WHITE PAPER

BITCOIN

BY **MORROW BAILEY**
SENIOR VICE PRESIDENT

Bitcoin (BTC) is a decentralized application that enables trust-minimized payments to anyone, anywhere in the world. BTC transactions are recorded on a *blockchain*, a distributed ledger controlled by no single entity. A good way to think about BTC is as a computer program that, like any program, just abides by the rules its creator promulgates. As an interesting aside, no one knows who that creator is. The original BTC paper was signed under the *nom de plume* Satoshi Nakamoto, but whoever s/he is has not come forward. Satoshi created the program, exited stage left, and all that has happened since is the result of others interacting with the rules s/he set forth.

continued on next page ›

While BTC is a cryptocurrency, it will not obviate the need for government-backed fiat currencies anytime soon (very likely, never). A currency must fulfill three major functions: (1) medium of exchange; (2) unit of account; (3) store of value. How does BTC perform on each of these dimensions? As a medium of exchange, it fails miserably. Very few merchants accept it, one cannot pay their taxes with it, and neither of these are likely to meaningfully change any time soon. As a unit of account, BTC is also not a winner. A key attribute of a good unit of account is stability and BTC has been anything but, with its dollar-denominated price doubling in the past month. In contrast, a doubling (or halving) of a major world currency in such a timeframe is virtually impossible outside of utter devastation from a war or a financial crisis. Likewise, such extreme volatility also makes BTC a not-so-useful store of value. In the past two weeks, it has been priced as low as ~$10,800 and as high as ~$19,600. While a 50% swing in a week might be exciting, an indicia of a stable store of value it is not! In addition to the foregoing limitations, BTC transaction processing capacity is capped at about 7-10 transactions per second. In contrast, Visa is capable of processing as many as 60,000 transactions per second across its network! Finally, if your private key (effectively your BTC password) is lost or stolen there is no recovery option, your bitcoin is forever gone. Do not pass Go. Do not collect $200.

So BTC fails as a traditional currency in an academic sense as well as in a more practical sense. Why, then, has its value soared so much? Three main reasons: scarcity, mobility, and censorship resistance. BTC is by definition a scarce asset. The program source code ensures that only 21 million will ever exist. In a world where all major central banks responded to the most recent financial crisis by printing exorbitant sums of money, a quasi-monetary asset that can never be debased by inflation holds obvious appeal.

If this argument sounds similar to the argument for owning gold, it is and it is not a stretch to say that a large number of BTC investors view it quite simply as digital gold. Typical arguments for owning gold center around its usefulness as an inflation hedge specifically and societal collapse more generally. Gold, like BTC, is not very useful as a medium of exchange (one does not often see customers transacting in bullion at the local grocery store) but has proven to be a good store of value over a long period of time. An oft-repeated anecdote that is perhaps true is that an ounce of gold has enabled its owner to buy a nice men's suit for generations. And gold is relatively scarce, although there is no absolute cap on its supply as there is for BTC, making it a good hedge against overactive government printing presses. However there are problems with gold ownership, and on many of these dimensions BTC is a superior alternative currency.

continued on next page ›

The major drawback is that, being both bulky and subject to theft, gold is expensive to store and hard to transport. While it might not be simple to own a bitcoin, storage costs are certainly much lower than they are for gold. Further, if one lives under the thumb of a repressive regime where wealth confiscation is a real threat, BTC is more amenable to cross-border transport than is gold. Private keys representing millions of dollars can circle the globe in their owner's pockets or even in their brains. Gold bars do not travel so easily in the pockets of anyone not of Brobdingnagian proportions.

Finally, as Chain CEO Adam Ludwin likes to say, BTC is censorship resistant. Since there is no centralized institution that runs BTC, assets on the BTC blockchain cannot be seized, access to funds cannot be blocked, and transactions are unstoppable. In this sense the BTC blockchain to some degree sits "above the law" at least relative to the traditional banking system where governments have an unquestioned ability to attach assets. While this is not unambiguously good (e.g. this attribute holds obvious appeal to criminals) it is also not unambiguously bad. If one lives in a place lacking well-defined property rights, confiscation of digital assets is much harder if not impossible to achieve compared to confiscation of more traditional physical assets.

So, given its limitations, BTC is probably not going to replace the dollars in your wallet or the electronic dollars in your bank account anytime soon. But it holds obvious appeal as a gold surrogate because of its scarcity, low storage costs, and mobility. Finally, it offers censorship resistance, a novel feature exhibited by very few, if any, other assets. While these attributes are interesting from a philosophical perspective the question that must be answered before BTC can be adopted on a broader scale is 'how can one trust a computer program colonized by strangers and which has no one in charge?'

Blockchain Risks and Promises

Trust, according to psychoanalyst Adam Phillips, is nothing more than a "risk masquerading as a promise." Who do you trust? Most people probably trust their family and close friends. Many likely trust their pastor, priest, or rabbi. On the opposite end of the spectrum, car salesmen and Congress routinely lead the way in Gallup's annual poll of the least trusted. Do you trust your bank? How much? Centralized power and its potential for abuse has been debated at least as far back as the first century when Roman poet Juvenal posed his now-famous question *quis custodiet ipsos custodes* (who will guard the guards themselves?)? Indeed, the mistrust of centralized power was a major concern of our forefathers, who designed our government with three branches and a system of checks and balances in an attempt to mitigate its potential hazards. Similarly, the

continued on next page ›

blockchain makes use of cryptography and a cleverly-designed incentive system to promote a system of checks and balances that work to ensure ledger integrity and promote user trust even though *there is no centralized point of authority*.

How does all of this happen? This is the real genius behind BTC. Third parties known as Miners compete to validate proposed transactions, because they are rewarded for so doing (in the case of the BTC blockchain, successful Miners are compensated with new bitcoin). Perhaps the best way to illustrate this is through a stylized example (courtesy of Rasheed Sabar at Ellington Management) contrasting a BTC payment with a typical bank transaction. Here's how I pay someone through my bank: I tell my bank that I want to pay my friend $50. The bank ensures that I authorized the payment and that I have enough funds in my account by comparing my request to their centralized ledger, essentially a (very long) list of all bank depositors and their account balances. If both conditions are met, the bank deducts $50 from my account and adds $50 to my friend's account.

Here's how the same transaction would happen on the BTC blockchain: I tell the community (Miners) that I want to pay my friend a fraction of a bitcoin equivalent to $50. The Miners ensure that I authorized the transaction by checking my digital signature, a unique identifier that only I know. At this juncture, things diverge from a traditional centralized bank. Multiple Miners check their individual copy of the BTC ledger (each Miner has a copy of the ledger, hence the name 'distributed ledger') to determine that I have enough BTC to send to my friend. So far, the only difference is that rather than having one centralized ledger, like the bank, BTC miners all over the world have many copies of the same ledger. Once a miner has verified that I possess the requisite funds, a competition begins to update the ledger with my new transaction. All miners who hope to update the ledger must solve a cryptographic puzzle by guessing a (very long) random number. This puzzle is both hard to solve (and therefore expensive…it has been estimated that BTC Miners collectively use as much energy as all of Denmark!) but easy to verify when it has been correctly solved, like a Rubik's cube. The first Miner to guess the correct random number broadcasts their answer to the entire network of Miners who check that the puzzle was solved correctly and if it has, all Miners update their individual ledger copy by adding a new "block" (my new transaction) to the existing "chain" (the distributed ledger). Last, the Miner who correctly solved the puzzle gets paid for their efforts in new BTC, and the process begins anew when another transaction is announced.

By incentivizing many Miners to participate while also making it costly in the form of energy consumption to propose ledger updates, BTC harnesses the safety of traditional banking controls without the potential for censorship associated with centralized control. For a Miner to defraud the system by proposing a fraudulent update they would also have to be the first to solve the

continued on next page ›

cryptographic puzzle associated with that update, something that could theoretically happen but the probability of which would be vanishingly small. For this reason there has been essentially no theft on the actual BTC blockchain.

So Satoshi designed a very clever incentive system that enables trust among anonymous parties thereby offering the accuracy of a traditional bank but without the tradeoff of potential censorship. While it might not function perfectly as a currency, BTC does share some similarities with gold and indeed appears to be even better than gold on several important dimensions. Given such a monumental achievement, BTC has to be a wonderful investment, maybe the opportunity of a lifetime, right?

Keynes, da Vinci, & Newton

In Chapter 12 of *The General Theory* Keynes contrasted the activities of *speculation* and *investing* (Keynes used the term "enterprise" rather than investing, but I have taken the liberty to update his terminology to a more modern usage), in a way that will be useful for us as we think about BTC's potential investment merits. He defined speculation as "the activity of forecasting the psychology of the market" and investing as "the activity of forecasting the prospective yield of assets over their whole life." Said differently, investing, at least intelligent investing, is the act of buying an asset for less than its *intrinsic value*, a conservative estimate of the cash flow it will produce over its life discounted back at an appropriate rate. An "investment" made on any other basis falls squarely into the camp of speculation. Interestingly, certain assets can *never* be investments under this definition because they will never generate unencumbered cash flow. Paintings, for example, or wine held as an "investment" are good examples. The converse, however, is not true. It is entirely possible to speculate in productive assets, as the tech bubble at the end of the last century proved. By the end of that episode, no one was buying a technology stock due to a sober appraisal of its long-term prospects. The investment thesis was 'these have been going up a bunch and therefore I think they'll continue to do so.' Or as Keynes more succinctly put it, tech investors were attempting to "forecast the psychology of the market", not their holdings' "prospective yield over their whole life."

In case the foregoing does not double underscore the point, BTC is not a productive asset and so any "investment" therein falls squarely in the camp of speculation. That does not mean that BTC and the blockchain will not change the world. But changing the world and producing strong investment returns are not always synonymous. Indeed, one of the great innovations of the 20th century was commercial air travel. However commercial airlines in aggregate have experienced a net loss since inception and virtually every mainline carrier has filed for bankruptcy protection, some more than

continued on next page ›

once. The fact that BTC is speculative, by my definition, also does not mean that it is destined to lose money. On the contrary, the price of BTC very well could increase a hundredfold from its current lofty perch. But forecasting mass psychology is an inherently challenging thing to do as the following examples will show.

Russian oligarch Dmitry Rybolovlev made headlines last month when he sold the 500-year old da Vinci painting *Salvator Mundi* at Christie's for an astonishing $450 million. Rybolovlev had owned the painting only briefly, paying just $127 million for it four years prior. Most interesting, however, is the story of why Rybolovlev decided to sell. As an established billionaire but neophyte collector, Rybolovlev turned to dealer Yves Bouvier for help building his art collection. Bouvier in turn sourced works like *Salvator Mundi* for Rybolovlev. It was apparently unclear whether Bouvier was acting as a principal for himself or an agent on behalf of Rybolovlev, a misunderstanding thrown into sharp relief when Rybolovlev discovered that Bouvier had paid only $80 million for *Mundi*, thereby netting himself a handsome $47 million "commission" upon flipping the piece. Disgusted, Rybolovlev sued Bouvier and began selling off his art collection in piecemeal fashion, incurring losses on many works in the process. Indeed Christie's had estimated that "Mundi" would likely only fetch in the neighborhood of $100 million. Needless to say everyone in the art world was shocked when the auction closed with a $450 million bid, 2.5x the previous most expensive auction price ever achieved of $179.4 million (fetched by a Picasso in 2015).

Perhaps the perfect counterexample to Rybolovlev's good fortune is Sir Isaac Newton--arguably one of the most intelligent people to ever live. Newton is estimated to have lost up to half of his fortune in the South Sea Bubble of 1720. Adding insult to injury, Newton appears to have sold all of his South Sea holdings well before the bubble burst, only to reinvest those proceeds weeks later at approximately double his sale price in a particularly brazen attempt to "forecast the psychology of the market." Even an intellect as towering as Newton's, it would seem, is not immune from the Buffettism that "nothing sedates rationality

continued on next page ›

Important Notes And Disclosures

like large doses of effortless money." After the bubble deflated, Newton is reputed to have forbidden anyone to speak the words 'South Sea' in his presence for the remainder of his life!

That's the thing about speculation, no one knows how it will turn out because mass psychology is fickle, subject to change violently at a moment's notice and for no good reason whatsoever. Rybolovlev speculated, thought he was going to lose a fortune, and ended up netting over $300 million in the process. Newton speculated, thought he was going to make a fortune, and ended up nearly going broke in the process. In light of these two cases, what, then, is the appropriate value for bitcoin? I'll outsource my answer to famed Austrian-British philosopher Ludwig Wittgenstein, "whereof one cannot speak, thereof one must be silent."

Even though bitcoin and the associated blockchain technology may be a monumentally good thing for the future of society, we at Diversified Trust have not included it on our investment platform and it is doubtful we ever will. We simply can't determine if we would, metaphorically speaking, be Dmitry Rybolovlev or Sir Isaac Newton. So we will press on, bitcoinless, guided by noted luminary Mark Twain's sage advice: "There are two times in a man's life when he shouldn't speculate: when he can't afford it and when he can."

ATLANTA

400 Galleria Parkway, Suite 1400
Atlanta, GA 30339
Phone: 770.226.5333

GREENSBORO

701 Green Valley Road, Suite 300
Greensboro, NC 27408
Phone: 336.217.0151

MEMPHIS

6075 Poplar Avenue, Suite 900
Memphis, TN 38119
Phone: 901.761.7979

NASHVILLE

3102 West End Avenue, Suite 600
Nashville, TN 37203
Phone: 615.386.7302