One cannot open a newspaper or website today without encountering a story about bitcoin or other cryptocurrencies. Advocates claim that cryptocurrencies represent a fundamental shift in the way we will use money in the future and that government-sponsored currencies such as the dollar and euro are intrinsically flawed. Critics see nothing but tulip bubbles and Ponzi schemes. Passionate cases are made on both sides of the argument. The truth, as is usually the case, lies somewhere in between.

In the commentary that follows, we attempt to sort through the hyperbole to better understand the opportunities and risks that cryptocurrencies pose by exploring not only bitcoin, but also the underlying blockchain technology on which cryptocurrencies rely. As usual, we start with a glance back at history.
A BRIEF HISTORY OF MONEY

Why does the dollar bill in your pocket have value? Its intrinsic value is practically zero: It is nothing more than a piece of paper with images, letters and numbers on it. Your dollar bill – or money in general – derives value solely from a common agreement, a collective story that we tell each other about value. The collective story has evolved over time, starting in prehistory with things that genuinely had commodity value, such as livestock or salt (from which we derive the word salary). As humankind tired of walking around with cows and bags of salt, money evolved into things that had representative value, such as cowrie shells, metal coins or pieces of paper. Intrinsic value was lost, but these artifacts were durable enough to be traded from hand to hand.

For most of the 19th and 20th centuries, major economies retained a modicum of intrinsic value by offering to exchange representative money for a certain amount of precious metal, usually gold. As gold standards came to an end in the modern era, money today is simply called into existence (fiat) by central banks and backed by nothing more than the issuing entity’s ability to manage an economy and levy taxes. All traditional currencies today are fiat currencies.

Money moved at the speed of humans for most of history, as payment required coins, bills or checks to literally change hands. In the digital era, the speed of money has accelerated: We bank online, check our investment accounts on our phones and pay bills through vendor websites linked to our bank accounts or credit cards. This is an improvement over putting checks in the mail but still requires centralized institutions such as banks to validate money flows and ensure that we aren’t spending the same digital money twice.

This “double-spend” problem is inherent in the internet. Sending a file to another person via email is an act of duplication: A copy of the data is sent, and a copy is retained by the sender. That’s problematic when it comes to money. It’s critical when someone executes a digital transfer of money that the money doesn’t remain in her account as well as that of the recipient. This requires one or more intermediaries to ensure that payments wind up in the right place and that the funds are deducted from the sender’s account. This creates friction, delay and cost and allows other entities (banks, money transfer firms, etc.) to know the details of transactions.

Programmable money, or cryptocurrency, represents an attempt to address these issues and evolve money once again. Today’s widespread use of digital fiat money is unquestionably an improvement from the analog world, and cryptocurrencies are intended to disintermediate centralized authority from digital payment systems in order to establish a genuine decentralized peer-to-peer transaction network without the friction, cost and oversight of middlemen.

“Instead of relying on a central trusted authority, such as a bank, to validate holdings and transactions, bitcoin and other cryptocurrencies distribute information widely across distributed ledger technology and use advanced cryptography to assure the legitimacy and security of financial information.”
THE CREATION OF BITCOIN

Bitcoin was created in the wake of the 2008 financial crisis, a period in which financial institutions around the world teetered, the stability of monetary systems was called into question, and global central banks adopted policy roles far beyond their original charters. In the midst of the crisis – on Halloween in 2008 – a white paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” was posted to a cryptography listserv. The purported author was Satoshi Nakamoto, a name that has never been positively linked to any known individual. Nakamoto – whoever he, she or they are – proposed a framework for a genuine peer-to-peer network that would establish trust without the presence of a central authority, solve the double-spend problem and disintermediate institutions as well as government entities such as central banks. The opening paragraphs of the nine-page paper propose that:

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. … What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

The tech community was intrigued by the notion that cryptography might replace institutions, and the libertarian community liked the idea of economic transactions without third-party oversight. Furthermore, for people concerned that central banks were debasing sound money in the pursuit of political goals, a currency free from government influence held great appeal. Unsurprisingly, some of bitcoin’s earliest advocates hailed from countries plagued with rampant inflation and confiscatory government policies. Finally, bitcoin offered an opportunity to lower transaction costs and time by disintermediating institutions whose very economic models were based on transaction fees.

Instead of relying on a central trusted authority, such as a bank, to validate holdings and transactions, bitcoin and other cryptocurrencies distribute information widely across distributed ledger technology and use advanced cryptography to assure the legitimacy and security of financial information. Anyone with sufficient computing power may join the bitcoin network and participate in the validation effort. Successful validations are rewarded with newly created bitcoins. This distributed ledger technology is called blockchain.
HOW DOES BLOCKCHAIN WORK?

Information is traditionally stored in a central location. Your bank has a record of balances and financial transactions, your doctor’s office holds your medical records, and various government entities hold a wide range of personal information such as Social Security numbers and tax returns. The beauty of centralized storage is that you know where to go to find the information you need. The downside is that the bad guys know this as well. In a world in which information is largely digital, central repositories can be (and often are) hacked, and it often takes days, weeks or months to realize it. Credit card numbers are stolen, identity theft is made possible, and celebrities run the risk of embarrassing photographs showing up on the internet. Central points of control can lead to central points of failure.

A blockchain, on the other hand, can spread this same information – appropriately encrypted – across a decentralized network of computers, without the need for an authoritative intermediary such as a bank or government. A blockchain is a type of distributed ledger technology, and, indeed, the two terms are often used interchangeably, although technically a blockchain is but one type of a distributed ledger approach to managing data.

Information contained within a blockchain requires a private key for someone to access it. These private keys are randomly generated numbers, with a nearly infinite number of possible combinations, making them difficult to the point of impossible to crack. A blockchain furthermore employs cryptographic security to ensure that information cannot be added, deleted or changed without a rigorous, costly and time-consuming application of an algorithm that confirms the new data, while linking it to all the previous data in the chain. A majority of the network participants must agree to a change, so a breach in one or even multiple points on the network doesn’t compromise the data.

On what basis do network participants agree to changes? Here is where rather advanced cryptography enters the picture.

New information (financial transactions, medical test results, etc.) is accumulated into blocks over a period of time, with the specific data encrypted so that only the holder of the correct private key can see the underlying information. Now it gets tricky. Network participants apply an algorithm, also known as a cryptographic hash function, to the block of encrypted data in order to create a unique identifier for the entire block. Bitcoin uses the SHA-256 cryptographic hash algorithm, created by the National Security Agency, but there are many others.

A hash function turns the block of data into an output (called a hash value) that appears to the naked eye to be a random string of numbers and letters, but always of a fixed length. The first feature of a hash function is that the same input must always result in the same output (hash) value. Since all network participants are working with the same input value, or block, to start, the output (hash) value will also be the same. Next, participants add to the block an arbitrary piece of input data (called a “nonce” in cryptography) so that the hash values created by different network participants differ, even when applied to the same block of data.

A second feature of a hash function is that the slightest change in the input data results in a completely different hash value. As the block data doesn’t change, the hash value only changes as a result of alterations to the random, or nonce, inputs.

See the nearby example for an illustration of this. Using the SHA-256 algorithm, the string “To be, or not to be” creates a completely different hash value when we change just the punctuation at the end of the phrase. Because the same input always translates to the same hash, you can try this at home. Google “SHA-256 encoder” and have fun!

The goal for network participants is to find a random, or nonce, input (like the punctuation mark in the nearby example) that,
when combined with the block, results in a hash value that meets certain preset conditions. Those conditions can be made more difficult in order to manage the speed of the process. The bitcoin protocol requires that a successful hash value begin with a certain number of zeros. The required number of zeros is somewhat arbitrary but changes over time in order to manage the difficulty of arriving at an appropriate hash value. This has a particular importance to cryptocurrencies, as the network participant who derives the appropriate hash value earns coins for her efforts. If solutions are occurring too rapidly, and therefore too many coins are being minted, the difficulty is raised, and vice versa.

A cryptographic function, such as SHA-256, is applied to ...
... a set of data common to all network participants ...
... plus an additional input unique to each participant designed to ...
... arrive at a hash value (output) with certain desired characteristics

Arriving at the desired string of zeros is an exercise in trial and error, which requires extraordinary computing power to work through (or “mine”) enough combinations. As of April 29, successful hash values on blocks of bitcoin transactions begin with 18 or 19 zeros. Again, try this at home by inputting random strings into an SHA-256 encoder for an easy demonstration on how difficult it is through brute force to derive a hash value that starts with just two zeros. Professional bitcoin miners use systems that can calculate trillions of hash values per second.

Once a hash value is found that meets the desired difficulty criterion, the solution is published to the network so that other participants can confirm the solution by combining the nonce value arrived at by the winner with the original input data from the block that everyone started with. This hash value is a digital fingerprint that is associated with one and only one block of data. Once determined, the nonce value for a particular block has no further use, as the next block of data will require a completely new random addition to create the desired hash value.

A final important feature of a hash function is that one can’t work backward from the hash value to the underlying data. The hash function, in other words, is a one-way cryptographic function. It can’t be used to reveal the underlying data, but it can be used to verify it. This is, by the way, how online passwords work. When you input a password into a website, the site itself doesn’t know your password – only the hash value associated with it. If you mistype the password – even slightly – the hash value doesn’t match, and the entry is rejected. The website doesn’t know what you know (your password), but cryptography allows it to know that you know what you know.

Once an appropriate hash value is derived for the current block of information, it is added to the chain of all previous blocks, and the cryptographic algorithm is applied again to the newly enlarged chain. This iterative hash process creates yet another unique hash value, or fingerprint, that now applies to the whole chain.

Because the cryptographic hash function is applied to new blocks as well as the whole chain, the integrity of the entire chain is constantly revalidated. Any attempted change in the entire chain of data – an attempted breach, for example – is rapidly identified and rejected.
Nakamoto’s white paper was turned into an operating protocol a few months later, and the first block was added to the blockchain – and the first bitcoins created – in the first week of January 2009. For over a year, the system remained nothing more than a libertarian experiment and a technological novelty. The number of people or computer nodes adding to the blockchain was quite small, and no one knew what to do with the bitcoins being created other than count them and occasionally trade them to each other.

A milestone took place on May 17, 2010, when an early adopter by the name of Laszlo Hanyecz posted a request online to trade bitcoins for pizza. A counterparty agreed to the transaction, and Hanyecz paid 10,000 bitcoins for two pizzas from a restaurant in Jacksonville, Florida, marking the first time that bitcoin was used in a commercial transaction. At the time, the dollar value of the transaction amounted to roughly $41. Those 10,000 bitcoins today would be worth around $89 million. We hope that Hanyecz got all the toppings on his pizzas.

Early bitcoin users leveraged the pseudonymity of bitcoin transactions to skirt anti-money laundering (AML) and other laws. Infamously, the Silk Road online marketplace for illicit drugs was launched in 2011 to match buyers and sellers and accepted only bitcoin in payment. (The site has been subsequently shut down, and its creator is serving a life sentence without possibility of parole.)

The legitimate use of bitcoin has skyrocketed. There are now 16,992,510 bitcoins in existence (as of April 29), with ultimate issuance capped at 21 million. There are 21,896,733 bitcoin addresses, each holding an average of 0.77 bitcoins. (Addresses represent specific holdings of bitcoins and can be aggregated into wallets.) Over the past year, volumes have averaged almost 263,000 transactions per day, representing an average daily commercial value of $1.5 billion.

Bitcoin is far from the only cryptocurrency in circulation. The bitcoin operating protocol is open source, which has allowed participants to tweak, change, shift and improve the bitcoin process to launch new cryptocurrencies so that, at last count (April 29), there are 1,589 cryptocurrencies in existence, using a variety of cryptographic algorithms. A new cryptocurrency is created through an initial coin offering (ICO), which raises funds for operations of a new currency through the issuance of that very currency. Bitcoin remains the largest cryptocurrency by far, accounting for 38% of the total value of cryptocurrencies. The five largest cryptocurrencies add up to 70% of the entire market.
IS BITCOIN A CURRENCY?

The answer to this question lies at the heart of the debate about bitcoin's viability. Proponents certainly believe that it and other cryptocurrencies can and should replace traditional fiat currencies, and retailers (particularly online) are increasingly beginning to accept cryptocurrencies alongside credit cards, PayPal and other traditional transaction mechanisms. This clearly argues that it is, or is at least becoming, a currency.

Economists would, for the most part, disagree. A thing has to meet three specific requirements to be considered a currency, and, despite their nomenclature, cryptocurrencies don’t yet meet any of these. First, a currency must act as a store of value, or a way to preserve value in anticipation of future spending. As the nearby bitcoin price chart demonstrates, bitcoin’s price has been anything but stable. From a low of $789 per bitcoin in early 2017, the price soared to a peak of $18,674 in December of last year, only to settle back to a current level around $9,000. (And, by the way, traded as low as a nickel per bitcoin in 2010.) This represents a rally of 2,267% over the course of 12 months, followed by a collapse of 52% in the space of a quarter. One would be hard pressed to claim that this degree of volatility represents a store of economic value.

Second, a currency must serve as a unit of measurement. Although more and more retailers are accepting bitcoin, they continue to price their goods and services in dollars, which are then translated into bitcoin at the prevailing exchange rate upon checkout. It is not a standard of measurement, at least yet, and until the price volatility settles down, it will be impossible for companies to set prices in bitcoins. Furthermore, companies will be understandably reluctant to price in one currency (such as bitcoin), if their costs remain denominated in another (such as dollars). To do so is to introduce potentially catastrophic currency risk into the operation of a business.
The top 100 bitcoin addresses hold close to 20% of all outstanding bitcoins, and the costs associated with mining new bitcoins is likely to increase that concentration even further. Concentration in other cryptocurrencies is even higher.

Finally, a currency must act as a medium of exchange. As discussed, bitcoin and other cryptocurrencies are increasingly accepted for financial transactions, but those transactions remain denominated in dollars. As long as companies continue paying suppliers and employees in traditional currencies, received bitcoins will be exchanged for dollars in order to pay those costs.

Perhaps the best way to gauge whether or not bitcoin is a medium of exchange is to conduct a simple thought experiment. Why do people acquire bitcoin? We believe that most traders are buying in anticipation of the price of the cryptocurrency rising, as measured in dollars or some other fiat currency, as opposed to buying in anticipation of using the cryptocurrency in a financial transaction.

We can measure this, at least to some degree, by analyzing the size and number of bitcoin addresses in existence. Thanks to the transparency of the blockchain, this information is publicly available and frequently updated. As of April 29, the 100 largest addresses owned 19% of all extant bitcoins, and of 21,896,733 total addresses, 21,196,732 (97%) owned less than a single bitcoin. This disparate ownership, on the high end, reflects a desire to hoard in expectation of rising prices. On the other (low) end, roughly 21 million people are curious enough to open an account and fund it with (on average) 0.03 bitcoins, worth $290 at current prices. Bitcoin holdings are quite concentrated, and ownership of other cryptocurrencies is even more concentrated.

So the market hasn’t, at least yet, adopted bitcoin as a true currency. The taxman agrees. In a ruling issued in March 2014 (Notice 2014-21), the Internal Revenue Service (IRS) stated that virtual currencies will be treated as property according to U.S. tax law, incurring capital gains or losses when bought or sold. As with other property, such as stocks and bonds, different rates are applied to short-term (one year or less) and long-term (more than a year) gains and reported on Schedule D of the IRS 1040 filing.

Furthermore, the IRS has ruled that even when used in transactions, the difference in U.S. dollar value in the cryptocurrency from the date of purchase to the date of use is also treated as a capital gain or loss. For example, if someone bought bitcoin at $1,000 and then used it to buy a new Tesla on a date when bitcoin was worth $8,000, the $7,000 difference is a gain on which she owes tax.

This is more than a quirk in the tax law. For the past few years, only about 800 tax returns per year have disclosed and paid tax on cryptocurrency gains, and the surge in cryptocurrency prices has attracted the attention of the IRS. In 2016, the IRS asked for details on cryptocurrency wallets held at Coinbase (one popular cryptocurrency exchange) and will likely step up its enforcement actions on noncompliance even more in the future. If you are trading or using cryptocurrencies, be sure that you have a knowledgeable and capable accountant who is fluent in the tax implications.

“...
RISKS

Taxation is just one of many risks that cryptocurrency owners should be aware of. Ironically, one of the biggest threats is something that the very design is intended to avoid: hacking. Many smaller owners of cryptocurrencies hold them in an online exchange for the sake of convenience. Recall that “owning” a cryptocurrency is simply having possession of a private key that allows the owner to exchange, spend or move a coin. If that private key is stored online in a central location, hackers can obtain it and effectively steal the holding without recourse. Multiple exchanges have been hacked over time, most recently when hackers infiltrated the Japanese exchange Coincheck in January 2018, making off with $530 million of cryptocurrencies. Coincheck partially refunded customers’ losses but was under no obligation to do so.

The regulatory environment for cryptocurrencies poses another challenge. Government agencies around the world are trying to determine how to regulate a rapidly evolving market where value can change hands instantaneously and pseudonymously. Some countries – particularly those that exercise more control over their citizens’ financial transactions – have simply banned cryptocurrencies outright, or at least prohibited their use in commercial transactions. The developed world is more hospitable but is struggling to develop central regulatory oversight of a market explicitly designed to avoid central oversight. In the United States, it is unclear how authorities can apply AML rules and anti-terrorism regulations such as the Patriot Act to the use of cryptocurrencies. Clearer or tighter regulations could reduce the appeal and price of cryptocurrencies.

As noted, one of bitcoin’s features is that its supply will be limited to 21 million coins. Unlike central banks, which can create currency by expanding their balance sheets, bitcoin avoids the risk of debasing its value by imposing a hard cap. This is the primary reason that advocates believe the price of bitcoin should continue to rise: Good old-fashioned supply and demand says that rising demand and limited supply lead to higher prices.

Yet as also noted, bitcoin isn’t the only game in town. Being the first in an industry is usually regarded as a benefit, but this first-mover advantage doesn’t necessarily apply to the world of technology. The parallel to the dot-com boom of the late 1990s is apt. Plenty of first movers were washed out in the bust that followed – remember AOL, Netscape and Napster? This analogy doesn’t guarantee that bitcoin will follow suit, but the plethora of other cryptocurrencies implies that supply might not be as constrained as originally thought. Indeed, the economics of commodity markets implies that as prices rise, participants seek out substitute commodities (such as other cryptocurrencies), thereby expanding overall supply.
The real game changer in this story is blockchain. The ability to establish trust without a central authority, and validate information and transactions through a genuine peer-to-peer network, creates a brave new world that leads to lower friction, faster transactions, better efficiency, tighter security, improved productivity and higher margins.”

One development to watch is whether or not central banks enter the cryptocurrency game by creating their own national cryptocurrencies. Opponents argue that this contradicts the very benefit of cryptocurrencies by reintroducing central authority and removing pseudonymity of ownership and transactions. A central bank cryptocurrency (CBCC) would, on the other hand, offer appropriate regulatory oversight while improving the existing system of payments. The point is that the threat of competition to cryptocurrencies, and bitcoin in particular, is rising.

The concentrated ownership of cryptocurrencies poses an additional risk. The top 100 bitcoin addresses hold close to 20% of all outstanding bitcoins, and the costs associated with mining new bitcoins is likely to increase that concentration even further. Concentration in other cryptocurrencies is even higher. Not only does this constrain bitcoin’s use in commercial transactions, but it also heightens the risk of manipulation as large holders decide to buy or sell in massive quantities. This isn’t just theory or speculation: A January 2018 article in the *Journal of Monetary Economics* concluded that the rise in the price of bitcoin from $150 to over $1,000 in late 2013 was attributable to a single actor pushing up the price.¹

Crypto markets are far larger today, but the combination of concentrated ownership and thin trading volumes still makes them ripe for manipulation. Furthermore, it is not clear that collusion among players to move markets would be illegal. Bitcoin is not a security, and therefore does not fall under the Security and Exchange Commission’s (SEC) regulations regarding insider trading. But to add to the regulatory morass, the SEC seems to make a distinction between pure cryptocurrencies like bitcoin and other, more project-specific tokens, the latter of which are considered securities. In testimony to the House Committee on Appropriations on April 26, 2018, SEC Chairman Jay Clayton noted that:

> It’s a complicated area. … [T]here are different types of crypto assets. Let me try and divide them into two areas. A pure medium of exchange, the one that’s most often cited, is bitcoin. As a replacement for currency, that has been determined by most people to not be a security. … Then there are tokens, which are used to finance projects. I’ve been on the record saying there are very few, there’s none that I’ve seen … that aren’t securities.

In other settings, Clayton has opined that any cryptocurrencies created through an ICO qualify as securities, which would include most of the cryptocurrency market today. In his testimony to the House Appropriations Committee, Clayton observed that “This area has grown substantially without the usual respect for the law that you would expect to see in financial markets.” A regulatory crackdown on the issuance of cryptocurrency seems inevitable.

A final risk to cryptocurrencies is economic. If bitcoin and other cryptocurrencies are to genuinely threaten the existing payment system in the United States, scalability is an obstacle. As shown in an earlier graph, over the past year, bitcoin transactions have averaged about 260,000 per day and about $1.5 billion in aggregate daily value. That implies an average of $5,400 per transaction, which is far above the level of a routine commercial transaction. Visa, in contrast, processes 150 million credit card transactions per day, with an average charge of $66. To replace existing payment systems, bitcoin transactions must become faster and easier.
THE FUTURE

We opened this article by characterizing the history of currency as a collective story we tell ourselves about value. Cryptocurrencies are writing the latest chapter in this story by challenging the notion that currencies must be issued by a sovereign state and that they require a central authority to make them work. Perhaps the biggest challenge facing bitcoin and its peers is that the incumbents – fiat currencies – are entrenched competitors with a powerful network value. Contrary to the occasional claim that the U.S. dollar is backed by nothing more than an unelected board of Federal Reserve governors, in reality the greenback is valuable because it greases the wheels of a $19 trillion economy, as well as serves as the global reserve currency. This is a tangible expression of this rather old and powerful collective story.

Having said that, we are convinced that cryptocurrencies have a role to play in the digital economy. We don’t believe that they will ever replace fiat currencies, but in a world increasingly defined by digital assets, why shouldn’t a digital currency play a role in acquiring those assets? There is no reason that cryptocurrencies and fiat currencies shouldn’t coexist.

The uncertainty, chaos and volatility that accompany the current menagerie of cryptocurrencies are common features of technological change and remind us of the similar environment in the late 1990s that accompanied the dot-com boom. This earlier technological revolution changed forever the way we live. Consumers were the clearest beneficiaries: Investors in the early days of the dot-com boom had to suffer through the painful bust that followed. We believe that cryptocurrencies markets are headed for a similar shakeout before becoming an established factor in the digital economy.

Cryptocurrencies are not likely to play a role in clients’ portfolios at Brown Brothers Harriman (BBH), either before or after this expected reckoning. We invest in assets with an identifiable intrinsic value. Our investment success is not predicated upon price anticipation, but on value recognition. Assets without intrinsic value – such as currencies and commodities – do not fit within this value-driven framework. For us, currencies – whether crypto or fiat – are a means to the end of investing, not an object of investing in and of themselves.

Although the drama of volatile price action attracts most of the attention, we believe that cryptocurrencies are just an epiphenomenon. The real game changer in this story is blockchain. The ability to establish trust without a central authority, and validate information and transactions through a genuine peer-to-peer network, creates a brave new world that leads to lower friction, faster transactions, better efficiency, tighter security, improved productivity and higher margins. In addition to the usual technology suspects, companies from Walmart to British Airways to UPS and FedEx have already introduced blockchain technology into their business models. More will follow.

BBH marks its 200th anniversary this year, and we’ve seen plenty of disruptive innovation over the past two centuries. We are keenly aware that the impact of technological innovation is always overstated in the short term but understated in the long term. The role that blockchain and cryptocurrencies play in the 21st century economy is likely to reflect this truism.
