Blockchain's Occam problem

Blockchain over recent years has been extoled as a revolution in business technology. In the nine years since its launch, companies, regulators, and financial technologists have spent countless hours exploring its potential. The resulting innovations have started to reshape business processes, particularly in accounting and transactions.

Matt Higginson
Marie-Claude Nadeau
Kausik Rajgopal

Amid intense experimentation, industries from financial services to health care and the arts have identified more than 100 blockchain use cases. These range from new land registries, to KYC applications and smart contracts that enable actions from product processing to share trading. The most impressive results have seen blockchains used to store information, cut out intermediaries, and enable greater coordination between companies, for example in relation to data standards.

One sign of blockchain's perceived potential is the large investments being made. Venture-capital funding for blockchain startups reached $1 billion in 2017. IBM has invested more than $200 million in a blockchain-powered data-sharing solution for the Internet of Things, and Google has reportedly been working with blockchains since 2016. The financial industry spends around $1.7 billion annually on experimentation.

There is a clear sense that blockchain is a potential game-changer. However, there are also emerging doubts. A particular concern, given the amount of money and time spent, is that little of substance has been achieved. Of the many use cases, a large number are still at the idea stage, while others are in development but with no output. The bottom line is that despite billions of dollars of investment, and nearly as many headlines, evidence for a practical scalable use for blockchain is thin on the ground.

Infant technology

From an economic theory perspective blockchain's stuttering development path is not entirely surprising. It is an infant technology that is relatively unstable, expensive, and complex. It is also unregulated and selectively distrusted. Classic lifecycle theory suggests the evolution of any industry or product can be divided into four stages: pioneering, growth, maturity, and decline (Exhibit 1, next page). Stage 1 is when the industry is getting started, or a particular product is brought to market. This is ahead of proven demand and often before the technology has been fully tested. Sales tend to be low and return on investment is negative. Stage 2 is when demand begins to accelerate, the market expands and the industry or product "takes off."

Across its many applications, blockchain arguably remains stuck at stage 1 in the lifecycle (with a few exceptions). The vast majority of proofs of concept (POCs) are in pioneering mode (or being wound up) and many projects have failed to get to Series C funding rounds.

One reason for the lack of progress is the emergence of competing technologies. In payments, for example, it makes sense that a

shared ledger could replace the current highly intermediated system. However, blockchains are not the only game in town. Numerous fintechs are disrupting the value chain. Of nearly $12 billion invested in US fintechs last year, 60 percent was focused on payments and lending. SWIFT's global payments innovation initiative (gpi), meanwhile, is addressing initial pain points through higher transaction speeds and increased transparency, building on bank collaboration.

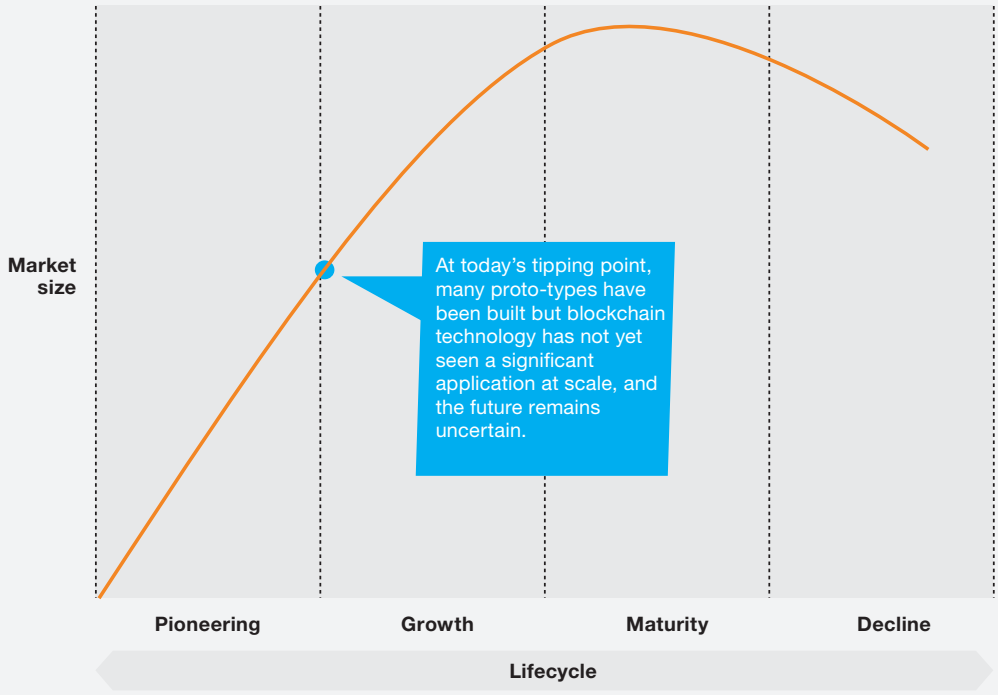
Blockchain players in the payments segment, such as Ripple, are increasingly partnering with nonbank payments providers, the businesses of which may be a better fit for blockchain technology. These companies may also be willing to move forward more rapidly with integration.

In addition, the payments industry faces a classic innovator's dilemma: incumbents understand that investing in disruption, and the likely resulting rise in customer expectations for faster, easier and cheaper services, may lead to cannibalization of their own revenues.

Given the range of alternative payments solutions and the disincentives to investment by incumbents, the question is not whether blockchain technology can provide an alter-

Exhibit 1

Blockchain: Stuck in the pioneering stage.



Source: McKinsey analysis

native, but whether it needs to? Occam's razor is the problem-solving principle that the simplest solution tends to be the best. On that basis blockchain's payments use cases may be the wrong answer.

Industry caution

Some sense of this dilemma is starting to feed through to industry. Early blockchain development was led by financial services, which from 2012 to 2015 assigned big resources where it was felt processes could be streamlined. Banks and others saw activities such as trade finance, derivatives netting and processing, and compliance (alongside payments) as prime candidates. Numerous companies set up innovation labs, hired blockchain gurus, and invested in start-ups and joint ventures. A leading industry consortium attracted more than 200 financial institutions to its ecosystem, conceived to deliver the next generation of blockchain technology in finance.

As financial services led, others followed. Insurers saw the chance for contract and guarantee efficiencies and the potential to share intelligence on underwriting and fraud. The public sector looked at how it could update its sprawling networks, creating more transparent and accessible public records. Auto makers envisaged smart contracts sitting on top of the blockchain to automate leasing and hire agreements. Others spotted a chance to modernize accounting, contracting, and fractional ownership and to create efficiencies in data management and supply chains.

By the end of 2016, blockchain's future looked bright. Investment was soaring and some of the structural challenges to the industry appeared to be fading. Technical glitches were being resolved and new, more private versions of the ledger were launched to cater to business demands. Regulators appeared to be more sanguine than previously, focusing on communication, adaptation, and debate rather than impediment.

From an industry lifecycle perspective, however, a more complex dynamic was emerging. Just as the financial services industry's blockchain investments were reaching the end of Stage 1—theoretically the moment when they should be gearing up for growth—they appeared to falter.

Emerging doubts

McKinsey's work with financial services leaders over the past two years suggests those at the blockchain "coalface" have begun to have doubts. In fact, as other industries have geared up, the mood music at some levels in financial services has been increasingly of caution (even as senior executives have made confident pronouncements to the contrary). The fact was that billions of dollars had been sunk but hardly any use cases made technological, commercial, and strategic sense or could be delivered at scale.

By late 2017, many people working at financial companies felt blockchain technology was either too immature, not ready for enterprise level application, or was unnecessary. Many POCs added little benefit, for example beyond cloud solutions, and in some cases led to more questions than answers. There were also doubts about commercial viability, with little sign of material cost savings or incremental revenues.

Another concern was the requirement for a dedicated network. The logic of blockchain is that information is shared, which requires cooperation between companies and heavy lifting to standardize data and systems. The co-opeti-

tion paradox applied; few companies had the appetite to lead development of a utility that would benefit the entire industry. In addition, many banks have been distracted by broader IT transformations, leaving little headspace to champion a blockchain revolution.

The key question now is whether those doubts are still justified. Or whether it is just that progress in developing blockchain has been slower than expected.

Over recent months some financial institutions have begun to recalibrate their blockchain strategies. They have put POCs under more intense scrutiny and adopted a more targeted approach to development funding. Many have narrowed their focus from tens of use cases to one or two and have doubled down on oversight of governance and compliance, data standards, and network adoption. Some consortia have shrunk their proof of concept rosters from tens in 2016 to just a handful today.

The emergence of cryptocurrencies, and in particular Bitcoin, as potential mainstream financial instruments prompted financial services to move first on blockchain experimentation, placing them 18 to 24 months ahead of other industries on the industry lifecycle. Given that gap, it is not surprising that the earlier concerns in banking are now emerging elsewhere, with initial enthusiasm being eroded by a growing sense of underachievement.

The reality is that rather than following the classic upward curve of the industry lifecycle, blockchain appears to be stalled in the bottom left-hand corner of the X-Y graph. For many, stage 2 isn't happening. In late 2018, blockchain's practical value is mainly located in three specific areas:

- Niche applications: There are specific use cases for which blockchain is particularly well-suited. They include elements of data integration for tracking asset ownership and asset status. Examples are found in insurance, supply chains, and capital markets, in which distributed ledgers can tackle pain points including inefficiency, process opacity, and fraud.
- Modernization value: Blockchain appeals to industries that are strategically oriented toward modernization. These see blockchain as a tool to support their ambitions to pursue digitization, process simplification, and collaboration. In particular, global shipping contracts, trade finance, and payments applications have received renewed attention under the blockchain banner. However, in many cases blockchain technology is a small part of the solution and may not involve a true distributed ledger. In certain instances, renewed energy, investment, and industry collaboration is resolving challenges agnostic of the technology involved.
- Reputational value: A growing number of companies are pursuing blockchain pilots for reputational value; demonstrating to shareholders and competitors their ability to innovate, but with little or no intention of creating a commercial-scale application. Arguably blockchains focused on customer loyalty, IoT networking and voting fall into this category. In this context, claims of being "blockchain enabled" sound hollow.

A future for blockchain?

Given the lack of convincing at-scale use cases and the industry's seemingly becalmed position in the industry lifecycle, there are reasonable questions to ask about

blockchain's future. Is it really going to revolutionize transaction processing and lead to material cost reductions and efficiency gains? Are there benefits to be accrued that justify the changes required in market infrastructure and data governance? Or is a secure distributed ledger primarily just one option when contemplating possible replacements for legacy infrastructure?

Certainly, there is a growing sense that blockchain is a poorly understood (and somewhat clunky) solution in search of a problem. The perspective is exacerbated by short-term expense pressures, cultural resistance in some quarters (blockchains may threaten jobs), and concern over disruption to healthy revenue streams. There are challenges in respect of governance—making decisions in a decentralized environment is never easy, especially when accountability is equally decentralized. And there are technical impediments, for example in respect to blockchains' data storage capacity.

It's estimated there will be over 20 billion connected devices by 2020, all of which will require management, storage, and retrieval of data. However, today's blockchains are ineffective data receptacles, because every node on a typical network must process every transaction and maintain a copy of the entire state. The result is that the number of transactions cannot exceed the limit of any single node. And blockchains get less responsive as more nodes are added, due to latency issues.

Finally, there are security concerns. In smaller networks where validation relies on a majority vote there is manifest potential for fraud (the so-called "51 percent problem"). Another potential security challenge arises from advances in quantum computing. Google said in 2016 its quantum prototype was 10 million times faster than any computer in its lab. That raises the possibility that quantum computers will be able to hack codes used to authorize cryptocurrency transactions; a particularly troubling threat for a network that claims to be fraud resistant.

Still, all is not lost. It's likely that many of the validation protocols used today will be upgraded or replaced in the next two to three years, and innovators are already finding solutions. Cardano, for example, is a so-called third-generation technology and the industry's first platform to leverage peer-reviewed open source code. The protocol is designed to be quantum-computing resistant. Private blockchains, meanwhile, are being built to give network members control over who can read the ledger and how nodes are connected.

In addition, there have been some promising advances in use cases, particularly away from the financial industry. Recent experiments in supply chains, identity management, and sharing of public records have been positive. We have seen grocery stores target customers with blockchain-enabled products and services, and shipping executives launch a new real-time registry of containers underpinned by blockchain.

An emerging perspective is that the application of blockchain can be most valuable when it democratizes data access, enables collaboration, and solves specific pain points. Certainly, it brings benefits where it shifts ownership from corporations to consumers, sharing "proof" of supply-chain provenance more vertically, and enabling transparency and automation. Our suspi-

cion is that it will be these species of uses cases, rather than those in financial services, that will eventually demonstrate the most value.

Moving through the cycle: Three key principles

There is no guarantee that any blockchain application will make a sustained move to the second stage in the industry lifecycle. To do so will require a strong rationale, significant capital, and increased standardization. Fintech leaders will need to take a more nuanced view of their target industries and hire the right talent. However, where there is potential to address pain points at scale, the opportunity remains in place.

To get there we see three key principles as minimum conditions for progress:

- Organizations must start with a problem. Unless there is a valid problem or pain point, blockchain likely won't be a practical solution. Also, Occam's razor applies—it must be the simplest solution available. Firms must honestly evaluate their risk-reward appetite, level of education, and potential gain. They should also assess the potential impact of any project and supporting business case.
- There must be a clear business case and target ROI: Organizations must identify a rationale for investment that reflects their market position and which is supported at board level and by employees, without fear of cannibalization. Companies should pragmatically consider their power to shape ecosystems, establish standards, and address regulatory hurdles, all of which will inform their strategic approach. Blockchain's value comes from its network effects, so a majority of stakeholders must be aligned. There must be a governance agreement covering participation, ownership, maintenance, compliance, and data standards. Finance arrangements must be agreed in advance so that sufficient funding through to commercial launch is guaranteed.
- Companies must agree to a mandate and commit to a path to adoption. Once a use case is selected, companies must assess their ability to deliver. Sufficient economic and technological support is essential. If they pass those hurdles, the next stage is to launch a design process and gather elements including the core blockchain platform and hardware. They must then set performance targets (transaction volume and velocity). In parallel, companies should put in place the necessary organizational frameworks, including working groups and communications protocols, so that development, configuration, integration, production, and marketing (to drive adoption at scale) are sufficiently supported.

***

Conceptually, blockchain has the potential to revolutionize business processes in industries from banking and insurance to shipping and healthcare. Still, the technology has not yet seen a significant application at scale, and it faces structural challenges, including resolving the innovator's dilemma. Some industries are already downgrading their expectations (vendors have a role to play there), and we expect further "doses of realism" as experimentation continues.

Companies set on taking blockchain forward must adapt their strategic playbooks, honestly review the advantages over more conventional solutions, and embrace a more hard-

headed commercial approach. They should be quick to abandon applications where there is no incremental value. In many industries, the necessary collaboration may best be undertaken with reference to the ecosystems starting to reshape digital commerce. If they can do all that, and be patient, blockchain may still emerge as Occam's right answer.

Matt Higginson is a partner in McKinsey's Boston office, **Marie-Claude Nadeau** is a partner in the San Francisco office, and **Kausik Rajgopal** is a senior partner in the Silicon Valley office.