomes apparent that cryptocurrencies, to some extent, are a libertarian project where the guiding reason for Bitcoin is not security, but privacy. There is a strong desire for a limited government and cryptocurrencies work towards this, either directly by moving base money from government control to private control or indirectly by hiding transactions so they would be untaxed. The political view can be expressed in a number of different ways.

People want a libertarian government and cryptocurrencies are an engineering task towards making a government more libertarian.

Libertarian share of the vote in the last four US presidential elections was: 0.3% , 0.4%, 1.0% 3.3%. I suppose you could say that it's on an upward trend, although the last election was unusual to say the least. But the reality is, people like big government (if not the paying for it) and have consistently voted that way.

Even if most people don't want a libertarian government, it allows some people to opt out of the government and "go Galt".

Say that 5% of the country would like to live under a libertarian government. Could they effectively secede economically from the US by making their transactions invisible to the government? The difficulty here is that while the transactions might be invisible, their lives are not. As long as people have an observable, physical presence, there is leverage to deal with tax evasion if the government wants to. Al Capone says hi.

Could people physically secede? This is a common libertarian fantasy, most famously with the notion that a bunch of libertarians could move to New Hampshire, a relatively libertarian state, and through numbers shift it further in a libertarian direction. We haven't seen it yet and I doubt we will since so much of the cryptocurrency community live in California and it is pretty cold in New Hampshire. Warmer suggestions have included seasteading near Tahiti, creating a new "independent" city in Honduras and having a number of rich crypto investors move to Puerto Rico and make it a rich crypto-friendly jurisdiction. Best of luck to them. I respect people who would actually make sacrifices to pursue their political vision, but right now it's all talk.

In very repressive countries, cryptocurrencies would allow people to hold assets outside of the country.

This is a complicated counterfactual to address since I'm not sure what people are envisioning. Say that I live in a despotic country where the currency is the despot. I want to move my wealth out of the country so I exchange my despots for Bitcoin. Who would want to be on the other side of that exchange? Or is it like in Venezuela, where people will use subsidized electricity to mine currencies. That won't last. Or is the idea that people in the repressive country will trade among themselves using cryptocurrency transactions? I think this doesn't give enough weight to the *repressive* part of repressive governments. https://xkcd.com/538/ says it better than I could.

The other people who value privacy

The people who value privacy the most are those engaged in criminal transactions. Cryptocurrencies are ideal for the ransom in ransomware as they are fast, hard-to-trace and anonymous. Can there be a stable demand for cryptocurrencies generated by this use? I suppose it's possible, but there are going to be strong incentives to crack down on its use if this is the primary reason it's held. US dollars are not issued in large denominations, in part, because their primary use would be for illicit transactions, so governments have shown a willingness to intervene here.

A new type of asset

Anything that has a price that goes rapidly up and down will attract speculative investors. But there is also an argument that cryptocurrencies might be desirable for investors to hold in the long run because of their hedging potential. Again, it's analogous to gold. If gold returns are negatively correlated with stock returns, then holding gold as part of your portfolio provides diversification. A related concept is that gold provides a "safe harbor" in a way similar to Treasury securities. When the economy goes into a recession, gold or Treasuries might better retain their value and so provide some downside protection.

Can Bitcoin provide this? Fundamentally, this is an empirical question. We can look at how gold has behaved over the last 50 years and either directly estimate the parameters of interest (correlations), or more qualitatively, look at what happens during times of economic stress. Bitcoin simply doesn't have enough of a history to meaningfully estimate parameters.

So we're left with speculation. In principle, cryptocurrencies could fill this role, but other assets that fill this role have advantages that Bitcoin does not. Treasury securities are backed by the taxing power of the US government and are built on a stable currency. Gold has non-monetary uses and a very long history as a store of value. But the next recession or financial crisis should tell us more.

A source of funds for companies - ICOs

An initial currency offering (ICO) is when a company creates its own cryptocurrency, sells the tokens to investors and uses the proceeds to build their business. Proponents of this say that it is a new way for companies to raise funds and allows small investors to participate in startup financing. Critics say it's a way to get around securities law to take advantage of naïve investors. To evaluate these claims we need to talk about some basic methods of financing a company.

There are basically two types of tokens used in financing: bonds and stock. Bonds (a type of debt investment) are the most straightforward. As a bond investor, I give the company money now in exchange for a token. The token promises me regular payments in the future along with the repayment of the principle at the maturity of the bond. Bondholders have a variety of protections. There may be covenants that restrict things that the company might do that would have a negative effect on bondholders. If the company goes bankrupt, bondholders are ahead of others in the line to get what remains of the value of the company.

Stocks are equity investments. In exchange for my money now, the company gives me a token that represents an ownership interest. I have some voting rights for the board of directors of the company, and if the company is sold, I will get my share of the proceeds of that sale. In addition, if the company is profitable they can pay those profits directly to the shareholders in the form of dividends. The rights of the stockholders and bondholders are enforced through securities regulation and the legal system. Bonds and stocks differ in that bonds offer specific payments and provide a number of protections but generally offer limited upside because there is only so much that the price could increase. Stocks have more risk but offer the possibility of a large upside if the company becomes very profitable. There is a clear connection between share price and profitability. If a company becomes more profitable, shareholders could receive greater dividends or would benefit if the now-more-profitable company is sold for more in the future.

ICOs work differently. Many ICOs boil down to you giving them money in exchange for nothing. They don't promise income streams, they don't come with ownership and they don't offer legal protections. Even though they don't offer the features of equity they are often marketed to mimic equity (when equity is first sold to the public it is call an initial public offering or IPO; the term ICO is used to make it sound like equity even if it isn't). Often, issuing companies *imply* a connection between their profitability and the value of a coin, but they don't provide a reason for it actually to be so. Actual equity has reasons for this connection; more profitable companies can pay greater dividends or can be sold for a higher price.

In an effort to provide a connection between the performance of the company and the financial return to the coin holders, there has been an increasing emphasis on the *use* of coins in the purchase of the company's product. Say that I sell some service, maybe an online video game. In order to play this game, you need to use my token. The value of this token will depend on how the payment process is structured.

Say that you can play one hour of my game online for $1. To raise money before I finish my online game I sell tokens for $0.90 that allow you to buy one hour of game time in the future. If the discount in price isn't too much, it may be a reasonable way to raise money, and perhaps a reasonable investment. The problem is that if the company turns out to very popular and profitable, it will make the equity holders rich, but not the coin holders. Coins are not equity. Because there isn't much upside to these coins, they don't have the advantages of an equity investment. But they also don't have the advantages of a debt investment; they don't have the same protections and there is substantial downside risk if the company fails. The combination of just a little upside and lots of downside is why you don't want to make debt-like investments in risky start-up companies.

Now imagine a different setup. Tokens don't represent time but they exchange for game time based on their online price. Playing costs $1 per hour. The only way to play is to use tokens that exchange with game time *at their market value*. If tokens are limited in supply and the game becomes popular, the increase in demand for tokens should result in an increase in price of tokens (If tokens sell for $3 then a token now buys you three hours of playing time - you need to make this adjustment, otherwise the cost of playing time goes up, driving away customers). Making the value of a coin dependent on market price is complicated for both gamers and the company but is technically feasible. But it's also a hassle and probably easier for the company to just introduce a new version of the coin or let you use dollars. The company can algorithmically promise to limit the supply of the original coin, but not the supply of perfect substitutes.

In summary, ICOs sell themselves by mimicking equity but they are not equity and there is no reason for them to behave like equity and use-tokens are structured like debt but without the protections of actual debt. At best, they are a way for naïve investors to provide cheap funding for companies, good for companies but bad for investors. At worst, they are a quick way to scam those naïve investors.

In the end

Could there be a cryptocurrency that solves an important problem, perhaps an ICO that is structured to provide the protection that other investors get and also the upside that should be associated with startup ventures? Perhaps, but we would probably just call that equity. The crypto part buys you very little.

Systems with common ledgers are useful. Blockchains might be useful. But the crypto part, particularly in connection with cryptocurrencies, does not seem to help address problems that people actually care about. That is the fundamental reason for skepticism.