INVESTMENTS & WEALTH MONITOR

A reprinted article from January/February 2019

BLOCKCHAINS AND CRYPTOCURRENCIES

Why They Matter and How They Work

By Bob Rice and Stan Miroshnik

INVESTMENTS & WEALTH INSTITUTE®
formerly IMCA

BLOCKCHAINS AND CRYPTOCURRENCIES

Why They Matter and How They Work

By Bob Rice and Stan Miroshnik

To answer the key question first: Yes, blockchains and cryptocurrencies will be extremely important to real-world enterprises—soon. For example, Facebook is planning to develop its own cryptocurrency for its 200 million WhatsApp users in India. These customers, many of whom are unbanked, then could make and receive global remittances efficiently, at almost no cost—while completely bypassing traditional financial institutions. Users could also presumably accumulate and hold assets within the app, pay merchants that choose to participate (which ones wouldn't?), and generally use WhatsApp like a bank account. And a recent move to unite the architecture of Facebook Messenger, Instagram, and WhatsApp would pave the way to eventually expand the service to billions of others.

What's happening for the unbanked is also happening for the unlawyered. Legal Zoom and Rocket Lawyer have teamed up to deliver standard, self-executing startup legal documents that will live on a blockchain, with the goal of streamlining the entire process and culling tens of thousands of dollars from the cost.

These two examples show why investors and advisors should take the digital asset space seriously, regardless of any interest in investing directly in cryptocurrencies. Recall that the internet created some massive winners among "normal," non-web focused companies: Netflix was just a movie rental company mailing DVDs to customers, but it recognized and exploited the advantages of streaming content. The internet also created lots of losers—such as the many retailers that did not adjust to online shopping. The digital asset revolution is likely to similarly alter the corporate competitive landscape, with consequences that will have important ramifications for every portfolio.

A VERY BRIEF HISTORY OF DIGITAL ASSETS

Bitcoin was invented in 2009 to do one thing, and it does that thing very well. It was designed as a new payment system. Median bitcoin transaction fees are measured in basis points and holding a bitcoin account is effectively free. This lack of cost results directly from blockchain, an ingenious system that does not require expansive centralized organizations to facilitate the transfer of value or maintain indisputable records of trades. It works at a fraction of the expense to users of established payment systems such as credit cards, checks, and wire transfers.

Bitcoin, of course, quickly got much bigger than "a payment system." Because the core bitcoin algorithms provide a fixed total number of coins that can be created over time, and because no centralized monetary authority controls their creation (or is capable of suddenly creating more), many perceived bitcoin as "digital gold." Its value rose slowly, then suddenly skyrocketed in a speculative frenzy, and, as everyone knows, inevitably crashed. Yet its market capitalization still hovers around levels comparable to that of Wall Street powerhouses such as Goldman Sachs and Morgan Stanley.

The press focused almost exclusively on bitcoin's valuation fluctuations as crucial developments in digital assets were happening outside the financial limelight. The first such development was the recognition that blockchain technology could be utilized to revolutionize all sorts of validation, recordation, and transfer needs in normal commercial and financial environments, such as supply chain management, insurance claims, and international shipping and permitting processes. This led to billions of dollars of corporate and venture capital investment in thousands of blockchain-based projects not related to digital currencies (venture firms alone invested more than $2 billion in such efforts in 2018). Indeed, the most important uses of a new technology often are not the primary ones envisioned by the inventor, and so it may be with blockchain.

The second key development was a fundamental extension of blockchain capabilities with the introduction of a rival cryptocurrency platform called Ethereum. Ethereum's big innovation allows snippets of computer code, rather than just inert "coins," to live and operate on a blockchain. As a result, algorithms can carry out instructions automatically on the occurrence of specified contingencies (such as transferring title or making payments), leading to "smart" self-executing contracts.

Crucially, different issuers can create their own unique Ethereum tokens—in effect, sub-cryptocurrencies—to serve their own goals.

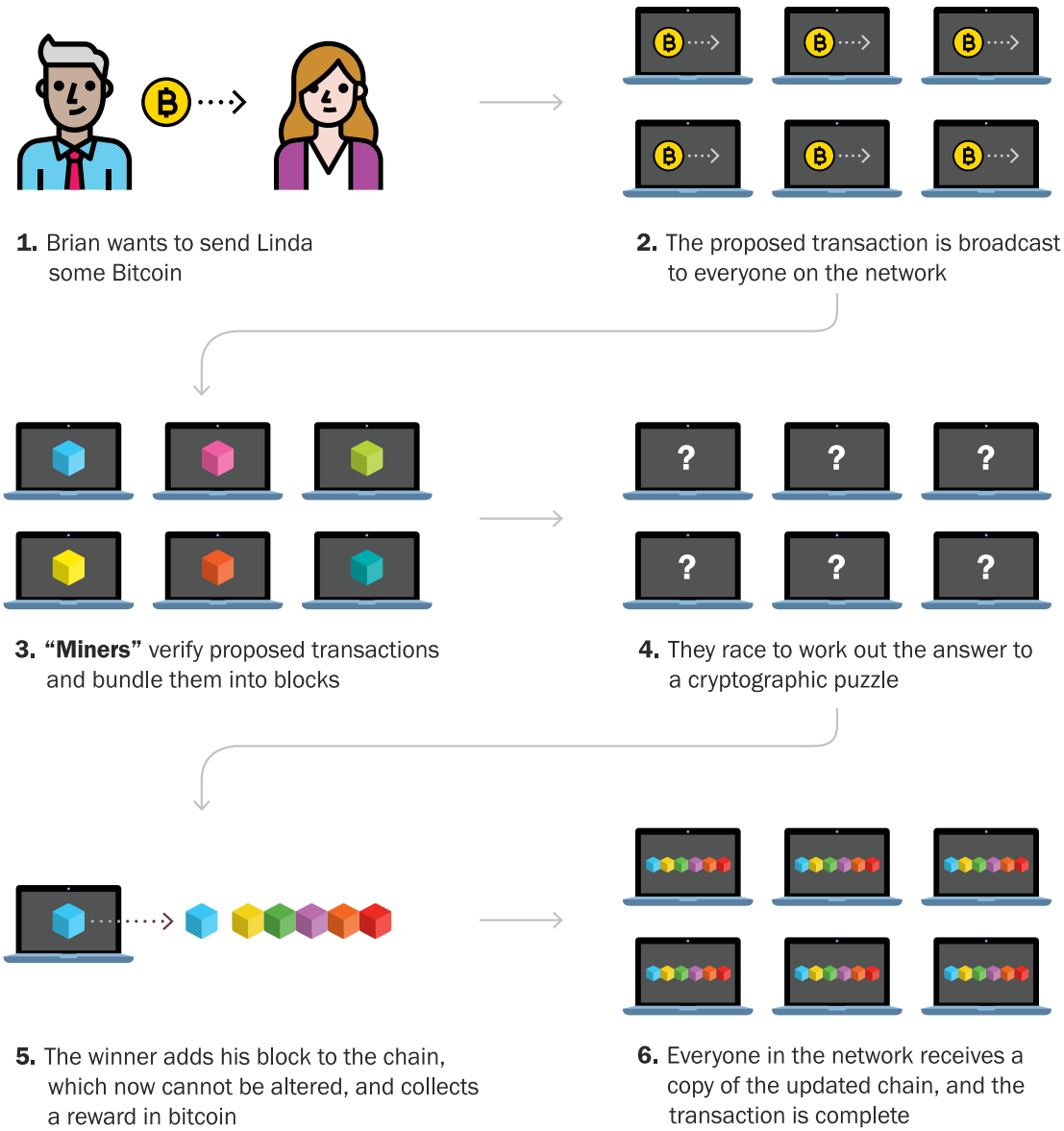
The third development was the advent of "stable value" coins. These are digital tokens with value tied directly to a traditional fiat currency, such as the dollar. In principle, the issuers hold the appropriate amount of the fiat currency in escrow and holders can exchange their tokens into fiat currency when they wish. On the one hand, this is a step back for the cryptocurrency vision, because it reintroduces central banks as primary players. On the other hand, the stable-value innovation allows the development of blockchain trustless payment systems by letting the tokens be a more-traditional store of value. This approach has paved the way for the Facebook's application of digital assets at WhatsApp, discussed above, and it may well have the greatest near-term disruption potential.

A TECHNOLOGY PRIMER
BLOCKCHAIN VERSUS CRYPTOCURRENCIES

Blockchain is the underlying technology that allows bitcoin and other cryptocurrencies to exist. To draw a parallel with the internet, blockchain is the transmission control protocol/internet protocol or TCP/IP level of the system, and it is the most critical piece of Satoshi Nakamoto's bitcoin invention. Blockchain allows participants of a public network, who do not know or trust each

Figure 1

BLOCKCHAIN, SIMPLIFIED



Source: Rice Partners (adapted from The Economist*)*

other, to agree, transact, and permanently memorialize the transactions—all without the aid of any central institution (see figure 1).

This is accomplished through specialized recording, organizing, sharing, and storing of data. Every transaction in an asset such as bitcoin is recorded simultaneously into an open network of thousands of nodes. The transactions are grouped and recorded in chunks known as "blocks." The network thus serves as a distributed ledger that can be used to verify the authenticity of each subsequent attempted transaction in the asset, including that the account attempting to transfer assets actually owns them. Subsequent trades are then also recorded and appended to the pre-existing chain of blocks. No single central authority is responsible or liable for sharing or updating this ledger, and its contents are immune from alteration because identical data, representing the entire history of the asset, exists in so many independent places at once.

As noted, however, cryptocurrencies such as bitcoin are just one use of blockchain. Others are being developed for insurance, shipping, supply chain management, digital identities, voting, managing personal ownership of online data, and, of course, financial transactions. All need efficient and immutable ledger systems, and blockchain appears to be a natural fit.

THE ETHEREUM REVOLUTION

From 2009 to 2013 bitcoin gained moderate traction in some circles, but the world remained mostly ignorant of the idea of cryptocurrency. The 2014 introduction of the Ethereum network and its rival cryptocurrency, known as ether, put cryptocurrencies on the global radar. Ethereum created a new layer of utility for blockchain technology by introducing smart contracts, pieces of computer code that automatically execute functions when certain criteria are met. Because Ethereum smart contracts run on blockchain, they are not susceptible to tampering by third parties and don't require a central authority to approve the execution process. This innovation exponentially increased the potential applications of blockchain and digital assets for the management of transactions, money, property, and information.

Ethereum's significance stretches beyond technological advancements, though. It was the first cryptocurrency to be made available through an initial coin offering (ICO). To fund the Ethereum project, its creators sold 11.9 million ether, raising about $US18.4 million, a seminal event in the history of digital assets. Today, most ICOs are made in smart contract tokens, specific to the venture doing the ICO, created on and for the Ethereum blockchain. Each venture issues its own flavor of an Ethereum token, specific to the particular project, but still enjoys the benefits of working within the Ethereum ecosystem.

KEYS

Anyone who owns (or wants to own) a cryptocurrency, such as bitcoin, also holds a set of two encrypted keys—codes in the form of long alphanumeric strings. One is public and is effectively the address of the holder's account, allowing coins to be sent to it. The other is private, known only to the holder, and unlocks the account for access to its contents. But anyone who knows the private key also can unlock the account, and the vast majority of thefts of cryptocurrencies occur because a private key is shared or exposed. Once a theft occurs and assets are transferred, they cannot be recovered, because transactions on blockchain cannot be reversed.

Using a two-key system serves a dual purpose. It allows direct trustless transactions, meaning that parties who do not know each other can reliably transact without a centralized organization standing between them. It also permits each transaction to be irreversibly and permanently recorded on a blockchain ledger.

VALIDATION AND MINING

From a practical perspective, "miners" are the most critical members of the bitcoin ecosystem. They're the folks who do the work of verifying the validity of proposed transactions and then record the transactions into the blockchain. To incent miners to do this work, the system generates new coins and uses them to pay the miners when new blocks are added.

But which miners actually get to do the work and earn the coins? There's an open, global competition that involves solving complex mathematical problems; the first miners to do so earn the right to append blocks to the chain and claim the reward coins. As a result, cryptocurrency mining has evolved into a competitive industry, featuring specialized computer chips, immense server farms, and the consumption of enormous amounts of electricity.

Note that all this sparked a tremendous growth spurt for chipmaker nVidia, whose products were (accidentally) particularly useful in the mining process; and the decline of mining interest in the second half of 2018 was a primary cause of the stock's subsequent fall—another case of digital assets having direct, real-world impact on typical investors.

The mining system, as decentralized and trustworthy as it is, has one huge drawback, however: It's slow. As a result, new crypto systems have developed alternative and faster validation systems such as "proof of stake" and "byzantine agreement." But, for now, proof-of-work mining remains the validation norm.

BUYING AND STORING CRYPTOCURRENCY

Buying, storing, and spending cryptocurrency is not quite as simple as using an ATM, but it's really not terribly complicated either. The fundamental requirement is a specialized wallet to hold a user's private keys. The most secure is a hardware wallet, a specialized

physical device that is not itself connected to the internet, so it is far less susceptible to hacks and attacks that plague web-based wallets. Some owners park these hardware wallets in vaults or safe deposit boxes, a rather ironic, but quite secure, method for storing digital assets.

To procure cryptocurrency, buyers typically use a specialized exchange or over-the-counter trading desk that will convert dollars (or another fiat currency) into the target digital asset. This is itself a simple process but, again, the entire issue is the security of the private key that controls access to the resulting holdings.

As a result, custody has been a linchpin issue for advisors interested in cryptocurrencies for clients. For example, Fidelity has announced a crypto custody system,[1] and several other traditional institutional custodians are developing digital asset capabilities as well. Thus, we can expect the custody issue to be resolved soon.

DIRECT INVESTMENT THESES AND OPPORTUNITIES

BITCOIN AND OTHER CRYPTOCURRENCIES

It is most likely fair to say that bitcoin is the reserve currency of the digital universe, despite all the developments since its inception. But from an investment perspective, what is it?

One view, noted above, is that it's digital gold. Enthusiasts love the idea that there is no central authority with the power to create more than the 21-million-coin limit programmed into the core bitcoin algorithms, and that the rate at which new coins can be issued until that number is reached is also tightly controlled by the original formulas. As Fred Wilson, founder of Union Square Ventures, likes to say, "I trust mathematics more than I do central banks." Indeed, there won't be any quantitative easing in the bitcoin universe.

But there is a major flaw in this argument, because it ignores the fact that an infinite number of rival cryptocurrencies can be created, and indeed several major ones already have been. Gold is unique by the fundamental laws of physics (and it is also useful for many purposes in real life); cryptocurrencies are not.

Nonetheless, humans can and have agreed to use just about anything as money, and certainly bitcoin has profound advantages. If cryptocurrencies do gain more traction as payment systems, pre-programmed limits on total issuance may help bitcoin sustain a market value.

ICOS AND THE 'UN-CORPORATION'

New ventures premised on blockchain and smart contracts typically have funded themselves through ICOs. Usually, these involve particular Ethereum tokens peculiar to a specific enterprise. These may merely convey the right to consume the services the new venture will develop (like a prepaid cell service card), but usually buyers also hope that the venture will become successful and they can profit from a later token sale.

As a result of this inherent or explicit investment motive, the consensus is that nearly all ICOs should be treated as securities for U.S. regulatory purposes and must therefore follow a private placement route in the United States (absent registration with the U.S. Securities and Exchange Commission [SEC]). But note that the currencies themselves, such as bitcoin and ether, typically are considered to be commodities (just as fiat currencies are); transactions in them typically will fall under the jurisdiction of the U.S. Commodity Futures Trading Commission rather than the SEC.

Does an ICO differ from a round of traditional venture capital funding? Some don't, at least not very much. Some token purchases may convey governance and economic sharing rights that can look like common stock, or founders' shares. But others are extremely different from classic venture funding, and they represent what some think is the next development in the nature of economic enterprises: the decentralized venture or "un-corporation."

Most ICO sponsors are hoping to kick off a self-reinforcing economic dynamic that will lead to a useful new system and greater valuation for the tokens. They think that many or all the investors or token holders will work toward a grand new vision, albeit reasonably independently, without the centralized direction of a typical corporation.

Filecoin is one example into which several big-name venture capital firms have invested. The idea is to create a decentralized cloud storage system (unlike the centralized ones controlled by Microsoft or Amazon). Holders of Filecoin tokens will have the right to use the system once developed, but they also have a natural incentive to help it along. As they contribute storage space to the joint effort, or help develop the technology to coordinate use of the combined capacity, the system would become more valuable, and so would the tokens that can be spent to use it.

A more ambitious case is WePower, which aims to change the way renewable energy is created and paid for. Renewable developers can sell Ethereum-based smart tokens to future consumers and use the proceeds to build out their alternative energy plants; the token owners can buy the produced electricity later with their tokens or, perhaps, trade them for profit. Meanwhile, all the complexities of typical power purchase agreements are standardized in the smart tokens, which in principle could be traded as easily as any other digital asset. Thus, the vision extends creating a standardized secondary power market that would constantly incent new renewable developers to join.

It's this kind of decentralized collaborative venture characteristic that most ICOs are trying to jumpstart. From the perspective of economic theory, these

novel ideas are not that strange. British economist Ronald Coase won a Nobel Memorial Prize in Economic Sciences for identifying why corporations exist in the first place: because individuals operating inside them can trust each other and work together toward a common goal with minimal "friction." What Coase meant was that, in the absence of a corporate envelope, individuals need to legally document and account for every interaction of every person, create systems for joint decision-making, and the like. Corporations made these efforts efficient.

The internet has been chipping away at friction for a long time. People can trust eBay sellers they haven't met, they can outsource tasks to others they don't know via Amazon, or they can even extract expertise from strangers via LinkedIn or Quora. Less friction leads to smaller companies, a trend that's been evident since the dawn of the digital era. In many ways, the un-corporations that ICOs are meant to ignite are the logical continuation of this trend.

CONCLUSION

The 2018 cryptocurrency crash attracted lots of headlines and to some the promise of digital assets has petered out. Bitcoin has achieved minimal traction in the real world, blockchain has yet to prove itself genuinely useful in the wild, and no dominant company or system has yet emerged from any ICO. The ventures that aim to digitize assets such as real estate or stock and put them on blockchain seem to be chasing an idea that is logically possible but ultimately not terribly useful compared with existing transfer and recording systems.

But under the covers, significant progress is being made toward the mainstreaming of digital assets.

Fully SEC-licensed crypto brokerages now can conduct a full range of digital asset services, bitcoin futures are trading at CME Group (the largest futures and options exchange operator), and traditional, trusted institutions now offer custody services. Major consulting firms such as PricewaterhouseCoopers have launched crypto practices, and several significant crypto-investment banks are now in business, populated by veterans of leading Wall Street institutions.

Perhaps most importantly, the utterly revolutionary ideas behind blockchain and cryptocurrencies are being pared back to make them more compatible with existing business practices. A little centralization might be just the fertilizer needed to stimulate the disruptive potential of blockchain and cryptocurrency (consider the Facebook example noted above). Stable value coins make trustless payment systems more realistic, new validation methods promise much faster speeds for digital asset transactions, and privately maintained blockchains are radically more practical than completely open ones.

Still, these are very early days for cryptocurrency—but not so early that advisors can safely ignore the space. At a minimum, advisors should be alert for the coming shifts in the corporate competitive landscape and the potential impact on their stock and fund selections. More adventurous advisors can consider direct investment in digital assets or in new ventures aimed at exploiting these wonderful inventions of trustless payment systems and decentralized ledgers.

Bob Rice is managing partner at Tangent Capital and Rice Partners, a director of Nasdaq Private Markets, and senior advisor to Macquarie Investment Management and Wilshire Associates. Contact him at rer@ricepartners.com.

Stan Miroshnik is chief executive officer and founder of Element Group, a full-service advisory firm for the digital asset economy. He earned BS and BA degrees from the University of California, Berkeley and an MBA from the Massachusetts Institute of Technology Sloan School of Management. Contact him at stan.miroshnik@elementgroup.com..

ENDNOTE

1. See, for example, https://www.fidelity digitalassets.com/overview.

CONTINUING EDUCATION

To take the CE quiz online, www.investmentsandwealth.org/IWMquiz

INVESTMENTS & WEALTH INSTITUTE®
formerly IMCA

5619 DTC Parkway, Suite 500
Greenwood Village, CO 80111
Phone: +1 303-770-3377
Fax: +1 303-770-1812
www.investmentsandwealth.org