Wilshire

Alternatives Research

Digital Assets: Potential Roles and Risks in Institutional Portfolios

September 2021

Michael Rush, CFA, Senior Vice President
John Holton, CAIA, Senior Associate
Kaivon Razavi, Associate

Contents

Preamble

The re-emergence of cryptocurrencies and their eye-popping returns has once again captured the attention of the institutional investment community. While the adoption and growth of the digital assets' universe are still in their very early stages, considerable operational improvements have transformed the space[1] from one that was untenable for institutional investors to one that might now begin to legitimately compete for allocations within portfolios. While the proverbial air came out of the crypto "bubble" following the 2017-2018 price surge, the digital assets universe continued to evolve. Large sums of both human and financial capital were drawn to the space while key areas of operational concern improved, such as custody, administration and audit. While these assets are still speculative and quite volatile, Wilshire believes there are multiple implementation options for risk-tolerant investors with an interest in attaining exposure to digital assets, whether through direct investments into cryptocurrencies/coins/tokens or via commercial enterprises engaged in the expanding area of digital asset infrastructure and/or decentralized finance. This paper is designed to serve as an update to Wilshire's 2018 paper,[2] which provided introductory and educational information related to blockchain technology and Bitcoin—the world's first cryptocurrency. Building from that background, this iteration focuses on implementation options for investors with various perspectives on digital assets and attempts to review both the improvements and remaining risks to investors. An updated series of appendices regarding blockchain, Bitcoin, and other applications of the technology is included. We encourage readers who are new to digital assets to begin with Appendix A, as that section provides useful background and context that may be helpful in appreciating the paper's main body.

Executive Summary Introduction

Bitcoin – the world's first cryptocurrency and largely synonymous with the entire realm of digital assets – once again rose to prominence during arguably the most eventful and globally meaningful environment in recent memory. In a year characterized by a global pandemic, widespread lockdowns, supply chain disruptions, and unprecedented monetary stimulus on the part of central banks around the world, Bitcoin managed to insert itself into the conversation with a calendar year return of over 300% (Exhibit 1). While the previous run-up felt in some ways premature, recent history has shown a large stepwise change in both adoption and security. While an exhaustive list of landmarks would be too tedious, a few on the adoption side include: allocations from prominent institutional investors like Harvard and Yale, integration to the PayPal and Square platforms, inclusion on corporate balance sheets like MicroStrategy and Tesla, notable investments from respected investors like Paul Tudor Jones and Alan Howard, inclusion into quant hedge funds and CTA trading programs, recognition of Bitcoin as legal tender in El Salvador, and finally increased long-only access to investors through reputable investment managers (e.g. Fidelity Bitcoin Fund).

Many of these milestones have been accompanied and enabled by operational improvements within organizations and functions necessary for investing. Security has always been top-of-mind for investors entering the digital assets space. The influx of blue-chip service providers has helped mitigate many of these concerns. Common service providers to digital assets investment managers now include custodians like Fidelity, the familiar "Big Five" audit firms, and leading administrators like SEI and Northern Trust. While these entrants do not fully mitigate operational concerns for digital assets (as they do not for any traditional asset), the improvements have opened the door for institutional investors to seriously consider allocations, whether via direct investments, through a variety of instruments and derivatives, or investment managers. To the degree investors align with the commonly cited investment merits of digital assets, such as a store of value or as a claim on the disruptive growth from a revolutionary technology that may literally transform the future of economic commerce, Wilshire believes there are corresponding implementation options that can give investors exposure in a more risk-controlled way.

[1] While we typically attempt to limit our use of terms like "space" and "area" when referencing investment opportunities, as they are both vague and risk a jargon-tone, we do use such generic terms (and others) throughout this note. We do so for convenience and to specifically avoid using the term "asset class," as we believe that the use of such a common label risks overstating the current potential uses of digital assets within institutional portfolios versus where these opportunities are in their life cycle.

[2] Wilshire Associates Incorporated (2018). *Cryptocurrencies: Thoughts and Concerns for Institutional Investors*: Rush and Lesh.

Exhibit 1

Data Source: Yahoo Finance

Investing in Digital Assets

Institutional Investment Options

Until a few years ago, institutional investors had few avenues to gain exposure to digital assets. The operational improvements that have been made have facilitated implementation through a variety of instruments (direct, futures, options) and investment vehicles (long-only funds, hedge funds, private equity/venture capital). Below is a brief summary of the investment options that are currently available (see Appendix C for an expanded discussion of these options).

Exhibit 2

Investment Options	Description	Pros	Cons
Outright Digital Asset Purchases	Purchasing digital assets on the market via an exchange	• Direct exposure to digital assets with no basis risk	• Low liquidity outside of leading assets • Exchange risk and custody responsibility
ETFs, ETNs, and closed-end funds	ETFs have not yet been approved in the U.S., but there are several ETNs and closed-end fund options	• Better liquidity • Investor doesn't hold private keys	• Could trade at significant premiums/discounts
Futures and Options	Bitcoin and Ether futures contracts, as well as listed options and various OTC derivatives	• Better liquidity • Investor doesn't hold private keys • Ability to short	• Poor liquidity relative to traditional futures markets • OTC market lacks standardization
Public Equity ETFs	Exposure to a bucket of public companies with blockchain in their business models	• Better liquidity • Less volatile than broader space • Low transaction costs	• Basis risk to direct digital asset exposure • High exposure to companies benefiting from Graphics Processing Unit demand
Crypto Lending	Loans facilitated by CeFi or DeFi lending platforms collateralized by digital assets	• Yield-based, lower volatility return profile • Typically overcollateralized • Compelling yields versus public fixed income	• Risk of financing bad actors through DeFi • High volatility of underlying collateral
Long-Only Investment Funds	Long exposure to one or multiple digital assets through a third-party asset manager	• Direct exposure to digital assets with minimal tracking error • Custody risk taken on by manager	• Lack of trading flexibility during bear markets • Limited institutional manager landscape

Investment Options	Description	Pros	Cons
Hedge Funds	Active trading of digital assets, ranging from fundamental concentrated and long-biased funds to smaller quantitative long/short strategies	• Benefit from active management of crypto experts • Long-biased and Momentum strategies can be effective due to retail-driven market • Exchange arbitrage has less directional risk	• Asset-liability mismatch due to low underlying liquidity • Mass market manipulation clouds trading signals • Exchange arbitrage opportunity unclear
Private Equity	Invest in GPs making equity investments in blockchain-based companies or direct purchases in early-stage tokens	• No crypto custodial risk • Best asset-liability match given liquidity and investment horizon • Reputable PE firms can drive value creation in blockchain startups	• Rapid tech innovation can quickly outdate investments • Exposure to cryptocurrency market events • Highly exposed to regulatory change

Asset Allocation

While each of the investment options listed above have their respective pros and cons, most implementation options have historically aligned with (if not surpassed) the levels of economic risk and return commonly associated with venture capital (VC) investments, making their inclusion within an expanded VC allocation an appropriate and relatively frictionless decision for institutions. Such an approach is also well-aligned from a qualitative perspective, as many private equity-style funds include investments in both early-stage companies and early-stage tokens. This approach can also make sense for investors that have doubts about, or simply disagree with, the "macro" story that is often supported by crypto acolytes around fiat currency manipulation and debasement. Regardless of the investor's view on this argument, the broader technology disruption thesis related to blockchain technology is extremely compelling, as the applications of blockchain extend far beyond digital currencies and financial services to the very nature of contracts themselves (Appendix B expands on the potential applications of blockchain technology). This catalyst for disruption has already attracted thousands of people and billions of dollars to various companies and projects, resulting in several fund offerings focusing on private equity investments rather than digital currencies like Bitcoin. Of course, even if these fund offerings include a liquid trading component or substantially invest in early-stage or more-established coins like Bitcoin or Ethereum, the higher volatility and increased line-item risk still lend themselves to the closed-end vehicles typically utilized by private equity managers. Such investments force investors to view the longer-term merits of an allocation, rather than leave investors exposed to the behavioral biases to harvest gains prematurely or "panic-sell" during extended drawdowns. One helpful perspective is to imagine that all of your venture capital investments are no longer only marked on a quarterly basis, but are instead continuously traded, globally, across countless exchanges, by both large and extremely small investors. Though the transparency and observable volatility of digital assets is a new variable for the private equity investor, the true volatility of venture investments may, in fact, closely align with the price action we observe in digital assets today.

While a venture capital program may provide the easiest home for investments in digital assets, more-liquid approaches can lend themselves to other areas of investors' portfolios. As a macro-thematic investment, opportunistic, hedge fund, or liquid

alternative composites can serve as appropriate places for long-only or long-biased fund allocations.[3] Many hedge fund investors (e.g., Paul Tudor Jones, Alan Howard) view these assets as massively asymmetric trades within their portfolios. This asymmetry is easily comparable to an option position, regardless of what investors believe this option is on exactly (a future reliable store of value, "a technology as revolutionary as the internet itself," etc.). For investors positively pre-disposed to the idea that digital assets can supplant fiat currencies as primary stores of value, or simply serve as an inflation hedge, compelling arguments can be made for allocations within real asset, inflation-hedge, or entirely new crypto composites. Regardless of the investment thesis, implementation within a more-liquid structure (or on an outright basis) leaves investors subject to the high volatility of these assets, which likely warrants smaller allocations to mitigate undue portfolio noise and behavioral biases – at least until the volatility exhibited by digital assets subsides to a more acceptable level. For example, even if one subscribes to the idea that crypto currencies are a store of value and capable of playing a similar portfolio role as gold, their current volatility makes such a portfolio role incredibly modest in size. Consider that very few institutional investors hold gold today and, those that do, hold only modest positions (usually well less than 5%). As such, once reasonably risk weighed to adjust for their relatively high volatility levels, there is very little capital appetite available for an asset such as Bitcoin, for example, to replace or supplement gold exposures within institutional portfolios.

There are more arguments to be made about the specific characteristics of various digital assets and where they may end up in institutional portfolios in the future, but the volatile nature of the assets tends to also overpower these aspects. For instance, Bitcoin's sole function is to transfer value between individuals. This draws many comparisons to a currency or to the aforementioned gold (which has relatively limited industrial uses), but current volatility levels undermine these comparisons. Digital assets like Ethereum draw many comparisons to commodities given that other applications built on the network use Ethereum as the "fuel" for various transactions; however, utility-driven demand hardly drives price relative to sentiment around digital assets themselves. Even coins that distribute an application's profits to coin holders (decentralized autonomous organizations, or "DAOs") draw direct comparisons to equities, but the prior point on volatility still holds due to the less-established nature of these coins.

It is worth mentioning that many investors may already be getting incremental exposure to digital assets. Examples include equity managers trading companies like PayPal or Coinbase, companies with digital assets on balance sheet like Tesla, established private equity firms making investments in blockchain companies like Andreesen Horowitz, and macro hedge funds incorporating Bitcoin futures and options into their trading strategies. As resources continue to pour into the space and governments maintain a relatively benign regulatory stance, digital assets are poised to become a significant part of the conversation for institutional investors, even if they elect to abstain from that first dedicated investment.

Risks to Digital Assets

While we are encouraged that significant operational improvements have made allocations tenable in today's environment, digital assets are still in the very early stages of their life cycle, leaving institutional investors exposed to many ongoing risks and considerations. Below, we address relevant updates, milestones, and remaining areas of concern in three primary areas covering regulatory risk, transactability, and volatility.

Regulatory Risk

The cryptocurrency market is proving to be uniquely difficult to regulate, given that its global and private nature allows for relatively easy regulatory arbitrage. Though many benefits of digital assets are often linked to their decentralized nature, lack of regulation is also said to enable numerous frauds and Ponzi schemes, which have proved consistent headwinds for digital asset adoption. While there are some large cap coins that have raised concerns in the past (Tether, Ripple, etc.), most issues occur in smaller coins (commonly referred to as "alt coins"). One way to mitigate this risk is the use of active fund managers, or by simply focusing on the larger coins that have attracted the most investment and attention from the investment community. Due to the combination of its technological complexity and rapid expansion, the digital asset universe has a uniquely steep learning curve, making the use of experts particularly valuable in helping to mitigate coin-specific concerns.

[3] Most dedicated institutional quality funds today will likely be long-only or long-biased (which is understandable given the difficulty in shorting assets that can post 10x returns in a calendar year. Additionally, the still developing derivatives landscape makes shorting possible for a very few digital assets.

The larger questions related to regulatory risk ultimately center around the long-term viability of digital assets, rather than the inevitable short-term hurdles of a very novel investment opportunity. The decentralized nature of the market makes a largescale regulatory crack down from all major nations highly unlikely, and all incremental steps toward widespread adoption serve as additional mitigants against these existential risks. In the U.S. specifically, points of comfort include a benign stance by the SEC and CFTC to-date, former SEC Chairman Jay Clayton taking an advisory position at a digital assets hedge fund, and current SEC Chairman Gary Gensler previously serving as senior advisor to the MIT Media Lab Digital Currency Initiative. Conversely, the space has seen various crackdowns from nations like China and Iran, and concerns around Bitcoin's environmental impact and mining costs. More recently, investors have witnessed comments around the need for regulation from the previously mentioned and assumedly friendly SEC Chairman. Further, U.S. lawmakers have called for various regulatory changes to be included in the pending bipartisan infrastructure bill (H.R. 3684), which would have meaningful (and potentially nonsensical) implications around tax and reporting burdens for the digital assets space. Still, the question is not if digital assets will see an increase in regulation in aggregate, but more around the pace of innovation and adoption in spite of regulation, as well as investor willingness to endure the resulting volatility.

Transactability

Many make the intuitive case that digital asset and cryptocurrency values ultimately depend on user adoption. A simple chart of Bitcoin's users relative to price makes the relationship seem quite compelling. Adoption is a critical component to the maturation story of digital assets, though several caveats are required before advancing on the topic of transactability. First, not all digital assets should be regarded as cryptocurrencies. To the contrary, many projects exist for entirely different purposes. This does not negate the importance of well-functioning, efficient networks; however, it does serve as useful context when making comparisons. For example, the relevant benchmark for transaction speeds should be vastly different for a simple wallet-to-wallet coin transfer versus the execution of a complex smart contract. Additionally, there needs to be a recognition that other primary benefits of digital assets – security and decentralization – often come at the cost of speed. This tension is commonly referred to as the blockchain trilemma, which speaks to the tradeoffs that developers consciously make (between decentralization, speed/scalability, and security) at the onset of their various projects in the digital asset space. Still, scalability remains a primary concern when considering widespread adoption and everyday use by the broader population.

Bitcoin often receives the most criticism regarding efficiency being that the cryptocurrency was the first of its kind, has the largest market cap, and only serves as a transfer of value between parties. While Bitcoin's outright trading volume rivals that of the largest publicly traded equity securities, comparisons to current fiat payment systems are much less favorable. The Bitcoin network is capable of verifying a maximum of 7 transactions per second (TPS)[4], while the most-common payments network, Visa, can process over 24,000 TPS[5]. Furthermore, transaction fees are often burdensome. This does not necessarily eliminate the longer-term ambitions of Bitcoin to become a store of value, as many stores of value are less-liquid and more-costly to transact than fiat currency (furthering the conceptual comparison to gold). There are potential off-chain solutions to Bitcoin's limited scalability, such as the Lightning Network, but the hurdle remains relatively high for Bitcoin (or any other cryptocurrency) to become the world's dominant payments network. We expand on this further in Appendix B.

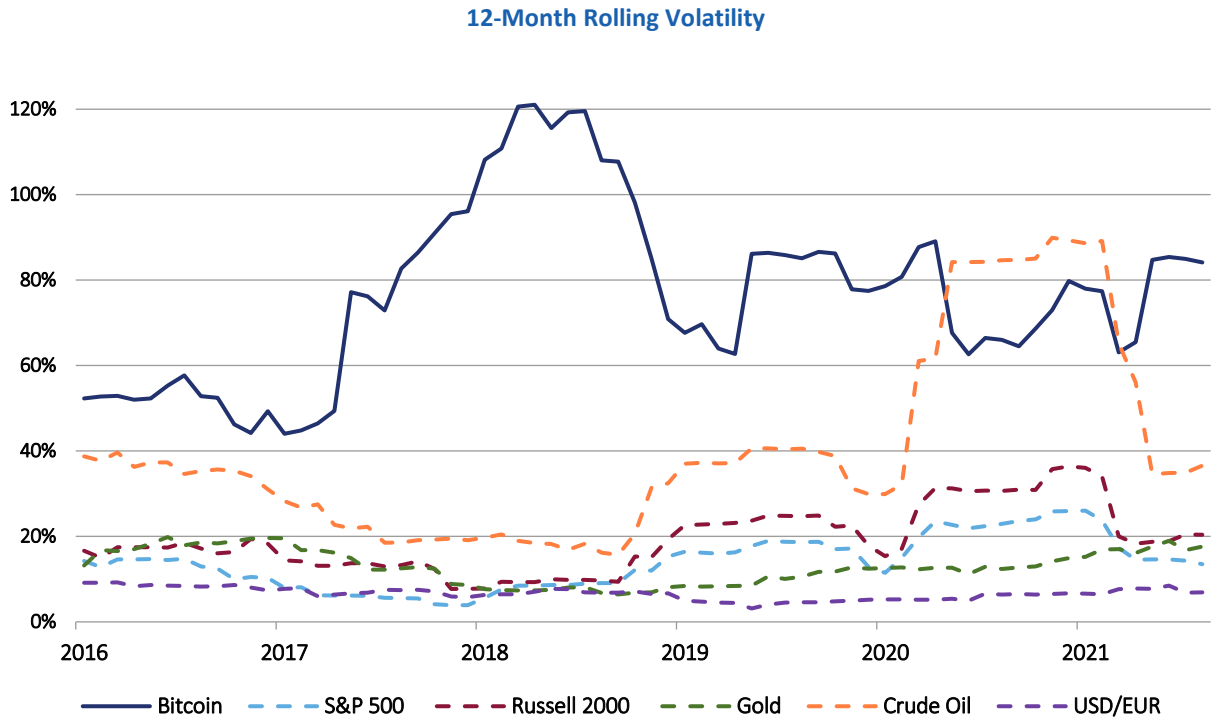
Volatility

As noted earlier, the adoption of digital assets has advanced meaningfully over the last few years and many of the operational hurdles for institutional investment have been substantially reduced. Still, there is a high degree of uncertainty in the early years of a new investment segment, and the market's primary signal of uncertainty remains elevated. Perhaps the largest hurdle for adoption – both by everyday users and investors – is the elevated volatility in the space.

[4] Croman, Kyle; Eyal, Ittay (2016). "On Scaling Decentralized Blockchains"

[5] Source: Visa, IBM

Exhibit 3



Data Source: Bloomberg

The volatility depicted above and its associated line-item risk serve as an impediment to institutional investment, while simultaneously undermining the thesis of Bitcoin as a future store of value. Furthermore, other coins often exhibit a high beta to Bitcoin and thus suffer from volatility contagion effects regardless of how diverse today's use cases are for digital assets. While it is helpful to exercise different perspectives when thinking about digital asset volatility – for instance, comparing a digital asset to a VC company or microcap stock – extreme volatility is likely to remain one of the more-stubborn hurdles for the digital asset universe. This volatility deters meaningful institutional inflows to the broader digital asset space, and thus further sustains the heightened volatility. Admittedly, the volatility and potential stabilization of Bitcoin will heavily influence the institutionalization of this unique investment opportunity, as this stabilization will allow other assets to trade on their own merits, and thus make digital assets more approachable from a fundamental standpoint, rather than remain a largely macro-driven, high risk, high reward, trade. While a continuation of current trends may slowly bring down volatility to more-approachable levels, the existing feedback loop is worth noting as a primary risk for investors for the foreseeable future.

Executive Summary Conclusion

During the second half of 2017, the price of Bitcoin – the world's first cryptocurrency and the flagship digital asset – surged by nearly 700%, before peaking in mid-December. Although the price retreated by roughly two-thirds the following year, investors took notice. Against the backdrop of a global pandemic, Bitcoin once again grew dramatically during the fourth quarter of 2020 and first quarter of 2021, up nearly 450%; far surpassing the heights achieved three years prior. A major difference between now and then, however, is that significant operational improvements have been realized in areas that are critical in supporting institutional investing. Important service providers, including custodians and audit firms, are now involved with digital assets. Additionally, several prominent investors have made allocations while some businesses have adopted digital assets as a small part of their business model.

The point about risk tolerance cannot be stressed enough. Returning to the specific example of Bitcoin, the standard deviation of the price of Bitcoin is approximately 80% during the past four-plus years. There are no broadly accepted institutional asset classes with long-term risk levels approaching those of Bitcoin. Greater adoption of digital assets and

investment dollars would likely reduce volatility, which then increases new investor interest. This reaction will likely be aided by the continued growth of the crypto derivatives market, continued operational improvements, and perhaps even increased regulation—which may drive short term volatility but ultimately provide long term comfort for the marginal investor. Still, it is unclear whether the operational improvements to-date are enough to bring about broad institutional approval. If and when that day comes, it will bring about a new challenge: benchmarking. The unique aspects of this investment opportunity suggests that the standard indexes that are widely used today will likely fall short of investor needs. Creating an acceptable benchmark for a relatively new and rapidly changing investment opportunity will be both challenging and will necessitate fluidity in addressing issues such as asset inclusion and concentration risk.

Wilshire believes that institutional investors with an understanding of the underlying complexity, and with the tolerance for the risks described above, should consider the potential portfolio role digital assets might play within a broadly diversified portfolio. Depending on the underlying investment thesis, possible entry points for digital assets within a diversified portfolio include venture capital programs, marketable alternatives (i.e., hedge funds/liquid alternatives), or even as part of a real assets allocation or inflation hedging basket. In doing so, position sizing should be appropriately scaled to accommodate the heightened level of uncertainty and the assets' extreme volatility.

Appendix A: Deep Dive into Bitcoin & Blockchain Technology

Introduction to Bitcoin

The first cryptocurrency was introduced to the world when a pseudonymous author, going by the name of Satoshi Nakamoto, published the Bitcoin white paper in 2008. Bitcoin was to be the first truly decentralized global currency and is still the most valuable by market capitalization today. The decentralized nature of Bitcoin is made possible through the technological breakthrough called "blockchain." At a high level, blockchain technology is a clever combination of existing cryptographic functions and economic incentives that has finally enabled the decentralized electronic exchange of value. Transferring value over the internet had historically only been possible if both sides of the transaction trusted a central authority (i.e. a bank) to facilitate the transfer. A trusted third party was necessary because of the "double spend problem." For an overly simplified example, imagine that Bob wants to send Alice one dollar. If Bob emails Alice a picture of a dollar, the image still exists on his computer so he can easily email the same dollar to someone else. Because of the double spend problem, the internet has only ever enabled the decentralized transfer of information as opposed to value. Satoshi Nakamoto solved the double spend problem by inventing blockchain technology.

Bitcoin claims to be completely "decentralized" and "trustless," which may be a suspect claim given that a single person or entity must have originally written all of the code that created Bitcoin and the rules governing the network. In fact, Bitcoin was far from decentralized when it was first created. When Satoshi Nakamoto published the first Bitcoin software in 2009, he was initially the only person running the code. It was only when more and more people began downloading the software that the network became "decentralized." The guidelines that had been coded into the software, such as how new Bitcoins are created and limits on how many can exist, are only the governing rules because they are agreed to by the majority of network participants. Once hundreds and then thousands of people joined the network, it was out of the creator's hands. The initial code was written so that the network would always be governed by consensus as opposed to a single entity. Consensus on the network is attained through the cryptographically secure operations and economic incentives that power the blockchain.

The Bitcoin blockchain has been running continuously since 2009 and has thus far proven immune to hacking. After years of what almost seem like weekly headlines announcing new high-profile hacks of governments or corporations, it is difficult to believe that something written in code can actually be as safe as blockchain claims to be. Fortunately, it is possible for someone without a PhD in computer science to understand how the ecosystem works and why the economic incentives make it so secure. Admittedly, anyone without a solid understanding of elliptic curve math and cryptographic hash functions will have to just trust that certain functions work as advertised. Many have chosen to take that leap of faith, if for no other reason than because no one has been able to successfully hack the blockchain after twelve years.

What is Blockchain?

The noun "blockchain" refers to a complete and accurate history of transactions that have ever occurred in its unit of account. It is a ledger, which, rather than being stored and downloaded from one central location, is distributed across a large network of peers (or nodes) who download and upload the ledger to each other. The cryptographic functions and economic incentives that underlie the rules of the blockchain ensure that the record of transactions is always accurate and complete. Because the ledger is distributed across thousands of network participants, blockchain is considered to be "decentralized" since no single entity is able to exert control over the network. Because there is no central point of failure for a hacker to target, blockchain is considered to be a highly secure method of value transfer.

Each "block" is a container for a group of transactions and successive blocks are "chained" together cryptographically to ensure the correct order of occurrence. In the days before computers, a business would record its transactions in a book. The book is analogous to a block, in that it is a container for a group of transactions. Once the book was full, the business would start a new book. A business could determine the correct order of all of its books by matching up the transaction dates, which is a simplified analogy to the "chain" that links blocks together.

Just as transactions in a U.S. business ledger are denominated in USD, transactions on a blockchain are denominated in its cryptocurrency. The difference, to echo a common initial apprehension towards Bitcoin, is that cryptocurrency is not tangible. In fact, the Bitcoin blockchain does not even have an explicit "account balance" to determine how much Bitcoin one owns. The only way to know how much Bitcoin is owned is to download the record for every single historical Bitcoin

transaction, single out every transaction involving a specific account, and add them up to find out the net amount that account holds. The reason why understanding the ledger is so critical to understanding Bitcoin is because Bitcoin's existence is entirely dependent upon, and derived from, the network's shared memory of every transaction record.

The Technology behind Blockchain

Blockchain technology is the term used to describe the innovation behind cryptocurrencies, but there is nothing new about the underlying technology. Rather, blockchain technology is a clever combination of three key technologies that have existed for decades – a description of which we provide below. A basic understanding of how blockchain applies these technologies from the start will facilitate a deeper understanding of the impactful possibilities throughout the economy.

Existing Technology #1: Peer-to-Peer Networks

A public blockchain, such as Bitcoin's, is shared between computers on a peer-to-peer network, as opposed to being hosted on a central web server. This peer-to-peer (P2P) network is actually the same technology that Napster made popular, and that is still used today, for file sharing among computers (i.e., via torrents). The benefit of hosting the ledger on a P2P network rather than on one web server is that there is no single point of failure for hackers to target. In a P2P network, a user downloads the ledger in pieces from other random users who are sharing their own personal copies of the ledger over the P2P network. After that user downloads their own copy of the ledger, the user can now allow others to download pieces from their copy. As more people download and share the ledger, it becomes more and more "decentralized." Cryptocurrencies like Bitcoin have incentive structures in place to encourage more people to download the ledger.

Existing Technology #2: Cryptographic Hash Function

Each cryptocurrency account that can transact on the blockchain consists of two addresses (called "keys"), one of which represents the account publicly on the blockchain. The second key is only ever known to the account holder and is aptly referred to as the "private key." The public key is analogous to an unbreakable safe whose contents and location are known by all. The account's private key is the combination to the safe, and it happens to be mathematically impossible to guess. The public and private keys are cryptographically linked via a decades-old breakthrough in cryptography called a "hash function." The private key is run through an algorithm – the hash function – which creates a seemingly random mix of numbers and letters: the public key. The function makes it impossible for anyone who only knows the public key to derive the original private key's code, even if they know the exact algorithm used in its creation. The incredible part is that every time the private key is run through the algorithm, it will always give the same exact output. The only way someone could figure out the private key is by testing every possible combination of random characters, one by one. The private key can be so long that it would be mathematically impossible to figure out, even with today's most advanced computers. The private/public key is just one example of how this hash function is used in the blockchain, but it is actually used in different ways throughout almost every element of the blockchain ecosystem. For example, when miners try to solve the cryptographic puzzle, all they are doing is trying to guess the input that generated a given output of a hash function. Miners are actually able to guess the input in this case because the network ensures that the difficulty (number of characters in the input) is such that it should take an average of ten minutes for the first miner to correctly guess the input.

Existing Technology #3: Cryptographic Digital Signatures

In order to send Bitcoin to another address, a trader must broadcast three items to the network: (1) their public key, (2) a message describing how much Bitcoin to send to whom and (3) their digital signature. The digital signature is able to prove to the rest of the network that the trader owns the private key without ever actually disclosing the private key. It is as if the holder of a key were able to prove possession of the correct combination to a safe without ever having to disclose the combination or unlock the safe. The digital signature is made possible with a set of algorithms that utilize unique mathematic properties of elliptic curves. Before the sender broadcasts the transaction to the network, the first algorithm uses the sender's private key, public key, and transaction message as inputs to create the "digital signature." When the network receives the three elements of the transaction, it runs them through a corresponding unpacking algorithm that is able to definitively determine whether the signature was created by using the account's private key. Never in this process does the holder ever have to disclose the private key. Applying this technology to cryptocurrency transactions on the blockchain ensures a "trustless" exchange of value, eliminating the need for a trusted third party (i.e., a bank) to be involved.

Mining the Currency

The Bitcoin network incentivizes users to verify and process new transactions by offering them newly created Bitcoin in return. This reward mechanism allows the blockchain to be entirely self-sustaining by ensuring that all new transactions are processed correctly while also controlling the introduction of new coin supply. People who believe that Bitcoin is worth more than the cost to earn it through this "mining" process can become "miners." Bitcoin is very similar to gold in that way, which is why the term "miner" is quite fitting. The addition of new miners to the network adds security by further decentralizing the ledger.

The rules governing Bitcoin state that every new block added to the blockchain comes with a certain amount of new Bitcoin to be credited to the individual who created the block. As such, a miner's only goal is to create the next block that the network adds to the blockchain. Recall that a block is just a container for a group of transactions. In order to create the next block, a miner will gather new transactions as they are broadcasted to the network until they have reached the block size limit. At this point, the miner will create a container for these transactions (a block) by performing a series of cryptographic hash functions to combine the transaction data until the miner is left with a seemingly random single string of numbers and letters called the "Merkle root." While it may seem random, any other computer could have performed the same series of cryptographic hash functions on the same data and would have come up with the same string of characters.

There is still more work for the miner to do before broadcasting the block to the network. In order for the network to accept the new block, the miner needs to solve a "cryptographic puzzle." A cryptographic puzzle is the term most often used in educational pieces in the industry, but it is not really a puzzle. The way it works is that the miner will combine the aforementioned Merkle root with a random number and run that through a hash function. If the output satisfies a pre-determined set of criteria set by the network, then they have solved the "puzzle." If it does not, then the miner will try adding a different random number to the Merkle root and run that through the hash function. They will keep trying random numbers until they find an output that meets the criteria for a solution. At the same time, every other miner is doing the same exact thing with their own blocks. Thus, there is a huge element of luck involved as to who solves theirs first.

The criterion for a valid solution is that the output begins with a certain number of zeros. If the network only requires the output to have one zero, it will take many fewer guesses than if it requires 20 zeros. The Bitcoin network actually adjusts how difficult it will be to find a solution so that the average time it takes for a miner to solve the puzzle is ten minutes. Every two weeks, the network looks to see what the average time to solve each block was over the prior two weeks, and then increases or decreases the level of difficulty (number of leading zeros required) accordingly. This method for confirming blocks is called Proof of Work ("PoW"). The same technology has been used for years for spam prevention, most recognizably by Microsoft Outlook. By forcing the computer to spend some amount of time calculating the "proof of work," Outlook can ensure that one cannot send millions of emails at once. At the same time, Outlook uses this technology to ensure that incoming emails have performed the "proof of work;" otherwise, they end up in the spam filter.

If a miner solves their block before any other miners, the miner broadcasts the block, and the solution to the block, to the rest of the network. If every miner were able to broadcast completed blocks to the network without performing the PoW, every miner would be able to submit many new, potential blocks every few seconds. The rest of the network would get extremely bogged down trying to figure out which one it should add to the blockchain. PoW ensures that only a minimal amount of completed blocks are submitted to the network, similar to how Outlook uses the same technology to prevent email spam.

Whenever a completed block is sent to the network, every computer connected to the network (called a "node") then tests whether each transaction in the newly completed block is valid before adding the block to their own copies of the blockchain. Validating the transaction consists of ensuring that the sender actually owns at least the number of Bitcoins they want to send. The node will search its copy of the blockchain for every transaction in which the sender's address has ever been involved. The node will then derive the amount of Bitcoin that the sender currently holds by adding all of their historical incoming transactions and subtracting all outgoing transactions. If the net amount they hold is greater than the amount they are trying to send, it is a valid transaction. If the majority of the network deems that the block is valid, the network agrees that the miner should receive the Bitcoin reward for that block. All of the other miners who did not solve their blocks in time will discard their blocks and start again with the next batch of transactions.

Appendix B: Blockchain Applications

Blockchain Applications – Currencies and Beyond

While digital currencies are the most ubiquitous application of blockchain technology since they are the headline unit of account in which transfers of value are recorded, the technology has moved far beyond currencies. Many of the largest cryptocurrencies today exist for entirely different reasons, all of which are made possible by "smart contracts." Ethereum is the first smart contract platform that allows developers to submit code to the blockchain that will automatically initiate transactions when certain criteria are met. Bitcoin transactions, on the other hand, only contain the information necessary to complete a peer-to-peer transfer of Bitcoin. Transactions on the blockchain can also contain other types of information, for example temperature readings and GPS coordinates of a crate of fruit as it moves along its supply chain. Ethereum expanded upon Bitcoin's original implementation of blockchain by allowing developers to utilize more of the capabilities that blockchain technologies offer in conjunction with smart contracts. Ether is the second largest cryptocurrency today but is really a "crypto commodity" because its primary use is to be the fuel that powers decentralized applications built on the Ethereum platform.

Applications of smart contracts may be able to take the place of the trusted intermediaries between transactions of all kinds, as they are more secure, faster, and less expensive. Potential applications exist across all industries and many regulatory functions, as is highlighted in Exhibit 4.

Exhibit 4

Financial Services	Technology, Media, Telecom	Consumer/Industrial
Potential Uses: • Trade finance • Payments • Regulatory info provision • Settlement and clearing • Lending • Fund distribution	Potential Uses: • Supports "internet of Things" • Lower priced micropayments • Securing intellectual property and digital creative works • Blockchain-as-a-service	Potential Uses: • Retail transaction payments • Digital signature technology • Streamline receivable

Healthcare	Transportation	Consumer/Industrial
Potential Uses: • Record keeping • Security of confidential patient information	Potential Uses: • Self-driving cars • Car self-maintenance • Shipping and supply payments • Ride sharing app	Potential Uses: • Official registry for government assets • Secure and faster voting mechanism for elections

Data Source: J.P. Morgan

Bitcoin and Other Digital Currencies

The concept of a digital currency is not as foreign to today's society as it may appear; only a small percentage of the U.S. money supply is tangible cash. When we check our bank account balances online, we are just looking at numbers on a screen. The bank is not holding everyone's cash in a vault. We trust the bank to be able to translate those digital numbers into real value when we need them to do so. This system has worked reasonably well, but new risks have emerged, as evidenced by frequent high-profile cyber-attacks. If someone wants to hack a bank, there is an obvious target. Blockchains have so far proven to be immune to cyber-attacks because instead of a single target, there are hundreds of thousands dispersed around the world that would need to be attacked at once.

Cross-border transactions will likely be the first area of currency transactions to see disruption from cryptocurrencies, as they still require a slow, expensive, painstaking process. Cryptocurrencies can provide a means of instant and low-cost cross-border transactions, and thus could see rather quick implementation. It might take longer for cryptocurrencies to become a part of normal everyday transactions, but even that is likely a matter of time. The benefits of blockchain-based transacting for both merchants and consumers are too great to ignore. Merchants would benefit from instantaneous transactions, lower fees, and an immutable record of transactions. Governments could benefit by receiving sales tax instantly at point of sale. Consumers could benefit because lower transaction costs for merchants could flow through to lower prices. They would also benefit from greater convenience and security.

The question is not if blockchain will make its way to everyday transactions; rather, when, and in what form?

When? Not yet. Even if every merchant in the U.S. decided to accept Bitcoin tomorrow, it functionally would not work. The network would be so inundated that transaction costs could be in the hundreds of dollars, and it could take days for transactions to process. It would be analogous to Netflix trying to launch back in the days of dial-up internet. Blockchain technology needs some time to work out how to scale before mass adoption becomes possible.

In What Form? A key risk to a decentralized cryptocurrency like Bitcoin ever becoming the dominant medium for every day transactions is government intervention. However, the following scenarios are possible:

- FedCoin: Multiple governments are seriously considering issuing tokenized versions of their fiat currencies – the most significant example being the U.K. Some believe that governments might ultimately decide against this as it could cause fewer people to hold money in bank accounts, which would disrupt the "money multiplier" lever that central banks can pull by adjusting the reserve ratio. Others disagree, citing economists with strong arguments dispelling the notion that the reserve requirement has any real impact on the amount of credit issued by banks. Further, bank deposits might not shrink meaningfully if the Fed did issue a tokenized version of the dollar. If banks were to custody the private keys and offer insurance, it is likely that many would still keep their cryptocurrencies in bank accounts since they would have no recourse if they lost them. Not depositing cryptocurrencies in an FDIC-insured bank would be a high-tech version of keeping money in a mattress.
- Transaction Intermediary: Cryptocurrencies may serve as an intermediary between transactions, rather than the primary transaction currency. There are already blockchain companies building platforms to facilitate automatic crypto-to-crypto or fiat-to-crypto exchanges. The idea is that a buyer can pay in whatever currency they please, be it crypto or fiat, and the merchant can accept the payment in whatever currency they favor. The platform's cryptocurrency would be used as the intermediary between the payment currency and receiving currency. The volatility of the middleman cryptocurrency would not matter since this conversion would take place almost instantly.
- Stable Coins: Stable Coins are cryptocurrencies that peg their market value to some external reference asset in order to avoid the volatility associated with traditional cryptocurrencies. Stable Coins can be pegged to a variety of assets including fiat currencies, commodities, and even other digital assets. Prominent examples include USD Coin, Binance USD, and Multi-Collateral Dai. By maintaining reserves of underlying assets, Stable Coins can offer fiat currency-like volatility through the blockchain. Stable Coins can also maintain their price through algorithms that adjust the supply of currency relative to demand. By narrowing the gap between traditional fiat and cryptocurrencies, Stable Coins make the digital asset world more accessible and useful to the average consumer, which in turn may help in the widespread adoption of blockchain-enabled technologies and use of cryptocurrencies for everyday transactions.

Ether, Smart Contracts, and DeFi

In 2014, then nineteen-year-old Vitalik Buterin introduced the idea of utilizing a blockchain's decentralized computing network to run computer programs rather than to just process simple peer-to-peer transactions. Buterin created Ethereum, which is a platform upon which anyone can build decentralized applications. Ethereum developed an additional layer on top of its blockchain such that one can submit code. When certain conditions written into the code are met, a transaction will trigger automatically. In order for the network to process this transaction, the user needs to pay the network a transaction fee. Instead of expending one's own electricity and computing power to process code, the decentralized network is paid a fee to provide this function in creating its form of cryptocurrency, Ether. Ether is known as the second largest cryptocurrency, but in reality it is much more akin to a commodity (i.e. digital asset). Ether is the "fuel" that powers decentralized applications. The transaction fee that is paid in Ether is even called "gas." Just as gas is burned when someone drives a car, so it is with a small fee "burned" when transacting on the platform. Ether had even higher percentage gains than Bitcoin in the bull markets of 2017 and 2020 because speculators felt that the demand for Ether would outstrip supply as more decentralized applications were built on the platform.

Developers on the Ethereum platform can even create their own cryptocurrencies on top of the Ether blockchain. These new cryptocurrencies receive the full decentralization benefit of the entire Ethereum network. Most of the excitement in the cryptocurrency community is surrounding the potential applications of these smart contracts. Innovation is happening at a rapid pace, largely due to a new method of obtaining financing that does not require traditional venture capital. A new blockchain company can conduct an initial coin offering (ICO) to raise hundreds of millions of dollars very quickly from anyone around the world with an internet connection. In return, ICO investors are given a pro-rata share of the new company's cryptocurrency. There are now thousands of these digital assets in existence. Most of these could ultimately fail, but in the meantime, the unprecedented ease of obtaining startup financing is allowing developers to experiment with countless applications of blockchain technology very quickly.

One of the challenges Ethereum has faced is its ability to facilitate the growing number of transactions on its platform with efficiency. Due to the significant uptick in use, "gas" prices have gone up while the speed of transactions has slowed. As a result, Ethereum has been undergoing an upgrade since 2015 to Ethereum 2, a process that will change its consensus mechanism from proof-of-work (PoW) to proof-of-stake (PoS). PoW requires computers to compete against each other to process transactions to earn rewards (highly energy and time intensive). PoS finds consensus by using an algorithm that chooses a node to win the transaction, and that node will create the next block of transactions in the chain. A node is chosen based on a couple factors including the size of the stake (of Ether), the time the coins have been staked for, as well as a randomness embedded in the algorithm. The goal is to increase Ethereum's transaction capacity, reduce fees, and make the network more sustainable. Although Ethereum has completed phase one of this transition, the time it has taken to complete this upgrade has made room for significant competitors. Cardano and Polkadot, both created by former Ethereum co-founders, are the biggest competitors to Ethereum and its role as the smart contract and decentralized finance leader. Cardano will be most suited to the financial and organizational sectors, while Polkadot's goal is to allow each app developer to create their own blockchain, collectively called Parachains. This differs from Ethereum's model where apps are run on smart contracts that run on a single blockchain.

The decentralized finance (DeFi) space is a prominent area within the realm of smart contracts, with the overall intent to decentralize the financial services and products universes. Today, the financials services world utilizes middlemen or centralized figures such as banks and governments that regulate financial markets, products, and the ability to operate in the industry. DeFi removes these hurdles and allows for the entire system to operate on a transparent, peer-to-peer regulated blockchain. Smart contracts built on the blockchain help facilitate and automate agreements between buyers and sellers or lenders and borrowers, which in turn allow the system to function.

Non-Fungible Tokens (NFTs) have also captured recent attention and serve as another example of smart contract applicability. NFTs are unique cryptographic tokens that exist on a blockchain, with unique identification codes that cannot be replicated and are completely distinct from other cryptographic assets. Cryptocurrencies are fungible assets that can be exchanged for one another—for example, one Bitcoin will always equal another Bitcoin. NFTs are non-fungible, meaning each token is unique. Today, the NFT market is mostly centered around digital collectables such as digital artwork. NBA Topshots, Cryptokitties and digital sports cards are some of the most popular examples. While these may seem frivolous, they serve as a proof of concept for other ownership applications. NFTs will most likely allow for the tokenization of unique physical assets in the future. We may see a digital representation of physical art pieces, luxury watches, or even real estate,

all with unique identification and ownership rights that are inscribed via smart contracts on a tamper-proof, secure, and transparent blockchain.

Appendix C: Digital Assets Investment Options

Outright Digital Asset Purchases

The digital asset market has continued to grow, bringing total market capitalization between $800 billion and $2.4 trillion in early 2021. Bitcoin alone comprises over $600 billion in market cap, with market share falling between 30-50% since the extended sell-off in 2018. The second largest coin, Ether, is worth $264 billion and the third largest coin, Tether, is worth $62 billion. Bitcoin trades roughly $30-70 billion a day throughout various global exchanges. By comparison, Tesla, which has a similar market cap of around $650 billion, trades approximately $20 billion per day. While Bitcoin and Ether appear to be large enough to take institution-sized flows, the remaining digital assets present a significant liquidity challenge for large market participants. As a result, big ticket direct purchases outside of the top two coins require finding a private seller off-exchange or need to be done very slowly on exchange. In either case, getting out of a large position would take a long time even in normal market conditions, and investors should be cognizant of potential issues around market impact.

The unique custodial challenges of digital assets have seen marked improvements in the last few years, making direct digital asset purchases a viable option versus a few years ago. For example, custodians like BitGo have attained "Qualified Custodian" status and have begun to offer insurance against theft of private keys. While keeping digital assets on exchange still presents a security risk, the availability of more secure custodial solutions lowers this operational risk for both direct and fund manager investments.

Digital Asset ETFs, ETNs, and Trusts

The SEC has received numerous applications for digital asset ETFs, and thus far the SEC has continued to delay approval. The Commission has recently cited concerns around price manipulation, and the current Chairman has also made comments about the lack of regulation and investor protections. However, concerns around custody have been largely mitigated, and the numerous applications and corresponding investor demand may drive an approval before year-end. Outside of ETFs, there exist a handful of ETNs offering exposure to Bitcoin, Ethereum, and other select digital assets, as well as closed-end funds from providers like Grayscale. However, most of these products trade at a significant premium to NAV.

Futures, Options, and Other Derivatives

The Commodity Futures Trading Commission approved Bitcoin futures contracts in late December of 2017 on the Chicago Mercantile Exchange (CME), which have been followed by the launches of both Ether futures and micro Bitcoin futures in 2021. Additionally, the CME offers listed options on Bitcoin futures, further expanding the tools by which investors and managers can access the space and avoid custodial and counterparty concerns. There are many other exchanges that offer derivatives on digital assets, though the CME's status as the world's leading exchange for futures trading has served as a point of comfort for many institutions and hedge funds. The ability for market participants to speculate on digital assets in both a long and short context yields multiple benefits, primarily an enhanced price discovery mechanism, which may lead to volatility normalization over time.

Public Equity ETFs

Multiple ETFs have been launched over the years that provide exposure to a portfolio of companies that are incorporating blockchain into their business models, such as BLOK and BLCN. Common holdings include Coinbase, PayPal, Square, IBM, Oracle Corp., Nvidia, and Microstrategy. While there is moderate concentration in companies that have benefited from increased demand for their GPU's due to more miners coming online, concentration seems to have decreased with events such as PayPal integration and the Coinbase IPO. As more companies look to incorporate blockchain technology or add digital assets to their balance sheet, the diversification of holdings should continue to increase through time.

Crypto Lending

Cryptocurrency lending facilitated by centralized or decentralized lending platforms present an opportunity to generate high single or double digit yields in a low interest rate environment. These loans are collateralized by the borrower's digital assets, and often substantially overcollateralized due to the volatility of the assets. With centralized lending platforms (Centralized

Finance, or CeFi), borrowers interact with regulated platforms such as BlockFi to secure lending. Customers must sign up for the specific platform through stringent protocols governed by the regulatory regimes in those specific regions. This involves three-tiered background/identity checks that limit potential fraud or illegal activity. Furthermore, these platforms typically stick to strict LTV ratios through high collateral in order to limit defaults. Records of deposits and withdrawals are recorded using blockchain technology, which are fully transparent and offer notable speed and efficiency. Decentralized finance (DeFi) platforms help facilitate transactions directly between borrowers and lenders through blockchain technology and code. These transactions are completely decentralized, though still completely transparent as they are completed on the blockchain. DeFi platforms are unregulated and have no middlemen, thus the process of getting loans is much more efficient. Similar to CeFi lending, DeFi loans are over collateralized, however the interest rates are typically lower. The smart contract technology of cryptocurrencies such as Ethereum allows for these transactions to take place, as individuals seeking to secure loans simply apply for loans through a platform and pledge the necessary collateral in order to secure financing (provided a lender chooses to negotiate or ultimately accept the terms of the loan). Although crypto lending is in its infancy, it provides significant liquidity to borrowers and significant yield to lenders, and thus an opportunity to earn a yield-based return rather than one directly linked to the returns of digital assets themselves.

Hedge Funds and Long-Only Investment Funds

Hedge funds were a predictable first mover in the crypto space, with over 200 crypto-focused funds appearing over the last few years. With the emergence of derivatives (and thus the ability to short), many existing hedge funds have expanded their market set to trade futures, swaps, or options on digital assets, and the improvements in custody solutions have made direct purchases more and more common. The actual investment strategies range from momentum trading within a broader macro or CTA portfolio, relative value trading between cryptocurrencies, futures basis trading, market making, and even exchange arbitrage, but many funds exhibit a long-only investment strategy. These long-only strategies range from single asset or quasi-index funds to actively traded strategies that maintain long exposure to de-risk in unfavorable market conditions. Overall, this long bias is understandable given the outsized returns of digital assets thus far. Additionally, the more arbitrage-oriented managers tend to have tight capacity constraints, limiting the ability to raise institutional capital.

Private Equity

Reputable private equity investors have made equity investments in blockchain-based companies, rather than in cryptocurrencies themselves, which helps to mitigate a layer of the custodial risk. This also allows investors to isolate investments within the blockchain landscape that are de-linked from the macro thesis around fiat debasement. Many private equity-style funds include investments in both early-stage companies and early-stage tokens, and even hold a percentage of assets in the more-established coins like Bitcoin and Ether. Structurally, private equity-style closed-end funds are also beneficial to manage both the illiquidity of private equity stakes and thinly-traded tokens, along with the elevated volatility of all digital assets.

Important Information

Wilshire is a global financial services firm providing diverse services to various types of investors and intermediaries. Wilshire's products, services, investment approach and advice may differ between clients and all of Wilshire's products and services may not be available to all clients. For more information regarding Wilshire's services, please see Wilshire's ADV Part 2 available at www.wilshire.com/ADV.

This material contains confidential and proprietary information of Wilshire, and is intended for the exclusive use of the person to whom it is provided. It may not be disclosed, reproduced, or redistributed, in whole or in part, to any other person or entity without prior written permission from Wilshire.

This material is intended for informational purposes only and should not be construed as legal, accounting, tax, investment, or other professional advice. Past performance does not guarantee future returns. This material may include estimates, projections and other "forward-looking statements." Forward-looking statements represent Wilshire's current beliefs and opinions in respect of potential future events. These statements are not guarantees of future performance and undue reliance should not be placed on them. Such forward-looking statements necessarily involve known and unknown risks and uncertainties, which may cause actual events, performance and financial results to differ materially from any projections. Forward-looking statements speak only as of the date on which they are made and are subject to change without notice. Wilshire undertakes no obligation to update or revise any forward-looking statements.

This material represents the current opinion of Wilshire based on sources believed to be reliable. Wilshire assumes no duty to update any such opinions. Wilshire gives no representations or warranties as to the accuracy of such information, and accepts no responsibility or liability (including for indirect, consequential or incidental damages) for any error, omission or inaccuracy in such information and for results obtained from its use. Information and opinions are as of the date indicated, and are subject to change without notice.

Wilshire Advisors LLC (Wilshire) is an investment adviser registered with the Securities and Exchange Commission. Wilshire® is a registered service mark of Wilshire Advisors LLC, Santa Monica, California. All other trade names, trademarks, and/or service marks are the property of their respective holders.

13520854 E1021