The Promises and Jeopardies of Blockchain Technology

The idea of the distributed ledger of everything, which burst into the public scene in 2008 with the publication of the fascinating white paper, *Bitcoin: A Peer-to-Peer Electronic Cash System,* has transitioned from hype to reality much faster than many experts had predicted. The author of the paper vanished soon after introducing the ingenious cryptographic concept, telling a fellow Bitcoin developer back in 2011 that he had "moved to other things." This nascent technology, however, which was introduced as a mere 31,000 lines of code, has now clearly grown far beyond its original intent. At the time of this writing, CoinMarketCap, a cryptocurrency market capitalization tracking website, listed 731 coins and 562 tokens, including Marijuanacoin, Cabbage, SatoshiMadness, PonziCoin, Monster Byte and several other absurd names.

Confirming the cryptocurrency mania, a start-up called Brave recently raised US $35 million in approximately 30 seconds during an initial coin offering (ICO) to fund the development of a new web browser. Inspired by traditional initial public offerings (IPOs), ICOs are a novel capital-raising method whereby start-ups grant investors digital tokens in exchange of cryptocurrency, such as Ether or Bitcoin. Ether is the cryptocurrency that powers the Ethereum network—a decentralized platform that runs smart contracts on a blockchain, referred to as the Ethereum Blockchain. But, unlike IPOs, the majority of ICOs are carefully crafted so that they do not classify as financial assets, as doing so will automatically invoke several financial regulation clauses.

Blockchain's use cases, however, extend far beyond the realm of cryptocurrencies; this technology is undeniably destined to redefine several industries. The healthcare sector, for instance, fits the bill perfectly. Through its core virtue of decentralized architecture, blockchain is anticipated to supplant archaic, fragmented and heterogenous healthcare systems, thus boosting interoperability of healthcare data. Furthermore, by creating "a common database of health information that doctors and providers could access no matter what electronic medical system they used,” blockchain will provide...
physicians complete view to sequentially arranged patient records, improving the quality of patient care and lowering healthcare delivery costs.

Another industry prime for blockchain disruption is the complex world of derivatives, swaps and futures trading. Within this sector, the existence of “multiple versions of the truth” results in significant inefficiencies and costs through reconciliations, exception handling and manual interventions. A case in point is the Depository Trust & Clearing Corporation (DTCC), a New York (USA)-based post-trade financial services giant that processes a staggering 100 million clearing and settlement transactions daily, worth trillions of US dollars. The DTCC is executing a blockchain proof of concept to enable it and its clients “to further streamline, automate and reduce the cost of derivatives processing across the industry by eliminating the need for disjointed, redundant processing capabilities and the associated reconciliation costs.”

Given the depth, breadth and credibility of this blossoming technology, it is no wonder that a leading thinker has equated blockchain’s strategic importance to that of the World Wide Web, saying that, arguably, blockchain “might give us back the Internet, in the way it was supposed to be, more decentralized, more open, more private, more equitable, and more accessible.”

The potential and benefits of this emerging technology are compelling. The distributed ledger of everything, however, also carries complex and hidden risk. Governments, enterprises and civilians can make strategic mistakes by ignoring or discounting blockchain’s downsides. The following sections explore in-depth three fundamental challenges enterprises face when adopting blockchain: the absence of clear-cut regulations, security vulnerabilities and interoperability with existing core systems.

“The distributed ledger of everything, however, also carries complex and hidden risk.”

The Absence of a Regulatory Framework

To appreciate the significance of this matter, it is worth briefly reflecting on some historical moments that birthed and shaped securities regulations, with focus on the United States (figure 1). In the aftermath of the market crash of 1929 and ensuing Great Depression, the US Congress passed the Securities Act of 1933 and The Securities Exchange Act of 1934. These regulations were aimed at restoring the badly dented public trust in financial markets. Among a raft of requirements, the two laws mandated that

The aim of this figure is solely to highlight some of the historical moments that gave rise to and shaped US securities regulations. A detailed analysis of the history of securities exchange laws is beyond the scope of this article.
several other jurisdictions are still scrambling to figure out how to respond to this new challenge. The limited examples cited also highlight the divergent nature of regulatory responses. As a result, due to the virtual nature and global reach of ICOs, subscribers all over the world can participate in an ICO, leading to potential conflicts of laws across jurisdictions.18 This means if investors subscribe in an ICO not registered in their country and things go wrong, local laws will do little to protect them. The patchy global regulatory frameworks have created significant risk for consumers and glaring loopholes for bad guys to exploit. This vacuum is quite troubling, albeit not surprising. The disdain for centralized governance is by design; it is not an omission by cryptocurrency creators. Invented soon after the 2007 global financial crisis, Bitcoin’s original intent was to act as a counterforce to central governments, big banks and other political schemes—a concept referred to as cryptoanarchy. What cryptoanarchists did not foresee, however, is that code and cryptography by themselves cannot shield investors from the unavoidable self-dealings, greed and other transgressions of the corporate world. Predictably, three stubborn challenges have emerged.

The Explosion of Ponzi Schemes
First, the regulatory voids and related market confusion have inevitably lured counterfeiters and Ponzi schemers. Through promises of extraordinary returns, predatory and fraudulent enterprises are ensnaring unwitting investors, and then vanish after closing the purported ICO. The unsuspecting investors are often left with very little to no possibility of recovering their hard-earned funds. As Reuters underscored:

...the recent flurry of ICOs raising millions of dollars has attracted some dubious business propositions and outright scams, as well as speculators looking to trade the coins for swift gains.19

A chilling example comes from OneCoin, a phony India-based corporation whose claimed blockchain “consisted of little more than a glorified Excel spreadsheet and a fugazi portal that displayed demonstrably fake transactions.”20 In April 2018, Indian financial enforcement officers raided OneCoin, seizing US $2 million and arresting 18 OneCoin representatives in the process. By the time of the raid, OneCoin, which billed itself as “the next Bitcoin,” had allegedly siphoned at least US...
Further compounding this complexity is the wide use of cryptojargon, some of it unfathomable, even by IT experts, such as segwit, altcoins, halving, multisig, proof of stake and an assortment of other complex lingo. Consequently, most investors cannot interpret the encoded rules and do not fully understand the implications of what they are signing and to what they are agreeing. Given these uncertainties, it is not surprising that Warren Buffet, the respected chief executive officer and chairman of Berkshire Hathaway, publicly distanced himself from cryptocurrencies, saying, “I get into enough trouble with the things I think I know something about. Why in the world should I take a long or short position in something I don’t know about?”

Without historical performance data or credible cash-flow projections, it is difficult for investors to benchmark ICO valuations. Once the ideas prove unworkable, the ICO project may have lost a significant proportion of the capital, leaving investors with no recourse. These glaring issues caught the attention of Vitalik Buterin, the cofounder of Ethereum and Bitcoin Magazine, who declared at the 2017 Ethereum Hackathon in Waterloo, Canada, that 90 percent of ICOs will go under. This was a weighty declaration, as Buterin himself has a significant stake in the game.

The majority of ICOs provide white papers and terms and conditions, articulating the underlying philosophy and formal agreement between investors and the ICO issuer, respectively. The agreements stipulated in the ICO terms and conditions are enforced by smart contracts—self-executing programs that automate the transfer of digital assets once the underlying conditions are met, without the need for a central authority. But as with any other software program, there is increased risk that the smart contract “executes prematurely because it misread the circumstances” or the code may not accurately reflect the expectations of the investors. How smart contracts are coded is beyond the comprehension of several investors. Furthermore, code developers may infuse their biases into the code or unintentionally introduce flawed code. Both factors may lead to undesired or unanticipated outcomes, often to the detriment of the investor.

$350 million in scammed funds through a payment processor in Germany. Insufficient Data to Benchmark ICO Performance

It is fair to say that a significant portion of startups do not set out to create fraudulent ICOs. In most cases, however, ICOs are established to finance envisioned futures or imaginary ideas. Most of the cryptotokens sold to the public have no track records, no proven products and no assets on their balance sheets. This loophole was also emphasized by the German Federal Financial Supervisory Authority (BaFin), which warned consumers, “Typically, projects financed using ICOs are still in their very early, in most cases experimental, stages and therefore their performance and business models have never been tested.”

Closing the Regulatory Loopholes

If an important lesson can be taken from history, it is this: The current irrationality and excesses of the inconsistently regulated cryptocurrency market are somewhat reminiscent of the malpractices that preceded the 2007 financial crisis. As the US government’s Financial Crisis Inquiry Report admitted, “The crisis was the result of human action and inaction, not of Mother Nature or computer models gone haywire.”

The growing list of high-profile embezzlements continues to convey a steady and clear-cut message: Investors are going to take serious losses from their exposures in the ICO markets unless governments intervene. The previous brief narrative on the evolution of the US securities regulation indicates that regulators have historically enacted or tightened laws after consumers have suffered heavy losses. This ought not be the case with cryptocurrencies. Kicking the proverbial can down the road or assuming the cryptocurrency industry will proactively self-police would be naïve and constitute turning a blind eye to the original intentions of cryptocurrency inventors, as discussed previously.
An outright ban on ICOs may, however, be imprudent. If harnessed correctly, ICOs provide a viable alternative for startups to raise capital to fund strategic projects. As one pundit argued, “…it would be a pity if ICOs vanished as quickly as they appeared due to overregulation, as they might be very useful.” On the other hand, issuing veiled rebukes to celebrities represents only form, not substance. Regulators could, for instance, take a cue from Canada’s Autorite des marches financiers (AMF), the financial regulator for the Quebec region. In an unprecedented 2017 move, AMF extended its regulatory sandbox to ICOs, exempting specific ICOs from strict securities registration requirements, such as issuing an investor prospectus or registering as securities dealers.

Allowing ICOs to operate in a regulatory sandbox has two distinct advantages:

1. First, it provides the ICO market with a crucial opening in which to mature without stifling its potential.

2. It provides regulators an opportunity to acquaint themselves with opportunities and risk associated with this budding concept, enabling them to develop pragmatic regulations.

Cybersecurity and Vulnerabilities

While the upsides of digital transformation to enterprises, nations and civilians are unquestionable, each nascent technology also introduces a new set of security vulnerabilities, some with implications that are not yet fully understood. This constant dichotomy continues to underscore the double-edged sword of innovation. Blockchain further complicates cyberrisk, at least in two significant ways.

The DAO Case Study: A Glimpse Into the Myth of Blockchain’s Immutability

A fundamental tenet that supposedly differentiates blockchain from traditional applications is its immutability—an assumption that once transactions are appended to the public ledger and digitally time-stamped, they become persistent and irrefutable. Deleting or altering confirmed transactions becomes computationally infeasible. Traditional applications, on the other hand, function differently; their transactions can be modified, deleted or forgotten at will, and doing so requires trivial effort.

The immutability claims by the blockchain faithful have considerable merit. In addition to the vast amounts of power required to reverse transactions, blockchain uses asymmetric keys to encrypt and decrypt content, thus ensuring high levels of authentication and nonrepudiation. Furthermore, Bitcoin, the first and most successful implementation of blockchain, was proficiently designed to fend off potential attacks—so much so that, in 2013, Dan Kaminsky, a heavily credentialed security researcher who previously discovered a pervasive Internet Domain Naming System (DNS) vulnerability, confessed that he had futilely attempted to hack Bitcoin on several occasions.

This widely held belief—that records affixed to blockchains cannot be reversed—is, however, a fairy tale, considering the fate of the Decentralized Autonomous Organization (DAO). The DAO, a now-defunct Ethereum-based application, was founded in 2016 as a for-profit entity that would sell tokens to investors in exchange for cryptocurrency. In return, investors would share potential profits generated by future DAO projects. The DAO was an instant hit,
raising more than US $150 million from more than 11,000 fanatics—approximately 15 percent of all Ether in circulation at that time.

But, in May 2016, before the DAO commenced its operations, the dreams and hopes of its investors were shattered. A hacker exploited a DAO coding flaw and drained approximately US $50 million worth of Ether into a replica of the original DAO. The value of Ether plunged. The Ethereum community had three options to resolve the theft: uphold the core principle of immutability and let the attacker walk away with the stolen funds; destroy the stolen Ether in the replica DAO, ensuring the hacker did not profit from it; or, most controversial, rewrite the Ethereum protocol and erase the theft, referred to as a hard fork.

The majority of the Ethereum community voted for a hard fork. The idea of unwinding, erasing or willfully opting out of digitally signed blockchain transactions, however, did not go down well with Ethereum purists. To them, cryptocode was law and the underlying principles of blockchain were sacred. As one expert wrote, “In the raucous arena of blockchain debate, immutability has become a quasi-religious doctrine—a core belief that must not be shaken or questioned.”

When compared to several other high-profile breaches, the financial value of the DAO hack paled in comparison. The consequences of the DAO breach and the resultant hard fork, however, rippled well beyond the cryptocurrency community. It prompted the SEC to investigate and issue a public report. It ignited heated debate among blockchain experts. It also incited a revolt from Ethereum fundamentalists, who chose to stick with the unadulterated version of Ethereum, now referred to as Ethereum Classic. The DAO case study provides two vital lessons.

First, the widely acclaimed theory that cryptocode can shield blockchains from human meddling is nothing more than hyperbole. As the DAO saga vividly illustrates, transactions digitally signed on a public blockchain can be manipulated by humans. To idealists, the DAO hard fork—in which two core principles of immutability and decentralized consensus were sacrificed—resembled the financial bailouts that followed the 2007 financial crisis, whereby some banks were deemed “too big to fail.”

Second, blockchains have historically been widely touted as “well-protected, reliable and immutable.” These supposed virtues, however, are fast becoming blockchain’s Achilles’ heel. They provide a false sense of invulnerability to enterprises, perpetuating indifferent attitudes toward security. By zooming into all high-profile cryptocurrency hacks, it can easily be concluded that the majority of underlying security issues are not specific to blockchain. They are the same fundamental flaws that have vexed the digital world for decades.

For instance, in early 2018, cybercriminals stole a staggering US $534 million from Coincheck, a Japan-based cryptocurrency exchange. Apparently, Coincheck’s coins were accessible from the Internet, a concept referred to as “hot wallets.” Coincheck also lacked multisig, the equivalent of multifactor authentication. Another example comes from Mt. Gox, another Japan-based Bitcoin exchange that was bankrupted in 2014 when thieves siphoned more than US $400 million. Mt. Gox, according to several reports, had poor version control procedures and was a victim of suspected malicious insiders. Using classic phishing scams—such as spoofed websites—crooks have also duped several unsuspecting individuals into divulging private keys to their digital wallets, leading to heavy losses.

Blockchain security problems, it turns out, are more human than technical.
Addressing Cybersecurity Matters

No framework or technology can provide impermeable defenses against cyberthreats. The right set of controls should be dictated by the value and exposure of the underlying assets. With that caveat in mind, here are five key issues enterprises should consider when embracing blockchains:

• Develop a baseline of nonnegotiable security controls and governance procedures to ensure no blockchain projects are opted out of any mandatory controls without stringent sign-offs.

• Implement robust technologies and processes to ensure cryptographic keys are protected from misappropriation or inadvertent loss. Consider storing private keys to digital wallets offline, for example, on removable USB drives, safe deposit boxes, offline hardware wallets or paper wallets. It is, however, important to emphasize that none of these will provide immunity against financial loss. For instance, while paper wallets are insulated from online attacks, they are also vulnerable to other hazards, such as fire or theft. Risk specific to each cold storage option should be carefully assessed, and appropriate mitigations should be implemented.

• Use multisignature (multisig) digital wallets, whereby two or more private keys, stored separately, are required to transfer funds from a specific address.

• Develop detailed security test scenarios and ensure that the effectiveness of each mandatory control is independently validated in a sandbox environment prior to implementation.

Impediments to Transformational Change

As with any other disruptive trend, the rise of blockchain reignites the dynamic interplay between continuity and change. Maneuvering past these constant dualities requires careful balance between innovation and business stability; neither of these two can be managed in isolation. Enterprises that blindly fight change, fail to adapt and hold on to established routines may eventually lose relevance to their customers. This risk looms larger for...
established players, whose market dominance is still underpinned by legacy systems and processes. According to research, incumbent firms that neglect digital innovations can experience up to 50 percent and 30 percent reduction in revenues and earnings, respectively.18

Unavoidably, blockchain renders a wide array of existing decentralized applications obsolete, particularly those that support back-office processes. Adding another layer of intricacy, most of these systems have operated steadily over many years and still underpin strategic revenue lines. Such is the case of the Australian Securities Exchange (ASX), which announced in 2017 plans to replace its Clearing House Electronic Subregister System (CHESS)—implemented in the 1990s—with a distributed ledger solution.29 Architecture documentation for most of these archaic applications has not been consistently updated as businesses have been transformed and original subject matter experts have either moved on or are now deceased.

Furthermore, an enterprise’s culture—“elements of social behavior and meaning that are stable and strongly resist change”40—can also present significant inertia to blockchain implementations as employees resist change and stick to their old ways of working. Business routines, mind-sets and norms are shaped and reinforced over years, making them harder to dislodge with the passage of time.

Response

To get past these technological and cultural hindrances to blockchain adoption, best-in-class enterprises set realistic expectations upfront when embracing blockchain. They actively resist the urge to jump into execution mode. Rather, they take measured steps and start their blockchain journey by asking hard questions, such as:

- Has the enterprise conducted an in-depth diagnosis to identify entrenched routines, bureaucracies and deep-seated interests? If yes, has the enterprise devised effective change management strategies to diffuse those cultural obstacles?
- What strategic advantages or areas of core differentiation can be amplified by embracing blockchain technologies?
- Which strategic platforms, if replaced by blockchain, lead to reduced long-term operational cost issues, increased business resilience and more scalable digital environment?
- What expertise is needed to develop required blockchain platforms, dislodge and migrate legacy applications, and interface blockchains with core applications?

Blockchain, which is still in its infancy, promises to tackle several pressing global challenges. For instance, blockchain-based smart contracts are anticipated to facilitate direct, transparent and irreversible transfer of funds from donors to those in dire need, eliminating needless intermediary costs and cutting global poverty.41 But, if the weighty challenges explored in this article are discounted, they could undermine faith in this important technology. A leading thinker and author agrees: “If we get this wrong, Blockchain technology, which holds so much promise, will be constrained or even crushed.”42

Endnotes

3 Ibid.


13 Mougayar, W.; The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, Wiley, USA, May 2016


18 Barsan, I.; “Legal Challenges of Initial Coin Offerings (ICO),” Revue Trimestrielle de Droit Financier (RTDF), no. 3, 2017, p. 54-65


25 Ibid.


28 Op cit Barsan


37  Mougayar, W.; The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, Wiley, USA, 9 May 2016


40  Rumelt, P.R.; Good Strategy/Bad Strategy: The Difference and Why It Matters, Profile Books, United Kingdom, 2011


42  Op cit Tapscott and Tapscott