Blockchain 2.0: What's in store for the two ends—semiconductors (suppliers) and industrials (consumers)?

Ten years after blockchain's inception, it is presenting new opportunities for both suppliers, such as semiconductor companies, and consumers, such as industrials.

Gaurav Batra, Rémy Olson, Shilpi Pathak, Nick Santhanam, and Harish Soundararajan

JANUARY 2019 • ADVANCED ELECTRONICS PRACTICE

Blockchain is best known as a sophisticated and somewhat mysterious technology that allows cryptocurrencies to change hands online without assistance from banks or other intermediaries. But in recent years, it has also been promoted as the solution to business issues ranging from fraud management to supply-chain monitoring to identity verification. Despite the hype, however, blockchain's use in business is still largely theoretical. A few pioneers in retail and other sectors are exploring blockchain business applications related to supply-chain management and other processes, but most are reluctant to proceed further because of high costs, unclear returns, and technical difficulties.

But we may now be at a transition point between Blockchain 1.0 and Blockchain 2.0. In the new era, blockchain-enabled cryptocurrency applications will likely cede their prominence to blockchain business applications that can potentially increase efficiency and reduce costs. These applications will be in a good position to gain steam since many large tech companies may soon begin offering blockchain as a service (BaaS). Rather than just providing the hardware layer, as they've traditionally done, these companies will extend their services up the technology stack to blockchain platforms and tools. As blockchain deployment becomes less complex and expensive, companies that have sat on the sidelines may now be willing to take the plunge. (See sidebar, "What advantages do blockchain business applications offer?")

Will blockchain business applications continue to grow and finally validate their promise? Industrial companies, which were largely on the sidelines during the Blockchain 1.0 era, want an answer to this question because they could find opportunities to deploy business applications that improve their bottom line. Semiconductor companies are also interested in the growth of both blockchain business applications and blockchain-enabled cryptocurrency because this could increase demand for chips.

Both industrial and semiconductor players will need a solid understanding of specific blockchain-enabled use cases and the market landscape to succeed in the new era. To assist them, this article reviews the changing market and then focuses on specific strategies for capturing value. One caveat: all information in this article reflects data available as of December 2018. Cryptocurrency values fluctuate widely, so the numbers reported, including those for market capitalization, may not reflect the most recent data. Blockchain technology and the competitive landscape are also evolving rapidly, and there may have been changes since publication.

Blockchain 1.0: The cryptocurrency era

It is not surprising that many people conflate blockchain with Bitcoin, the first and most dominant cryptocurrency. Until recently, the vast majority of blockchain applications involved enabling cryptocurrency transactions. Around 2014, however, private companies began investigating the use of blockchain for other business applications. Since most of these players are still at the pilot stage, it is fair to say that blockchain-enabled cryptocurrency has been the focus of the Blockchain 1.0 era.

The emergence of cryptocurrencies

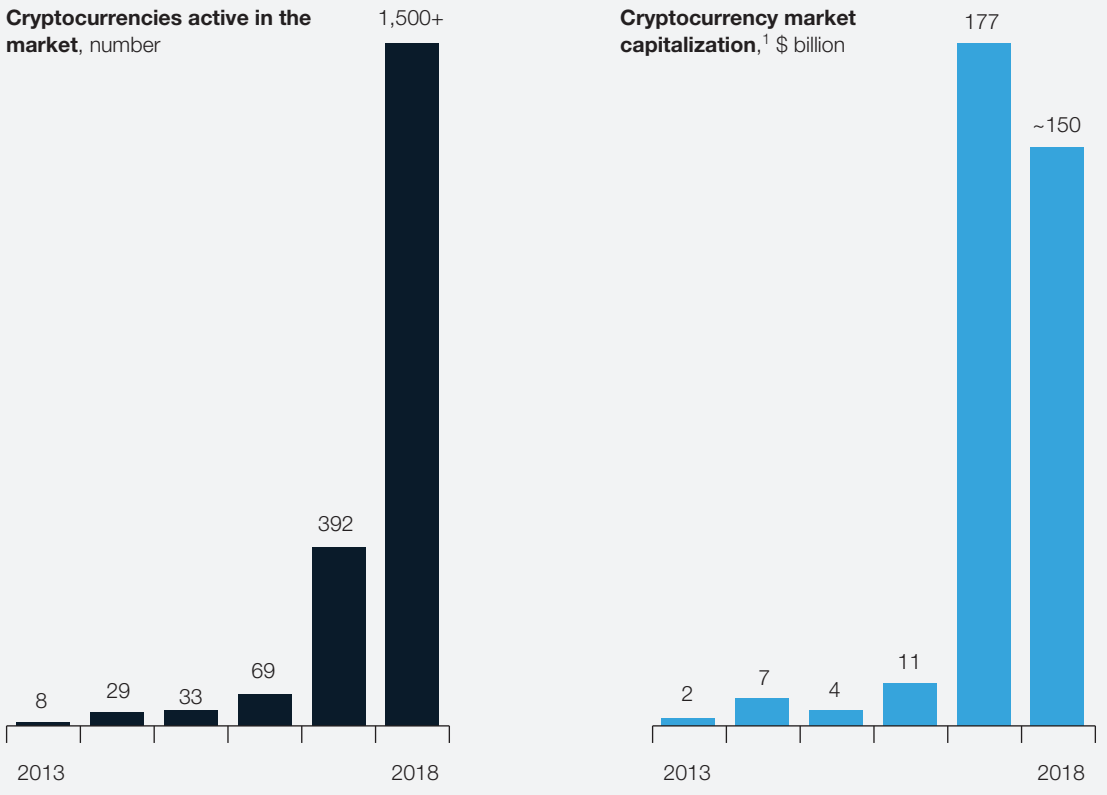
Bitcoin hit the market in 2009 as an open-source software application. It was first used in a commercial transaction in 2010, when two pizzas were bought for 10,000 bitcoin (under $10 then, but about $35 million as of December 2018). With no central authority or server to verify transactions, the public was initially skeptical about Bitcoin and reluctant to use it. Beginning in 2014, however, Bitcoin has experienced a meteoric increase in user base, brand-name recognition, and transaction volume. Its value is extremely volatile, however, and it has declined sharply from its late 2017 peak of over $19,000.

The past two years have seen the most growth in blockchain-enabled cryptocurrencies, with the number increasing from 69 in 2016 to more than 1,500 in 2018. Even though Bitcoin's value has decreased this year, an influx of initial coin offerings (ICOs) has increased the market capitalization for cryptocurrencies (Exhibit 1).

Many of the additional currencies—also called "altcoins"— were created to address certain gaps or inefficiencies with Bitcoin, and they are available through various networks. Popular altcoins include Dash, Litecoin, and XRP (offered through Ripple). Of all the alternative cryptocurrency networks, Ethereum is most popular. It is an open-source platform that allows users to build and launch decentralized applications, including cryptocurrencies or digital ledgers. Users must spend a specific digital currency, Ether, to run applications on Ethereum. Ether can also serve as an alternative to regular money, but its primary purpose is to facilitate Ethereum operations.

Together, the market capitalization of a select set of major cryptocurrencies was about $150 billion in December 2018, with Bitcoin and the four leading

Exhibit 1 **The number of active cryptocurrencies and their market capitalization has soared.**



[1] This is the market capitalization for a select bundle of cryptocurrencies. Bundle includes: Bitcoin, Dash, Ethereum, Litecoin, Ripple, and several other altcoins. Figures are as of Dec 11, 2018.

Source: McKinsey analysis

altcoins representing about 75 percent of this value. Bitcoin's market capitalization of about $60 billion was the highest.

Transaction verification

The method used to verify transactions varies by cryptocurrency. With Bitcoin, the first participant, or "miner," to validate a transaction and add a new block of data to the digital ledger will receive a certain number of tokens as a reward. Under this model, which is referred to as a proof-of-work (PoW) system, miners have an incentive to act quickly. But validating a transaction doesn't simply involve verifying that Bitcoin has been transferred from one account to another. Instead, a miner has to answer a cryptographic question by correctly identifying an alphanumeric series associated with the transaction. This activity requires a lot of trial and error, making the hash rate—the compute speed at which an operation is completed—extremely important with Bitcoin.

In the beginning, many individuals mined Bitcoin as a hobby. But as interest in cryptocurrencies grew, the number and size of Bitcoin miners soared, necessitating more sophisticated hardware and more intense computing power. This shift has favored the rise of large mining pools. Many of these, including AntPool and BTC.COM, are based in China. The top five mining pools account for 70 to 85 percent of the overall Bitcoin network's collective hash rate, or computing power.

Hardware for cryptocurrency players

In the early day of cryptocurrency, amateur hobbyists relied on central processing units (CPUs) to optimize compute performance. When the Bitcoin network began expanding around 2010, the graphics-processing unit (GPU) replaced the CPU as the accelerator of choice. The ascent of GPUs was short lived, however, since many companies began designing application-specific integrated circuits (ASICs) for cryptocurrency mining to improve hash rates.

About 50 to 60 percent of companies that manufacture ASICs for Bitcoin transactions are based in the Greater China region (Exhibit 2). (Some of these began creating ASICs for cryptocurrency mining before Bitcoin entered the market in 2008, since this was already viewed as a potential growth area.) BitMain Technologies, a China-based company, supplied 70 to 80 percent of the cryptocurrency ASICs in 2017. Its customers typically use "crypto rigs"—basically, multiple ASICs working together—to optimize compute speed. By conservative estimates, BitMain Technologies has a gross margin of 65 to 75 percent and an operating margin of 55 to 65 percent—equivalent to $3 billion to $4 billion in 2017. That figure is roughly the same as the profit margin for NVIDIA, which has been in business for 20 years longer.

Although most major cryptocurrencies now reward miners with high compute speed, some have taken steps to prevent large mining pools with crypto rigs from dominating the market. For instance, Ethash, the hashing algorithm that Ethereum uses, is designed to be ASIC resistant—and that means miners must fetch random data and compute randomly selected transactions to solve their cryptographic questions. Both activities require frequent access to memory, which ASICs alone won't provide. Ethereum miners primarily rely on a system that utilizes a GPU in combination with memory.

Blockchain 2.0: Uncertainty about cryptocurrencies and the emergence of business applications

The Blockchain 2.0 era will likely usher in many changes. The cryptocurrency market could become more diverse if Bitcoin continues to decrease in price, since ICOs may see the situation as an opportunity to stake their claims. Consumers may also begin demonstrating more interest in other established altcoins. For instance, users may come to favor Dash or Litecoin for some transactions, since they

Exhibit 2

Many companies have developed application-specific integrated chips specifically designed to mine cryptocurrencies.

A timeline of cryptocurrency chip manufacturers

Company	**INNOSILICON Technology**	**Bitfury**	**BitMain Technologies**	**CoinBau GmbH**	**Butterfly Labs**
HQ	Ningbo, China	DC, US	Beijing, China	Dresden, Germany	Leawood, KS, US
Recent product	**T2 Turbo+ 32T**	**Bitfury Tardis**	**Antminer S9-Hydro**	**WolfCAVE XE**	**Monarch**
Launch	Sept 2018	Oct 2018	Aug 2018	Not available	Aug 2014
Hash rate	32 Th/sec	80 Th/sec	18 Th/sec	4.8 Th/sec	725 or 825 Gh/sec
Power efficiency	0.069 J/Gh	0.055 J/Gh	0.096 J/Gh	0.27 W/Gh	0.7 W/Gh

2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018

Company	**Ebang Communication**	**Black Arrow**	**Canaan Creative**	**CoinTerra**	**Halong Mining**
HQ	Hangzhou, China	Guangdong, China	Beijing, China	CA, US	Not applicable (online only)
Recent product	**EBIT E11+**	**Prospero X36**	**AvalonMiner 851**	**TerraMiner IV**	**Dragonmint T16**
Launch	Oct 2018	Dec 2015	Aug 2018	Jan 2014	Mar 2018
Hash rate	37 Th/sec	2.2 Th/sec	15 Th/sec	1.6 Th/sec	16 Th/sec
Power efficiency	0.055 J/Gh	0.7 W/Gh	0.11 J/Gh	0.6 W/Gh	0.075 J/Gh

Note: Gh = gigahash; J = joule; sec = second; Th = terahash; W = watt.
Source: McKinsey analysis

offer faster transaction speed than Bitcoin does. Companies and the general public are generally becoming more comfortable with cryptocurrency transactions, which could increase usage rates.[1]

In tandem with these changes, the market for blockchain business applications is heating up as BaaS simplifies implementation. Demand for these applications is expected to be strong, and corporate users could soon outnumber cryptocurrency miners.

Investors are showing continued interest in blockchain, although funding levels have recently declined. Venture-capital funding peaked in 2017 at about $900 million for both cryptocurrency and business applications, and it will likely still be between $600 and $800 million in 2018. It is unclear whether 2019 will show continued decline, a plateau, or greater investment.

Although it is difficult to make predictions about blockchain, since it is a relatively new technology, we were able to identify several trends in the cryptocurrency and business-application markets that could affect demand for this technology. Here is what we found.

The cryptocurrency market is evolving rapidly but uncertainties remain

Despite the widespread press attention that cryptocurrencies receive, their practical value is still limited. Most people regard them as something of an online Swiss bank account—a haven for activities that can't be closely tracked by authorities. In many

cases, potential users hold back because they don't believe cryptocurrencies are secure. Digital-ledger technology, the backbone of blockchain, has never been hacked, but cryptocurrencies are vulnerable in other ways. The most infamous theft occurred in 2014 when someone took 850,000 bitcoin from the Mt. Gox exchange by assuming another person's identity. In the corporate sphere, only about 3,000 companies now accept Bitcoin transactions.

Future growth of cryptocurrencies

It is difficult to predict whether cryptocurrencies will experience strong growth in Blockchain 2.0, since corporate leaders and members of the public may have lingering doubts that are difficult to overcome. But we do expect to see greater usage rates. In addition, miners will have a greater number of options from which to choose. Although Bitcoin now represents about 40 to 50 percent of market capitalization for cryptocurrency, other altcoins are becoming more popular. Ethereum, for instance, now accounts for more than 10 percent of the market capitalization. And small ICOs—those beyond the top 20—now represent about 20 percent of market capitalization, up from 5 percent only two years ago.

Government intervention—particularly the development of laws and regulations—may strongly influence the cryptocurrency market over the next few years. If the current market provides any clues, it is unlikely that a global consensus will emerge. For instance, some governments allow individuals to use cryptocurrency but prohibit banks and securities companies from doing so. Other countries take a much stricter approach by forbidding ICOs to operate within their borders. If additional governments adopt this stance, cryptocurrency uptake could be limited.

Another big question relates to investment. Funding for ICOs usually comes from venture capitalists because pension funds and other institutional investors consider cryptocurrency too risky. (The majority of ICOs do not yet have customers nor do they generate revenue.) Even though venture-capital investment in cryptocurrency has increased, the lack of interest from institutional investors could restrict future growth to some extent.

Changing algorithms

Behind the scenes, more subtle changes are occurring in the cryptocurrency market as players try to minimize the importance of compute power by developing new algorithms. For instance, Ethereum is considering the replacement of its PoW system with one based on proof of stake (PoS). In a PoS system, participants are rewarded based on the number of coins they have in their digital wallets and the length of time they have had these stakes. The participant that rates highest on these factors is chosen to validate a transaction and receive a reward. Many other large cryptocurrency networks, including Cardano, Dash, and EOS, are also investigating PoS algorithms.

PoS systems have several advantages. First, they help cryptocurrency networks build a trusted network of loyal participants—and this may make security breaches less common. Second, they level the playing field for cryptocurrency miners, since those with the greatest compute power will not necessarily be the winners. Players also appreciate that PoS systems are more energy efficient and allow faster transactions. A shift to PoS systems could have major implications for semiconductor companies that serve cryptocurrency players, since it would shift chip demand in new directions.

A new look at business applications, but with doubts about scalability

Recent McKinsey research has identified more than 90 use cases for blockchain business applications across industries. Many near-term use cases will involve applying blockchain to reduce costs associated with existing processes, such as the exchange of medical records among providers,

insurers, researchers, and patients. In these activities, blockchain can remove the need for intermediaries and decrease administrative costs associated with record keeping. Over the longer term, blockchain might be used to improve fraud management, supply-chain monitoring, cross-border payments, identity verification, and the protection of copyrights or intellectual property. It could also help companies with smart contracts—transactions that execute automatically when certain conditions are met.

Many companies and organizations are now supporting the development of blockchain business applications. The Linux Foundation has created Hyperledger, an open-source collaborative effort to develop blockchain technologies for multiple industries. Similarly, the company R3 leads a large consortium that developed Corda, a blockchain platform for use in financial services and commerce. Corporate investment in blockchain hit $1 billion in 2017 and is expected to grow at a compound annual growth rate of 50 percent through 2021.

Despite these efforts, blockchain business applications arguably remain stuck at the pilot stage, with most companies still attempting to demonstrate proof of concept (PoC). (The greatest wave of business applications undergoing PoC occurred from 2016 to 2017; the number at this stage is now smaller.) Many start-ups that offer business applications have failed to obtain Series C funding—the investment designed to promote growth and scale operations. The emergence of competing technologies is the major reason for the lack of progress. For instance, with payments, financial institutions can now use a messaging network that allows for greater transaction speeds and more transparency than past methods. This technology reduces the need for blockchain-based solutions and discourages incumbents in the financial sector from investing in blockchain.

Much interest in blockchain business applications stems from the recent advent of BaaS, which simplifies the creation of the complex, five-layer blockchain technology stack (Exhibit 3). Until the past year, enterprise customers had to build individual layers themselves or cobble them together from disparate sources. Among other tasks, they had to customize existing digital-ledger fabric platforms (distributed computing platforms with a base protocol and configurable functions). They also had to acquire and integrate data, define permissions and governance protocols, and code software. Most enterprises simply lacked the funds or in-house technology talent to make this happen.

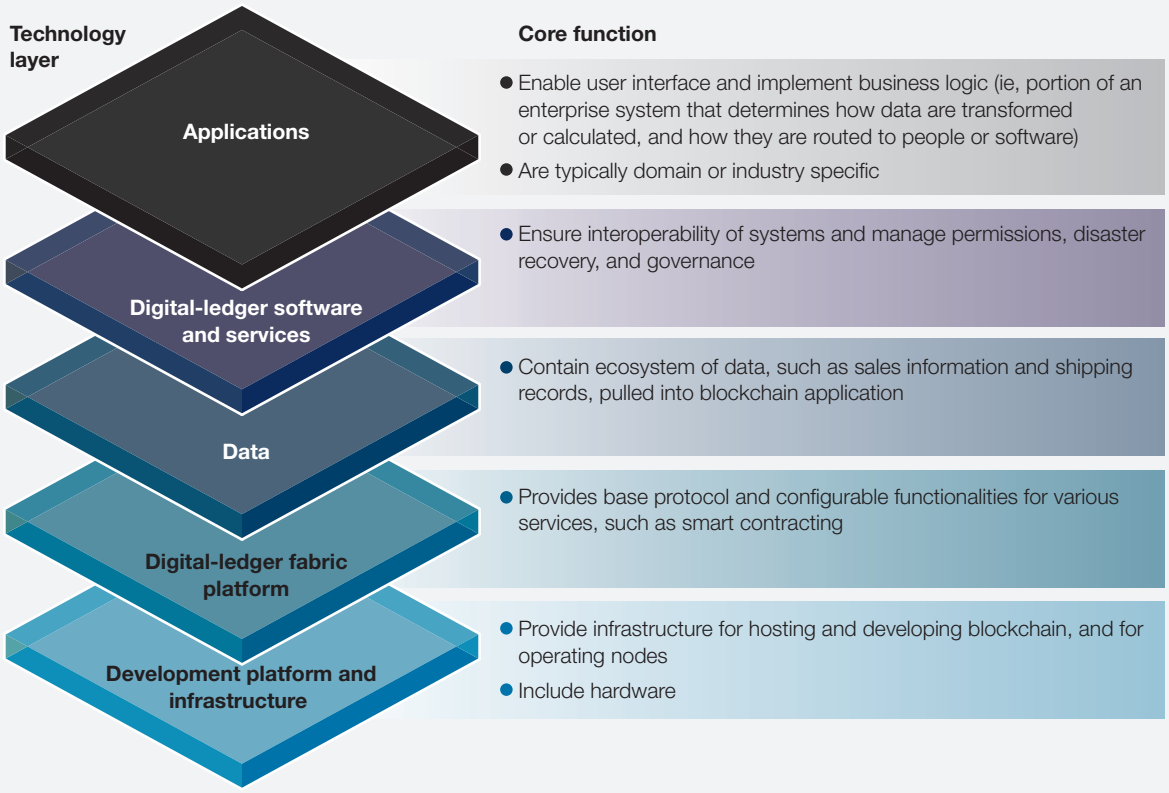
With the emergence of BaaS, the onus of deployment has moved from customers to providers. While BaaS is typically limited to the infrastructure layer, some providers also create tools that extend into the data and digital-ledger layers. With access to these offerings, customers can significantly reduce the deployment costs of a new blockchain system. For instance, they will no longer have to invest heavily in data or in ledger software and services to make their fabric platforms operational.

How industrial companies can create value in Blockchain 2.0: Core beliefs

Across industries, companies have been exploring blockchain opportunities. Many consumer-facing and industrial companies were somewhat late to the game because most applications were geared toward cryptocurrency or financial transactions during Blockchain 1.0. But their involvement will increase as more blockchain business applications move from the concept stage to reality. For industrial companies, the potential use cases span all areas of their operations, and a few have already become reality:

- An industrial company formed a partnership with a technology business that uses blockchain to track the origin of goods and their progress

Exhibit 3 **The blockchain technology stack includes five layers.**



Source: *Asian Venture Capital Journal*; VCCEdge; McKinsey analysis

along the supply chain. By providing greater transparency, the company helped customers understand the quality of its materials, the supply-chain process, and the sources of raw ingredients.

- A leading manufacturer of Internet of Things (IoT) devices formed a partnership with a blockchain start-up to create "digital passports" for individual IoT devices. The goal was to improve the expensive and time-consuming process for authentication, which involved obtaining physical certificates from authorities. By registering a device on blockchain, the company could give it a unique digital identity that could not be altered. The company could easily update the digital identity in real time to reflect any changes—a service it could not perform with physical certificates.

To help blockchain applications gain traction at industrial companies, stakeholders must address four structural challenges: inertia that prevents players from collaborating, a lack of standards, unclear legal and regulatory frameworks, and latency issues that make it difficult to verify mult-

iple transactions rapidly. For instance, Bitcoin is limited to seven transactions per second, and Ethereum can achieve 20 transactions per second. Financial institutions, such as credit-card companies, can handle between 24,000 and 56,000 transactions per second.

Based on our review of the industrial sector, we have identified three core beliefs about the ability of players to create and capture value during Blockchain 2.0.

Belief 1: The value is in specific use cases that depend on incorruptible record keeping

Blockchain's value proposition is clear: it functions as a decentralized, incorruptible database that allows peers to conduct transactions without relinquishing control to an intermediary or accepting counterparty risk. For industrial companies, such incorruptible record keeping (IRK) can be invaluable. For instance, a global wireless-network-equipment company used blockchain to provide cybersecurity for various industrial companies that used IoT, including those in utilities, oil and gas, and transportation. The IoT devices had tens of thousands of nodes, each of which represented a potential entry point for hackers. With blockchain, the company could track security threats by assigning each node a unique key that allowed it to detect unusual behavior or hacker intrusions immediately. In those cases for which IRK is not essential, industrial companies should consider using a traditional shared database for transactions, since it is less expensive to maintain.

Belief 2: Scalable use cases will involve high value, low volume, and collaborative mechanisms

The list of potential blockchain applications that industrial companies could implement is long. They could facilitate smart contracts, provide customers with a clear record of a product's origin, enhance logistics and supply chain, improve product quality, or help satisfy regulatory requirements. But not every industrial use case with strong potential will survive past the PoC stage. Those that are most likely to gain traction share three characteristics:

- *High value.* Each blockchain application must deliver significant value to the bottom line. If an information breach could cause a company to lose millions of dollars, a blockchain application might be infinitely preferable to a traditional shared database, for instance. Similarly, blockchain applications that significantly reduce cost by increasing efficiency are well worth exploring. For instance, a machinery manufacturer may have a supply chain that involves multiple intermediaries. A blockchain application that could reduce cost and complexity during shipping would deliver enormous value.

- *Low transaction volume.* Blockchain technology still has limited processing power, which makes it difficult to perform many transactions simultaneously. Until the technology advances, industrial companies should apply it to use cases that involve limited transaction volume. For instance, a consumer-equipment manufacturer could use blockchain to track and manage a few SKUs for select end consumers, rather than its entire customer base.

- *Market mechanisms for ensuring collaboration.* Several blockchain use cases, such as those for tracking goods through supply chains, will require players to share data and participate in a common blockchain platform. Initially, few companies may be willing to engage in such collaborations. In some specific cases, where companies have the market power, either because of their size or position, they will be more likely to have other players participate and obtain value from blockchain solutions.

By concentrating on use cases with these characteristics, industrial companies will prioritize

What advantages do blockchain business applications offer?

Think of blockchain as a database shared across a number of participants, each with a computer. At any moment, each member of the blockchain holds an identical copy of the blockchain database, giving all participants access to the same information. All blockchains share three characteristics:

- *A cryptographically secure database.* When data are read or written, users must provide the correct cryptographic keys—one public (basically the address) and one private. Users cannot update the blockchain unless they have the correct keys.
- *A digital log of transactions.* Transactional information is available in real time through the blockchain network. Companies doing business with each other must thus store most of their transactional information in digital form to take advantage of blockchain.
- *A public or private network that enables sharing.* Anyone can join or leave a public network without express permission. Admission into private networks is by invitation only.

Blockchain's cryptographic keys provide leading-edge security that goes far beyond that found in a standard distributed ledger. The technology also eliminates the possibility that a single point of failure will emerge since the blockchain database is distributed and decentralized. If one node fails, the information will still be available elsewhere. Another advantage involves the audit trail. Users can go back through the blocks of information and easily see the information previously recorded in the database, such as the previous owner of a piece of property. And perhaps most important, blockchain maintains process integrity. The database can only be updated when two things happen. First, a user must provide the correct public and private keys. Second, a majority of participants in the network must verify those credentials. This reduces the risk that a malicious user will gain illicit access to the network and make unauthorized updates.

those that are most likely to provide a suitable return on investment. As blockchain technology progresses and the cost of application development falls, they may investigate additional use cases.

Belief 3: Blockchain 2.0 will take off in private, permissioned networks within the industrial ecosystem

Unlike cryptocurrency transactions, industrial business applications will occur over private blockchains that limit access to invited participants, rather than over public blockchains. Some of these blockchains will have central administrators to determine which nodes have permission to access, edit, and validate data. Along with providing greater confidentiality, these private, permissioned networks are the most technically feasible, given that blockchain speed decreases and latency increases as more nodes are added.

For industrial companies, the first private, permissioned blockchains will focus on specific

"microverticals"—groups of related tasks—such as supply-chain management. Within such microverticals, participants are more likely to identify a common problem that they want to solve through blockchain and recognize the return on investment. They are also more willing to share implementation cost, since they can easily see blockchain's value. For example, leaders at industrial companies and the vendors that serve them will all benefit if they can optimize a process, reduce cost, and improve efficiency. These players will be the most willing to participate in private, permissioned networks in order to restrict access to sensitive information, such as pricing data, to select groups or individuals.

BaaS providers typically offer their platforms for free and then charge customers for each node deployed. This pricing strategy could help industrial players, since companies generally deploy few nodes during early implementation. Since industrial companies' financial risks are lower, they may be enticed to embark on more blockchain projects, even though they are uncertain about the potential returns.

How semiconductor players can create value in Blockchain 2.0: Core beliefs

Semiconductor companies have found many opportunities in blockchain since its inception. That will still be the case in the Blockchain 2.0 era, but we anticipate some important changes as the cryptocurrency sector evolves and business applications potentially become the primary sources of chip demand. So, what trends must semiconductor players understand to succeed? And who will win in this new era, for both cryptocurrency and blockchain business applications? After analyzing the hardware market, we reached four beliefs about value creation and capture by silicon players during Blockchain 2.0.

Belief 1: Value for silicon players will migrate away from cryptocurrencies (and therefore compute power) in the near future

Until blockchain business applications gain traction and demonstrate a positive return on investment—something that is not expected to occur for at least two to three years—semiconductor companies should continue to focus on cryptocurrency customers. In particular, they should try to optimize compute power and minimize power consumption to satisfy the large mining pools that rely on crypto rigs. Recently, BitMain Technologies made an important advance in this area by developing a seven-nanometer node miner.

A long-term focus on compute power isn't the best strategy, however, since many altcoins are considering moving from PoW to PoS systems, in which compute power is less important. For blockchain business applications, which could represent the wave of the future, compute power is essential but not a differentiator. Instead, semiconductor companies and other players will win by enabling or providing BaaS.

Belief 2: To win in Blockchain 2.0, semiconductor companies can't just understand their customers—they also have to understand their customers' customers

Cryptocurrency ASICs have been in extremely high demand since 2016, because miners began getting higher rewards for adding the next block. Most orders come from the top five Bitcoin mining pools in China, and the demand could increase over the next few years. This trend will keep orders flowing into substrates, ASIC designers, foundries, outsourced assembly and testing companies, and equipment manufacturers.

With value migrating from cryptocurrencies to blockchain business applications, and with BaaS players gaining market share, semiconductor companies will need to develop new strategies that align with their customers' priorities. To do so effectively, they must ask themselves four questions:

- In which specific use cases and microverticals are customers likely to adopt a blockchain solution at scale?

- Which customers or end markets have the market position and structure to ensure that all relevant players will be willing to collaborate?

- How do end customers plan to use blockchain and what aspects of our hardware—for instance, cost, compute capability, or power consumption—will differentiate the winners from the losers?

- How can we work with (or without) BaaS players, including those who provide other hardware components, software integration, or go-to-market capabilities, to enable end-to-end solutions for customers?

Belief 3: As value migrates away from hardware, semiconductor companies must go 'up the stack'

Within the current BaaS technology stack, value predominantly lies within the lowest layer: hardware. But over the next several years, as blockchain business applications start to gain a foothold within large industries, demand will increase for hardware customized for specific use cases or microverticals. This development will cause value to migrate up the technology stack from hardware to other layers.

Given these trends, semiconductor companies should consider enabling or providing the entire BaaS technology stack for specific microverticals or use cases. After developing a clear understanding of how customers plan to use their blockchain chips, semiconductor companies could then provide platforms and plug-ins that help integrate the layers of the blockchain technology stack, allowing for easier implementation. A combined offering would meet all customer needs for blockchain, just as TensorFlow does for machine learning and deep learning.

This strategy will become even more important as the use cases and microverticals start to mature, since hardware will become a commodity. Those semiconductor providers that don't move "up the stack" will have an increasingly difficult time in capturing value and thriving. In fact, they could find themselves in the same situation they face in the data-center market, where "hyperscalers" have a great deal of control because of their purchasing power.

Belief 4: The semiconductor companies that were leaders in Blockchain 1.0 are not preordained to be future winners

Today's top blockchain hardware providers, including BitMain Technologies, Canaan Creative, and Ebang Communication, are now in strong positions. But they might not be the long-term winners, despite their first-mover advantage. The barriers to market entry are low, since new players with domain expertise can easily design ASICs, and some well-known players are already planning to move into the market.

If the new players can differentiate themselves based on product performance or price, they may dethrone the current market leaders. Companies with strong end-to-end BaaS offerings may lead the pack, while those that continue to focus on hardware alone may find themselves sidelined.

If blockchain were a tool, it would be a Swiss Army knife that has a blade, a screwdriver, a can opener, and many other attachments—a clever technology that enables a diverse set of use cases that go far beyond cryptocurrency. But like a Swiss Army knife, blockchain can be unexpectedly complicated. Industrial companies must know what networks and transactions are most likely to benefit their business. They must also understand which use cases have features that are most likely to deliver value at scale—for instance, characteristics that encourage other participants to join the blockchain and collaborate. Likewise, semiconductor players must understand how blockchain is being applied, within both the cryptocurrency market and the business sphere, and

closely follow market developments in both areas. With blockchain evolving so rapidly, it can be difficult to keep pace with change. But those semiconductor companies and industrials that pursue innovation while aggressively enabling blockchain use cases are likely to reap the greatest rewards. ■

[1] Josh Ong, "The branding of cryptocurrency," *Forbes*, March 1, 2018, forbes.com.

Gaurav Batra is a partner in McKinsey's Washington, DC, office; **Rémy Olson** is a consultant in the San Francisco office; **Shilpi Pathak** is a consultant in the Chicago office; **Nick Santhanam** is a senior partner in the Silicon Valley office; and **Harish Soundararajan** is a consultant in the Boston office.

The authors wish to thank Jo Kakarwada and Celine Shan for their contributions to this article.

Designed by Global Editorial Services.