Is any current cryptocurrency a legitimate currency?

by Kevin Loney

While this is an issue that people have invested in emotionally as well as financially, we need to have an adult conversation about it.

Q: Is any current cryptocurrency a legitimate currency?

A: No.[1]

———————————————

[1] **Legitimate currencies have publicly disclosed asset owners**. On a weekly basis there are reports of the current and potential dollar values of NFL contracts, IPOs, executive bonuses, royal art portfolios, and lottery jackpots. But over 99.99% of people reading those numbers will *never* be professional athletes, children of royalty, or lottery winners — so why is this seemingly irrelevant data repeatedly published? Why are the wealthiest people ranked, and compared to last year's list? What's the point?

Such publications are very important to the public legitimacy of an economy. Given that currency is the means by which people keep score, all of the participants in the economy must agree that the means of keeping score is fully understood and valid. For any currency to be valid — for it to have the backing of the full faith and credit of a country and its government — it must have the full faith and backing of the people who will use it. The people of the country must accept it, must collectively decide it has a common value across the country, and must assess its worth consistently. They must be able to compare a dollar in one use to a dollar in another use, verify those two dollars are interchangeable, and agree the two uses are both valid. A dollar must be worth a dollar as part of a sports contract in San Diego or an RV purchase in Nebraska or a community college tuition payment in Maine (economists would say this currency therefore functions as a 'unit of account'). A dollar's value cannot fluctuate wildly over a short time period as that would lead to economic, political and social instability — so a dollar next week has to be worth very nearly the value of a dollar this week. The dollar's value varies, but it varies consistently and in a controlled fashion.

Any attempted defense of the current cryptocurrencies as legitimate public currencies fails at this point. Cryptocurrency prices vary *across exchanges*, have unpredictable surges from week to week, and have no disclosure of wealth distribution. If you hold an Ether token today, you have no idea what its price will be next week, if any; you hope it will be worth at least what you paid for it but you know that is not guaranteed. The token has a distinct price (not value) at one point in time, and its historical prices cannot be used to predict its future price. For stability and backing, **real currency has to be issued and supported by a central bank**.

The last significant disclosure of bitcoin holdings was that Bulgarian police in May of 2017 announced the seizure of 1% of all bitcoins that could ever be mined. The news focused on the sensationalized worth of the holdings and ignored the concentration of coins, their source, and their future disposition as issues. The current asset holders are important because you're not just exchanging your money for cryptocurrencies; since their lifetime quantity is capped, you're buying bitcoin that someone else is selling via an exchange. Who are you dealing with, and how did they get their holdings? What did they pay for it?[2]

[2] **Currency is a medium of exchange to purchase things, with a consistent value that everyone agrees to**. You know what gas costs week after week, as expressed in dollars, because the dollar's worth is stable. That's what currency looks like.

It does not look like this:
Jan 14, 2018: $1389/Ether token
Jan 14, 2019: $125/Ether token
May 7, 2019: $173/Ether token
Two months from now: Nobody can say.

While it is possible to use cryptocurrencies for purchases, the widespread commercial use cases for them are minimal. Regulated banks refuse to accept cryptocurrencies since banked funds must by law come from verified owners (forcing cryptocurrency exchange users to capture, verify, and report account holder identities), and most legitimate vendors dealing with verified owners already use actual banks (thus receiving no benefit from using cryptocurrencies other than opening themselves to new customer bases and new types of fraud). And vendors themselves *want* to deal with verifiable customers so they can market to them, email them, enroll them in loyalty programs, target their product offerings and lower their operating costs. Historically, many transactions using cryptocurrencies are just exchanges with other cryptocurrencies, or transfers among accounts (this skew is due in part to the volume of transactions that are used to hide the proceeds of illegally obtained cryptocurrency).[3]

[3] **Regulated financial institutions have to verify the identity of each account holder** (KYC, or Know Your Customer regulations), monitor for money laundering, report suspicious activity, and prevent transactions that involve countries and individuals under sanction. Such basic regulations for transactions are not enforced by all cryptocurrency exchanges even though FinCEN requires them to register as MSBs (money service businesses). **Without that transparency there is no shared accountability, and no legitimacy for cryptocurrency transactions in the real world**; they only serve use cases that rely on secrecy, are conducted between parties that already know each other, or represent a real world purchase that someone wants kept off a bank credit card.

The exchanges that host these trades generally profit from transactions or transfers, and the financial dealings of the exchanges themselves lack transparency. In the current news cycle there are cryptocurrency exchanges where the owners have died/disappeared, or the owners used money from another exchange to obscure financial status, or the owners are under investigation for incorrect reporting of their activity. While a token's price is going up, an exchange's customers think they are winning, but their investment could be devalued by 90% at any time, or the exchange could be hacked or shut down, or both. It's happened before even to major exchanges; there is no reason to think it cannot happen again.[4]

[4] Then what is a cryptocurrency? It's a speculative investment, an unsecured security. **The crypto security being purchased has no intrinsic value; it only gains in price if someone else decides to pay a higher price for it** at a later time, not for any intrinsic reason.

If a proposed currency is not used for the purchase of goods or services, and all you can do is sell it, **it's a tulip without the color, scent, or texture of a tulip**. It's like a penny stock in a company whose board, products, and strategic direction are never shared with the investor, bought on an exchange that could disappear tomorrow. Cryptocurrencies are misnamed; they're just electronic tokens, with a name they have borrowed that gives them more credit than they are due.[5]

[5] **Picture cryptocurrency tokens as commemorative plates depicting Quidditch scenes from Harry Potter films**; maybe the resale price of the plates will go up, maybe it will go down — you cannot forecast. All you know is there is an anonymous active group of commemorative plate traders somewhere who trade plates among themselves, and who have decided to try to maintain secrecy as they do so, and occasionally they trade a plate for a consumable item such as a chocolate frog. It is possible that at some point all the traders will stop trying to acquire new plates via trades, or plates will be taken out of circulation (due to breakage, fading, or the loss of their security keys) or traders or exchanges will stop accepting a particular type of plate — resulting in the market price of a plate dropping to $0 as the demand evaporates with no warning.[6]

Just being able to trade a plate for something doesn't make it currency. That may seem like an easy logical mistake to avoid, but it tripped up a Forbes columnist.

[6] **All exchanges involved in cryptocurrencies must meet the regulatory controls enforced on federally insured banks and securities brokers in order to be considered legitimate. They don't.** New entrants in a market have to outperform the legacy providers in all aspects of business functions, including controls and security. But it is common today to read of hacks at exchanges that are discovered months after they took place; if the same behavior were to happen at real banks at the same pace nobody would deposit money in a bank. Instead of protecting identities and losing coins, exchanges should be publishing identities and protecting coins. Considering the organized crime groups targeting the exchanges, repeated attacks on exchanges should be expected, and the higher the price of a token goes the more appealing it is as a target for hacking groups. Calling those groups 'hackers' is misguided, as it understates their level of evident cooperation, organization, and planning.

In addition to being vulnerable to inadequately secured exchanges, cryptocurrencies are inherently vulnerable to attacks on their networks. Any cryptocurrency that uses the blockchain distributed ledger model is dependent on a shared work concept and is theoretically susceptible to an attack in which a rogue operator commands 51% of the available resources. In such attacks, an operator takes over enough resources to inject transactions into the shared ledger and then cashes out redirected wealth before the problem is resolved; this has been an obvious design concern since the start. The retort to that design challenge had always been that such an attack would invalidate the system as a whole and would be detected quickly. And with such an impact, the argument continued, it would not make sense for a participant to engage in damaging the network and crippling it for days and devaluing its remaining assets — but it was executed against Ethereum classic (Jan 2019), Bitcoin Gold (May 2018), and others.[7]

[7] Blockchain technology itself has significant architecture issues impacting performance, energy consumption, scalability, security, and resilience that are evident even at a high level review. To consider just one: **To comply with GDPR and CCPA, data storage systems have to be able to selectively delete records for specific individuals, across all date ranges**. **Blockchain systems that rely on permanent immutable records do not support the removal of prior committed data, inherently violating these privacy regulations**. To work around this issue, developers and data architects need to obfuscate, tokenize, or aggregate data prior to publishing anything out to a shared distributed blockchain — and in tokenizing data they are usually hitting a database to store the mapping data. (For a more detailed writeup than is appropriate in a footnote, see this article). Developers would be implementing a more optimized design pattern if they just completed the rest of the business transaction in that mapping database instead of also using a blockchain. In this example, the blockchain usage is adding work on both the transaction storage and on subsequent queries, not replacing it. By creating a second repository for the data, the blockchain usage also adds to the physical security risks (both in storage and in transit) and the data synchronization challenges inherent in any replica— you're adding complexity and risk while gaining a benefit that may be available at a much lower cost.

Commercial vendors have production solutions that integrate blockchain technology into their offerings. That doesn't mean all vendors are fully implementing a distributed, secure, scalable solution based solely on blockchain technology, or one that allows you to effortlessly migrate and automatically comply with data privacy regulations. As IBM notes concerning data privacy compliance for its solutions, "In most cases, that means any personal data should be kept off-chain." And any critical processing could suddenly be unavailable if it relies on a distributed network outside your control that can crash, like Stellar did for several hours in May 2019.

If read carefully, the common theme found across most articles touting blockchain-based solutions is that they are actively solving the problems of the year 2007. They offer solutions that support data sharing, change data capture, data replication, resilience, event processing, and hardware virtualization — but these problems have all been solved, better, in the last decade. And in the process of offering a solution for past concerns the blockchain solutions defer on addressing the key requirements of 2019: data privacy governance, power consumption, scalability, and security at every single point along the data path. They solve an already-solved problem in an inelegant fashion while adding significant risk.[8]

[8] **Speaking of risk: as a blind investment, cryptocurrencies cannot compare with other securities in the marketplace**. For a moment, let's set aside the 1400 cryptocurrencies that are considered dead (inactive) coins or outright scams. Every commonly traded stock fund in the US market issues quarterly reports showing the underlying companies whose stock it holds. And those companies whose shares are held disclose their largest individual shareholders, their numbers of shares in circulation, their board members, their liabilities, their income and expenses, and their expected earnings per share. The stock market is not immune to overspeculation, fraud, insider trading, theft, misstatements, political unrest and natural disasters; but since there is an active regulatory environment all of those are governed and reported so the consumer has at least some of the transparency needed to make an informed investment decision.

Here, for example, is the public list of insider stock transactions at Microsoft for the last two years: https://finance.yahoo.com/quote/MSFT/insider-transactions/ . Compare that to the blindness that greets an investor in the cryptocurrency world: on April 2, 2019, a single buyer bought $100 million worth of bitcoin with orders across 3 exchanges. The outcome of this bulk purchase was to bump the bitcoin market price ever since as those purchases drove the price up and speculators jumped on the tail of the price improvement wave hoping the price increase had some sort of intrinsic merit. But those speculators have no idea who made that purchase or when the purchaser will sell (pump and dump) or the impact that sale will have on the market. Is it possible the large purchase was intended to be seen and to pump up the market price to make a subsequent sale of those bitcoins even more profitable? Has the market been played?

Consider: with no transparency, one cannot make any defensible judgment about the legitimacy of the single largest transaction that has occurred in cryptocurrency this year. There is no fact-based assertion about where that transaction came from — if it came from a hedge fund or from an organized crime organization or from a country currently under financial sanctions or from another Ponzi scheme targeting Samoan church congregations.

So what can you do with a cryptocurrency token? You can't buy eggs at the farm with it, and you can't say with any assurance how may eggs it could buy next week (if any) or why its price would change. If all the exchanges suddenly stopped allowing you to convert the token to dollars (aka fiat currency), it would rapidly devalue. All you can do is sell it and hope there is at least one more person out there willing to buy it.

Meanwhile, there are at least 900 cryptocurrencies currently listed as inactive, with another 500 considered outright scams with their local wallet software infecting your machines with malware and keyloggers.

Arthur Weasley was right:
"Ginny!" said Mr. Weasley, flabbergasted. "Haven't I taught you anything? What have I always told you? Never trust anything that can think for itself if you can't see where it keeps its brain." [9]

— J.K. Rowling, Harry Potter and the Chamber of Secrets

[9] In terms of the legitimate currency Mr. Weasley was more familiar with:
"The gold ones are Galleons. Seventeen silver Sickles to a Galleon and twenty-nine Knuts to a Sickle, it's easy enough."
— Rubeus Hagrid, in J.K. Rowling's Harry Potter and the Sorceror's Stone

- Kevin Loney, May 2019. The views and opinions expressed in this article are my own and do not necessarily represent official policy or position of any company or organization with which I have ever been affiliated.