Bitcoins, Blockchains and Bubbles: A Trusts and Estates Practitioner's Guide to Cryptocurrency

by Angelo M. Grasso

Few subjects are as prevalent in the news, yet completely foreign and confusing to readers, as cryptocurrency. In an effort to demystify one of the more intriguing innovations of this century, below is a Q&A for trusts and estates practitioners that discusses the concepts of cryptocurrency and blockchain, why they have received so much attention over the past few years, and what to know when discussing them with clients, colleagues, or at cocktail parties.

What is cryptocurrency?

Answering this threshold question requires first asking and answering an even more fundamental question...

What are money and currency?

Without getting too philosophical, money is any item or verifiable record that is generally accepted as payment for goods and services and the repayment of debts. Currency is a generally accepted form of money in circulation in the form of coins and notes, which then becomes the basis for trade. Stated another way, currencies are "systems of money" for a particular nation (such as the U.S. Dollar) or a confederations of nations (such as the Euro). Currencies are also referred to as "mediums of exchange."

Okay, fine. So what is a cryptocurrency?

It is also a medium of exchange, but unlike "hard" currencies, a cryptocurrency only exists in the digital world; a "physical cryptocurrency" is an oxymoron. The "crypto" portion of the portmanteau signifies that it relies on encryption to ensure that transactions using it are secure. And unlike most currencies—dollars, yen, yuan, rubles, pesos, reals—a cryptocurrency is not issued by a government or confederation.

Currency issued by something other than a government? I've never heard of such a thing.

Actually, you probably have without knowing it. Tokens issued by private vendors—such as amusement parks, subways, or driving ranges—act as a form of currency. They have intrinsic value for the particular vendor or commercial entity, and allow you to do things within that vendor's purview, such as go on a merry-go-round, ride the train, or hit golf balls. But those tokens are not legal tender,[1] and generally speaking, cannot be used for most transactions. Try using your ride tickets from Playland to buy a slice of pizza in Manhattan. I suspect it will go nowhere.

What are some examples of cryptocurrencies?

Bitcoin is by far the most famous. Other (relatively) well-known cryptocurrencies include Ethereum, Litecoin, and Ripple. There are at least 1,500 known cryptocurrencies in the world, and that number is only growing.

How did cryptocurrency start?

The notion of a digital currency is as old as the internet. One of the first people to try to come up with a secure mechanism for digital currency was David Chaum, who in the early 1980s wrote the paper *Blind Signatures for Untraceable Payments*.[2] Therein, Chaum described acquiring digital currencies from banks, and spending them in manners that could not be traced by the bank, or for that matter, any third party. A later paper by Chaum attempted to address the problem of "double-spending," i.e., ensuring that the holder of a unit of digital currency did not spend or use that particular unit more than once.[3]

Despite Chaum's papers and the work of many others, no well-accepted online currency developed over the next two decades. For example, Chaum's major attempt at a cryptocurrency—Ecash—failed because it was dependent upon credit card companies and governments to provide the infrastructure and maintain a ledger of transactions. The innovators of cryptocurrency wanted it to be completely untethered from governments and third parties, both philosophically and practically. The problem was that until 2008, nobody devised a method to ensure that a unit of digital currency was not spent multiple times without involving a third party to keep and maintain the ledger.

What changed in 2008?

The breakthrough came in October 2008, when Satoshi Nakamoto[4] published the white paper *Bitcoin: A Peer-to-Peer Electronic Cash System*.[5] The paper summarized the double-spending issue:

> The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned

Angelo M. Grasso is a partner at Greenfield Stein & Senior, LLP, practicing in trusts and estates litigation.

> to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

To cut out the middleman—i.e., a private third party that would maintain the ledger—Nakamoto proposed a *public* ledger where every single transaction using the cryptocurrency would be made public. This would mean that every person or entity using the currency would know that each coin had not been spent multiple times:

> We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

How would this work?

The system would record each and every transaction using the cryptocurrency in a data form known as a "block." Every block would contain certain pieces of information concerning the transaction, including the date, time and amount of money exchanged. The block would also record the parties to the transaction, but would do so anonymously by assigning each party a unique "digital signature," which is largely an unintelligible group of numbers and letters. Finally, each block would also contain a unique code (called a "hash") to distinguish that particular block from each individual transaction. For example, if every Tuesday at 8:30 a.m. you bought a dozen donuts from the same vendor using a cryptocurrency for the same amount of money, each entry in the ledger would have a different hash because each was a different, discrete purchase.

But how do these transactions get processed?

If you'd like the answer complete with numerous Greek letters and math that goes beyond A.P. Calculus, the white paper lays it out pretty thoroughly. Assuming that you're looking for a more simplified version of the process:

- A transaction needs to occur. For the sake of this example, let's say you're buying a crate of bespoke bathroom tiles from a merchant in Alabama. You make the purchase online for a set price.
- Next, the transaction needs to be verified. This is done by an array of computers around the world that are connected to the cryptocurrency's network. Their job is to verify the date, time, amount, and parties to the transaction.
- Once a transaction has been verified, its details are stored in a block. This won't be the only transaction in the block; there will be hundreds of others joining it. What these transactions have in common is that they were all verified at roughly the same time.
- Once *that* happens, the block is given its hash, which includes the hash of the most recent block that was published. Once this has happened, the new block is ready for publication.

What does publication mean?

Blocks that have been given a hash are then published in chronological order on the cryptocurrency's ledger. This ledger is known as the "blockchain"—literally, a chain of blocks in chronological order, linked by the hashes (the prior one and the new one). And this blockchain can be viewed by anyone.[6]

Wait, so I can see what other people have done with their cryptocurrency?

Sort of, not really. Anyone—including you!—can log on to the blockchain and review each and every transaction in a particular block. But doing that will likely be unedifying. Remember, the parties to a transaction were made anonymous by their digital signatures. So while you can see the date and time and amount of money exchanged, all you will know is that it was between two anonymous digital signatures. You will have no idea who was part of the transaction or why it occurred. It could have been people buying pizzas,[7] couches from Raleigh, weapons from Moldova, or gambling proceeds from Antigua.

Okay, so a block is added to the ledger. Why is this a big deal?

This goes back to the "hash," which is what ensures against double-spending. As noted above, each transaction's code includes two hashes: the one in the immediately prior block, and the one in the current block. The hashes are created by a mathematical function that relates to the specific data contained in the block. Hence, if someone tried to edit any portion of a prior block, its hash would change. This would break the blockchain, because the adulterated hash would

no longer link up with the prior or subsequent block. To fix this, a hacker would have to edit the prior block, and then the block before that one, etc. This makes the blockchain virtually impossible to edit or delete.

So what's the big deal about making the ledger public?

Remember how we said you could view the blockchain at any time? You can go a step further and connect your computer to the blockchain network. This gives you a copy of the blockchain and all updates to it—think of it like a constantly updating feed on Instagram or Twitter. This is known as "peer to peer" networking, where there is no central computer, but the data and information live on all the users' computers. The most famous example of "peer-to-peer" networking was Napster, where you could download a kajillion songs not off of some central repository, but rather off of the myriad computers of other people in the Napster network.

The peer-to-peer setup means that if someone wanted to change what's in the blockchain—presumably nefariously—she wouldn't only have to change the ledger that's in the hands of a private third party. She would have to change the ledger that's in the possession of *every person* who is linked to the blockchain network. In the case of large cryptocurrencies like Bitcoin or Ethereum, this would require altering hundreds of thousands of computers, and is, practically speaking, next to impossible.

So transactions are public and yet not public. This sounds sketchy.

That's certainly one interpretation and what many other people have concluded. Another conclusion is that it's not that different from dealing with cash, when there's no oversight or records of transactions at all.

I think I understand how a blockchain works. But what does this have to do with Bitcoin?

The blockchain is the ledger that contains a record of how all of the units of a particular currency move from party to party, and ensures that there are no shenanigans when people enter into transactions using cryptocurrencies. The currency itself—be it Bitcoin, Ethereum, or IceNineCoin[8]—is what is actually used between the parties for the transactions. If you want to actually conduct a transaction using cryptocurrency, you care about the coin itself, and the blockchain is the apparatus that gets the transaction done.

If cryptocurrencies aren't tangible items, how can I get one?

What you'll first need is to get a wallet. Not a pleather item from Canal Street, a digital wallet, which is software that is designed to make cryptocurrency transactions and view balances. While we could spend paragraphs going over the different types of wallets, what's important to know is that digital wallets have two forms of identification: a public key and a private key. The public key is analogous to a username, and is the code that appears in the blockchain to show you are the person making the transaction—think back to the digital signature we discussed earlier. The private key is your password to transact with cryptocurrency.

Broadly speaking, there are two different types of wallets: "hot" and "cold" wallets. The difference is how the cryptocurrency is stored—hot wallets keep the currency online, while cold wallets keep the currency on a hard drive, or more often, a flash (USB) drive.

I thought the whole point was this currency was online. Why would I want to then store my currency on a flash drive?

Security. If you're holding your currency in a "hot" wallet, it's probably through one of the many cryptocurrency exchanges where you can buy and sell cryptocurrency and effectuate transactions. Probably the most popular exchange in the United States is Coinbase, in large part because it's fairly easy to use, has an app, and trades multiple currencies (Bitcoin, Ethereum, Litecoin, and some others).

The issue with an online exchange is the same issue we see in stories every month concerning life online: they can be hacked. Infamously, Mt. Gox was a popular Japanese exchange, and in 2013 handled over half of all Bitcoin transactions. Then in 2014, it was hacked, and lost 750,000 of customers' Bitcoins, plus another 100,000 of its own. Since then, many people have been skittish about keeping their currency online, despite the exchanges' assurances that their security is top notch.

I don't blame them! I think I'll keep my currency on a flash drive. There's no downside, right?

Well . . . not quite. That flash drive with your cryptocurrency on it is quite literally the entire record of the currency's existence and your ownership of it. If you lose the flash drive, your money is gone. If you forget the password, you're in trouble. If you drop dead and don't leave your heirs with instructions about how to find and access your cold wallet, odds are they're out of luck. Think of it like having a buried treasure chest with gold. It's great if you know it exists and where to find it. It's worthless if you can't.

That's far-fetched. I'm sure that almost never happens.

If only that was true. QuadrigaCX was a Canadian cryptocurrency exchange founded by Gerald Cotten that traded currencies including Bitcoin and Litecoin. At the end of 2018, QuadrigaCX had over 100,000 clients and $190 million in cryptocurrency and regular money (also called "fiat"). To protect the currency from hacking, Cotten elected to keep most of the exchange's currency in a hard wallet on his laptop. This proved to be a problem with Cotton died of Crohn's disease in

India in December 2018, and nobody knew the password to his laptop that held all of the currency. As of the writing of this article, there's no reason to believe the QuadrigaCX account holders will be getting their currency back.[9] One cryptocurrency analyst estimates that of the 17.5 million Bitcoins that have been created, four million have been lost forever.[10]

Suddenly that hot wallet doesn't sound so bad after all.

No, and you're probably going to want one anyway if you actually want to conduct any transactions with your cryptocurrency.

Got it. So circling back, what do I need to do to get some Bitcoins?

After creating a wallet, you'll need a secure internet connection (of course). You'll also need proper government identification to comply with SEC regulations and, if you're using an exchange, their internal compliance. Then you'll need a credit card or a bank account to link with your wallet—you do have to pay for the cryptocurrency somehow.

"While cryptocurrencies were initially intended to be used as a currency to replace (or supplement) the Dollar and Euro, many have treated them as investments and have purchased them in the hope that their value will skyrocket, and they can sell them for a profit."

Finally, you need to pick an exchange. (Often the wallet and exchange are the same, but they do not need to be.) As we mentioned earlier, Coinbase is a popular exchange. There are many others such as Gemini, Binance, Coinmama, Kraken, and BitPanda. We are not making any recommendations or judgments on any of these exchanges, except to note that some of their names are absolutely fabulous.

Can you buy or use only part of a Bitcoin?

Yes—transactions can be carried out to decimal points. For example, if you want to pay for an $80 rug using your Bitcoins, and Bitcoin is presently trading for $5,600, you would send the seller 0.0142857 Bitcoin. Generally speaking, the exchanges will do the math for you.

How much does a cryptocurrency cost?

Much like traditional currencies, the prices fluctuate. We've all heard about times the dollar was "strong" or "weak," especially in relation to other currencies such as the Pound Sterling or Euro. The big difference is how volatile they are. Over the last five years, the value of a Euro has ranged from $1.05 to $1.38. Over that same time period, a Bitcoin has been worth between $327 and nearly $20,000.

That type of volatility sounds more like a stock than a currency.

A fair point. While cryptocurrencies were initially intended to be used as a currency to replace (or supplement) the Dollar and Euro, many have treated them as investments and have purchased them in the hope that their value will skyrocket, and they can sell them for a profit. Of course, they're not stocks because they're not equity in anything. When you own 100 shares of AT&T, you are a part owner of the corporation. Owning 100 Bitcoins doesn't make you the owner of anything except 100 Bitcoins.

This sounds like a bubble.

That's exactly the conclusion many people have drawn. And there are a lot of elements of a bubble here: new technology, a lot of press, a lack of understanding by people as to what exactly they're buying, and blind speculation about the future. Most important, the prices of the most popular cryptocurrencies have soared like a bubble. In January 2017, one Bitcoin was worth less than $1,000. By December 11, it had peaked at $19,511, before crashing down to under $3,500. Ethereum and Litecoin followed similar trajectories. All of these currencies are still operating today, they just cost a lot less than they did in December 2017.

Is inflation a concern? What's to stop someone from just minting a billion Bitcoins?

Not really, because there are only a finite number of Bitcoins that can be created, and there's a process to generate them, known as "mining," which is how all Bitcoins came into existence after the first block. Mining is a two-step process: auditing and proof of work. On the front end, miners are the auditors for the Bitcoin blockchain, and they verify the transactions. When a miner has verified a certain number of transactions (1 megabyte's worth, to be precise), they have satisfied the first condition and are eligible to earn a set number of bitcoins that decreases over time. (Presently, it is 12.5 coins.)

To earn those coins, the miner then has to engage in the "proof of work" phase, which involves providing the right answer to a numeric problem—namely, correctly guessing the next hash in the blockchain. This is basically asking someone to guess what number a computer is thinking of, only here, it's a number with 64 digits and that can also include the letters a, b, c, d,

or e. In other words, it's almost impossible to guess, which is why miners have devoted inordinate amounts of computing power to guessing these hashes.

I heard about this. Isn't Bitcoin mining going to melt the polar icecaps?

That's overstating the case, but only slightly. By some estimates, the amount of energy used to mine Bitcoins in 2018 exceeded Hungary' energy consumption for the same year.[11] There has been some speculation that this might change with Bitcoin's decline in value, but no real indication this is happening.

What are the differences between all these various cryptocurrencies?

There are some differences from a technological perspective which are too complex for this essay. For example, Bitcoin and Litecoin use different cryptographic algorithms. Litecoin purports to have a faster transaction speed than Bitcoin: the claim is Litecoin's transactions can be completed in two minutes, versus five hours for Bitcoin. Ripple has attempted to brand itself as the best cryptocurrency for cross-border transactions. Possibly the most interesting one for the long-term is Ethereum, which has a secondary purpose of having what are called "smart contracts" utilize the blockchain.

Now that I've read all of this, I don't understand why this is necessary. Other than sounding cool, why would people use cryptocurrencies instead of regular currencies?

Setting aside speculators who are hoping just to get rich from cryptocurrencies, there are a couple of advantages. The first is speed: for long-distance transactions, cryptocurrencies are quicker than wires, which requires multiple banks to communicate with each other and update their respective ledgers, whereas with Bitcoin, you would only need to update the blockchain. It's less costly to transact on a blockchain because there are no fees to the banks or middlemen. The transactions are more secure; even noting concerns about Mt. Gox, it is still far more difficult to hack a blockchain than a company like Equifax or Yahoo.

Finally, cryptocurrencies offer unmatched privacy. This has its obvious benefits, but more cynically, can be used for nefarious means. For example, The Silk Road was a notorious site for the buying and selling of narcotics on the black market. Most if not all transactions were performed using cryptocurrencies because it allowed the transactions to be completed and remain anonymous. The same is true for other illicit transactions like gambling and arms sales.

You know what? I'm going to stick with dollars.

A perfectly reasonable conclusion. But hopefully now you understand what all the fuss is about.

Endnotes

1. "Legal tender" is defined in the U.S. Code as "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues." Coinage Act of 1965, 31 U.S.C. § 5103 (1982).
2. *Blind Signatures for Untraceable Payments*, D. Chaum, Advances in Cryptology Proceedings of Crypto 82, D. Chaum, R.L. Rivest, & A.T. Sherman (Eds.), Plenum, pp. 199-203.
3. *Untraceable Electronic Cash*, D. Chaum, A. Fiat, & M. Naor, Advances in Cryptology CRYPTO '88, S. Goldwasser (Ed.), Springer-Verlag, pp. 319-327.
4. Trillions of electrons have been expended on the internet fruitlessly attempting to identify the person(s) behind this pseudonym.
5. https://bitcoin.org/bitcoin.pdf.
6. https://live.blockcypher.com/btc.
7. May 22, 2010 is known as Bitcoin Pizza Day, as on this day, a programmer paid someone 10,000 bitcoins to bring him two large Papa John's pizzas. At the time, the coins were worth $30. On January 1, 2019, those same Bitcoins were worth around $38 million.
8. A completely fictional currency. But Kurt Vonnegut would have had a field day writing a satirical novel based on cryptocurrency.
9. There are many more layers to the QuadrigaCX story that will not be delved into here, including a belief by many that Cotten faked his death in order to steal the money or to conceal the fact that the exchange actually did not have most of the funds it claimed to have in the first place.
10. https://coincodex.com/article/2018/jameson-lopp-estimates-4-million-bitcoin-are-lost-forever/.
11. https://www.newsbtc.com/2019/03/14/bitcoins-energy-consumption-equalled-that-of-hungary-in-2018/.