Building a better working world

Blockchain: the hype, the opportunity and what you should do

By Angus Champion de Crespigny, Ernst & Young LLP

New technology often sounds like science fiction. Then it's mocked and feared. And then it seems inevitable, but only in retrospect.

Blockchain, a type of database that records an ongoing list of tamper-proof records, or "blocks," has reached the peak of the hype cycle. Given the extraordinary amount of attention the technology has received, it's not surprising that some think blockchain is the answer to everything. Claims that it will disintermediate large clearinghouses and make existing payment networks irrelevant are common despite the technology's relative immaturity. Public blockchains (e.g., bitcoin) have been immune to the sensationalism of late, but they too were subjects in the hype cycle early on.

There has been plenty of noise, no doubt, but deep down there is substance. Blockchains (both public ones and those requiring permissions) carry great promise — databases are ubiquitous in every industry, and distributed consensus across an open network or a group of organizations is a valuable proposition and will force existing business models to evolve, creating entirely new business models in the process. And while in hindsight such developments seem to happen overnight, they take time, usually several years, to develop and mature.

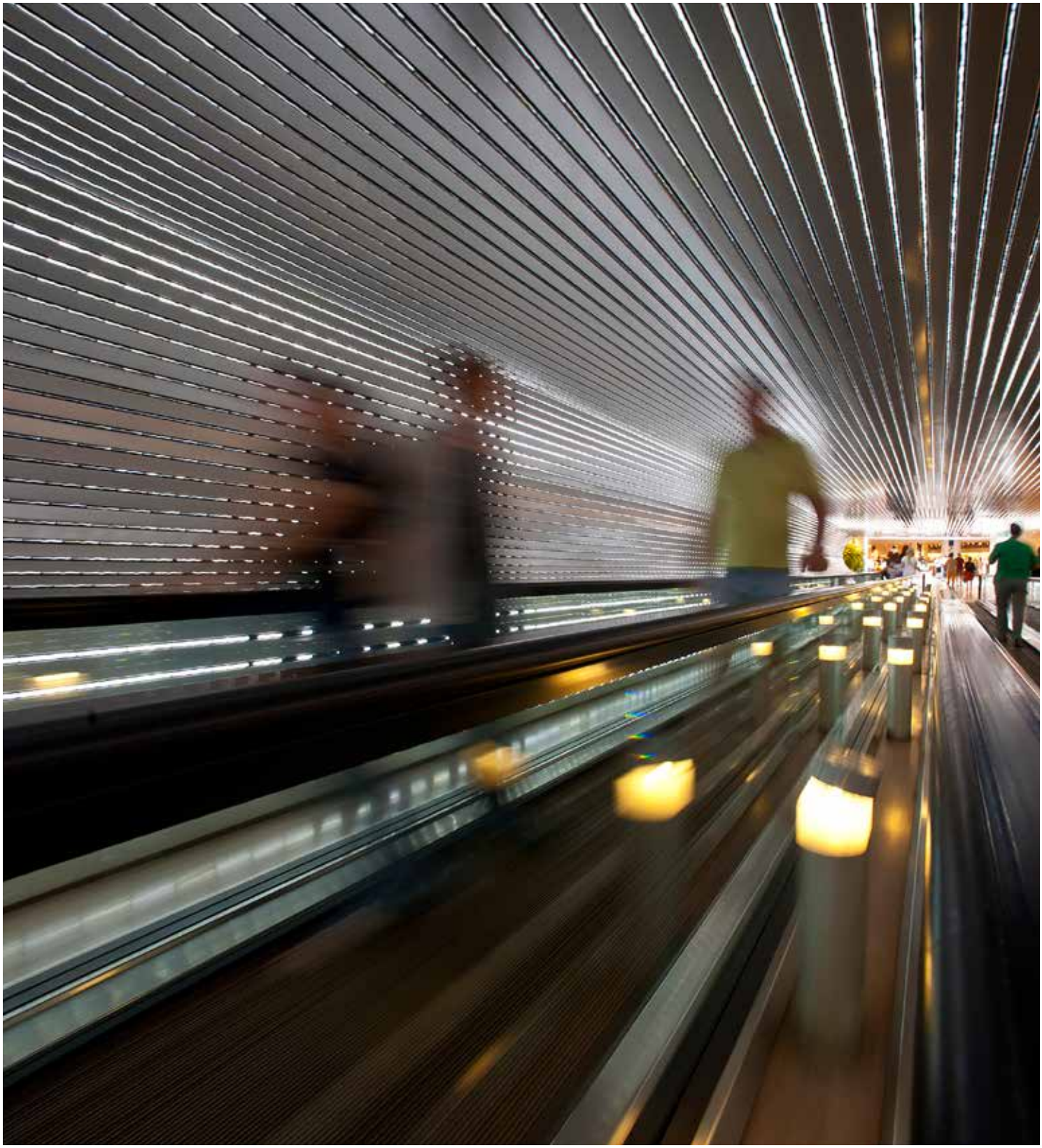
As with any new technology, there are risks, both technical and operational, associated with adoption, and organizations are right to consider these during their evaluations.

Level setting

Database technology is not new. In fact, distributed databases have been around for a decade, and relational databases have existed for even longer. Blockchains are another form of database, and while they share many elements with more traditional forms, the differences make them truly innovative. By design, blockchains are intended to be shared, by individuals, organizations, even devices. In a digital world, where databases are the infrastructure, blockchains are common infrastructure — shared "plumbing" through which many data types can be stored, referenced and transferred as well as a mechanism by which that activity can be immutably recorded.

With blockchains, one size does not fit all. A blockchain-based system can either be open and public, or private and requiring permission to access. Public blockchains are open to anyone. No permission is required to join and participate in the network. They are also inherently transparent; all actions on the network must be validated by, and visible to, all participants on the network. If any action is not visible to all participants, the action cannot be properly validated.

Private, permissioned blockchains are quite the opposite. Permission is required before a participant can join, and thus participate in, the network. Participants may be assigned a mix of read and write permissions. Certain participants can have the ability to read and write, whereas others may only have permission to read or write. The ability to assign a variety of permissions to network participants is particularly suited for use in more commercial contexts, such as financial services, where certain actions and information are not intended to be public. In this example, participants would retain the benefit of a shared infrastructure while maintaining a level of security and privacy.



As with any new technology, there are risks, both technical and operational, associated with adoption, and organizations are right to consider these during their evaluations.

Reality check

It is fun to talk about new technology and the opportunities that follow, but a healthy discussion of blockchain must acknowledge its immaturity and the growing pains it will likely experience. Here are some of the issues in relation to blockchains.

1. Technology limitations

Being a young, still-evolving technology, there are certain aspects of the technology that may require further development or modification to reach its anticipated potential. For example, the same mechanism that provides trust to a public blockchain also introduces latency to the network. Transaction verification requires consensus: consensus requires some amount of computation, and computation takes time. As a result, transaction processing is not instantaneous and can often take several minutes. Certain protocol designs have decreased the processing time to less than a minute, but real-time processing is still prohibited with current models.

Consensus and computation also limit transaction throughput. Transactions on a public blockchain need to come to consensus with a large number of untrusted participants, which requires time. Permissioned blockchains or existing transaction platforms, however, do not have the same limitations considering their different trust models.

2. Regulatory uncertainty

Broadly speaking, technological innovations are subject to regulatory requirements and expectations that apply to bank operations more generally (safety and soundness, risk governance and risk management, cybersecurity, data security and privacy, vendor/third-party risks, compliance, BSA/AML, etc.). Nevertheless, policymakers and regulators continue to evaluate the regulatory framework as new technologies, like blockchain, emerge and evolve. Policymakers and regulators want to ensure that any potential risks to the safety and soundness of financial institutions, the stability of the broader financial system and other important policy objectives like consumer and investor protection posed by evolving technologies are appropriately addressed. The need for any specific regulatory response concerning blockchain applications and the distribution of digital assets across multiple environments, both of which continue to evolve, remains uncertain.

3. Insufficient enterprise testing

With the exception of bitcoin, which has been in "production" for more than seven years, most blockchains have not had the benefit of production-level testing or the pressures that accompany a live environment (real transaction volumes, system penetration attempts, system interoperability, etc.). This has started to change of late, as more organizations have announced permissioned blockchain implementations that will run live, albeit in parallel to existing systems. As the focus continues to shift from proofs of concept and pilots to production implementations over the next five years, testing will be a key factor in the technology's success.

4. Security

New IT systems introduce new cybersecurity risks, particularly a distributed IT architecture across multiple business functions or organizations. The type and amount of data stored on the blockchain will affect the risk profile, as will the permission mechanisms used. There has also been little talk of key management — keys being the equivalent of passwords that provide access to the network — which has been a sore spot for the technology in the past few years and contributed to a number of high-profile exchange hacks that resulted in hundreds of millions of dollars in losses.[1] This will be a greater topic of discussion in the coming years.

Smart contracts, or programming code that is executed independently and has its output confirmed by multiple participants in a network, thus creating a program whose logic can be trusted by all network participants, are particularly susceptible to security risks. More and more, smart contracts are being used to deploy business logic on a blockchain. The logic can represent contractual terms between parties or rules associated with a particular workflow. There have been a number of widely publicized exploitations of smart contracts, due in part to the lack of review and testing prior to deployment. However smart contracts are being used, the underlying code should be tested as extensively as the network itself.

We're in the first iteration

New technologies are iterative — the first version is never perfect, but it forms the foundation for subsequent and improved versions. As is apparent from the list of challenges above, blockchains are in their infancy. They lack the interoperability required for enterprise deployment and introduce new issues regarding identity management and data security. But the technology will develop, existing business processes will change, and new business models will emerge.

Private blockchains have already gone through a first iteration for securities settlement and clearing and trade finance. Similarly, public blockchains are starting to address elements that cross industries, including identity management and payments. As the iterative process for public and permissioned blockchains continues, positioning your organization to take advantage of the development is critical.

Development is happening

- Venture capital investments into public and permissioned blockchain start-ups via publicly disclosed funding rounds:[2]
  - 2015: $360+ million
  - 2016 (through April): $1,020 million
- Blockchain start-ups: 400+[3]
- Banks looking into blockchain: All of them

Development is happening on both public and permissioned platforms and at all levels of the respective technology stacks. Foundational, standardized protocols are being built horizontally to support specific industries. Middleware and applications are also being developed vertically on top of these protocols to address specific business applications and processes. Once protocol standards are accepted for a given industry, vertical development will accelerate.

Much of the development at the moment on public blockchains relates to scalability. Increasing transaction speed and throughput may be necessary for any real commercial activity. Performance is less of an issue for permissioned blockchains, where much of the development has been focused on building specific applications with the requisite business logic to process specific transaction and data types.

To prepare, financial institutions need to understand the technology so that they can make informed choices about how and when to respond to technological advancements and subsequent process and business model shifts.

Small steps and giant leaps

An imaginary line is often drawn between public and permissioned blockchains, and organizations may feel that they need to choose one model or the other. The truth is, both are powerful, and both will have significant, yet distinct, effects on financial services.

In the context of permissioned ledgers, the conversation has generally been "How do we use this technology to perform an existing business process faster, at a higher level of accuracy and with fewer resources?" There is tremendous value in achieving this efficiency, but the underlying business model is essentially the same. These are small, efficiency-driving steps forward for industry incumbents.

On the other hand, in the context of public ledgers, the conversation has generally been "How do we use this technology to completely disrupt an industry?" The answer is usually by distributing and automating previously centralized functions. From a purely technological standpoint, bitcoin was an attempt to completely disrupt peer-to-peer payments. It circumvented the existing payment infrastructure, completely changed the fee structure for moving money and gave anyone with an internet connection the power to store and transfer financial value from a mobile phone. This could yet be a giant, control-shifting leap forward for consumers, except for a small number of missing pieces. (More on this later.)

Small, efficiency-driving steps (more frequent), and giant, control-shifting leaps (less frequent) will happen in parallel, with one likely laying the groundwork for the other. It's important to participate in the small steps forward while keeping an eye out for big-leap opportunities. Preparation for the leap is as much about awareness as it is about readiness.

Evolution vs. revolution

Blockchain technology, when used in a private manner, allows the development of different business and operational processes that previously were not possible due to the distribution of data or trust among the parties in the system. Fundamentally, however, the technology in this form is simply a reengineering of current data management paradigms.

The differences when moving from a private, semi-trusted user group using a permissioned ledger to a fully public, untrusted user group will enable some fundamentally new capabilities that should not be easily dismissed.

Bitcoin and other public blockchains have often been dismissed by institutions and enterprises, primarily for three reasons:

1. A reputation of a historical association with transactions on the dark web

2. The lack of control or ability to govern the network by regulatory-sensitive organizations

3. Its use as a currency, which has little practical use in many current regulatory environments

First, to effectively innovate, technology should be evaluated on its own merits and not by its reputation: some of the attributes that made the technology valuable to those on the dark web, such as irrevocable trust and immediacy of value transfer, can be just as valuable to those in the traditional financial sector.

Second, the ability to leverage the concept in a manner that keeps the network safe in a semiprivate system, embedding additional facilities and being able to control the network to provide comfort to risk-averse institutions, is a logical first step. This is appropriate to manage risk; however, over the longer term, this will limit the future potential of the technology: in the same way that intranets are significantly safer for organizations than the open internet, they will be limited in their benefit.

Last, bitcoin's utility as a currency is limited in the current regulatory environment; however, this limitation is because of a disconnect between two aspects: the sending of value and the identities associated with the parties involved. While bitcoin allows the sending of value instantaneously in a peer-to-peer fashion, our definition of identity still resides in the physical world, such as passports, driver's licenses and birth certificates. Assuming that bitcoin and other cryptocurrencies will never be effective for compliance reasons assumes that the regulatory environment will always look the same. This regulatory environment changes significantly when a reliable digital identity can be established.

Establishing a reliable, robust and easily available digital identity is no easy feat, however, but it will have a significant impact on financial services more broadly. Retail payments would become accessible outside of the traditional financial system, reducing customer engagement for financial institutions. With reduced customer engagement come reduced abilities to build customer value through cross-selling other financial products. In short: the financial ecosystem changes drastically by becoming far more competitive, requiring different business models to build value in new ways.

In this manner, value transfer becomes simply another form of data, moving financial services from a vertical industry into a horizontal capability. Value transfer can

be performed by devices, integrated into apps, web browsers and mobile devices, automatically purchasing products as required without needing the configuration of a separate payment rail. Physical assets such as vehicles, factory equipment and medical devices can be integrated directly into cryptocurrency blockchains so that they can be financed directly by lessors or financiers, with critical asset data being simultaneously transferred on the same network.

This future state enabled by bitcoin and other public blockchains, consequently, is not necessarily in replacing current products and services but in the creation of brand-new products and services that work entirely outside the current recognized model.

Bitcoin as a global source of truth

Bitcoin, when seen purely as a cryptocurrency, however, does not do justice to the full power of a public blockchain. A public distributed ledger is built to do one thing very well: establish an agreed-upon record of data among its participants. In bitcoin, this is used to record who has sent the currency to whom, and occasionally to record logic (in the form of smart contracts), which is agreed to be executed when later data is accepted onto the network. What a public blockchain consequently provides is a global source of truth, where activity or data is time-stamped when it occurred and is stored independently of any party able to modify it undetected.

To this point, verifications have typically required a trusted party to provide evidence of the existence, validity, timing, integrity or any other number of points

The ability to create digital assets that can be uniquely identified and traded can bring the concept of property rights to the digital world, which may have a meaningful impact on consumer adoption long term.

in a digital asset. Without the need for trusted parties to provide this verification, however, new business models can be created in a purely peer-to-peer fashion, establishing trust in a far more frictionless manner.

Immediate opportunities may include the recording of ownership or existence of a digital agreement stored on the bitcoin blockchain. Such a record would provide evidence whose existence, integrity and timing of creation could not be questioned, and could be established through the simple process of sending a microtransaction on the bitcoin blockchain.

Once such records can be digitized on a blockchain, they can also be transmitted across the network. This leads to the theoretical possibility of being able to make secure and trade any object that can be digitized onto the blockchain, leading to the potential for many new financial instruments.

The value of open source

When the original version of bitcoin launched in January 2009, it was released under an open source license, allowing anyone to use, copy, iterate on and make derivative works of the software. As the community of enthusiasts grew, subsequent years saw an explosion of new cryptocurrencies, many of which were forks (i.e., copies) or minor adaptations of the original bitcoin software. This would not have happened without open source software.

The history of open source is a history of innovation. From Linux to bitcoin to the discovery of the Higgs boson, the beauty of open source is its ability to enable progress. It encourages experimentation and rewards collaboration and sharing. Development is not beholden to revenue targets, regulatory constraints or the needs of a particular market segment.

Public blockchains, by their nature of being open source, will be the sandboxes for "big leap" innovation. Development will ultimately happen faster, and in more directions, than it will on permissioned blockchains. Some things will succeed and be adopted, others will fail and be ignored, but the collective pursuit will produce truly revolutionary change.

Key milestones that will drive adoption

Blockchain is often described as a "foundational protocol" similar to Transmission Control Protocol/Internet Protocol (TCP/IP) — interesting technology by itself but having little consumer or commercial application without a complementary technology stack on top. As discussed earlier, the development of technology standards will accelerate vertical development and produce the applications that drive adoption. The technology will also need, and greatly benefit from, a legal framework that enables, supports and protects contractual arrangements on the blockchain. Smart contract technology allows parties to engage in transactions according to predefined terms. But to be commercially viable, issues in relation to intent, custody, liability and indemnification will need to be figured out.

The proliferation of digital assets also introduces new issues regarding property rights. There is a reason you acquire property rights to a physical album upon purchase but only a license to a digital copy of that same album upon downloading. The ability to create digital assets that can be uniquely identified and traded can bring the concept of property rights to the digital world, which may have a meaningful impact on consumer adoption long term.

Regulation may have an impact on adoption as well. Consumers, policymakers, regulators and the financial services industry more broadly have a common interest in ensuring that the adoption of technological innovation is subject to a consistent set of protections across the industry. This will require a delicate balance, as blockchain technologies could potentially introduce new or different risks that are not fully contemplated in current regulatory frameworks. Depending on the nature of the risks and strength of controls, this may require changes or enhancements to existing regulatory frameworks and processes to protect the broader financial system.

Be proactive, not reactive

We recommend that financial institutions proceed with the following steps:

1. Get educated

No matter what you think of the technology, it's worth your time to become educated on how it works. Read up on it, gain in-house expertise and encourage your business teams to do the same. Ask yourself these questions:

- What could your products and businesses look like when trust is distributed?
- What does your business look like when value moves like data and finance is openly accessible?
- In this broader digital world with open financial markets, how can you help customers engage with your business because they want to and not because they have to?

If you start too early with your response to blockchain, the worst case is that you'll have wasted some time on research and development. Even if you start early, learning about blockchain technology has increasing relevance to ongoing challenges in areas related to IT strategy and cybersecurity. Blockchain has become an increasingly visible part of the financial ecosystem, and even organizations that decide not to make it part of their service lineup will need to compete with organizations that do.

However, if you wait too long to respond, you may miss the opportunity to capture and develop foundational components of the future ecosystem.

2. Start small and expand

While the benefit of blockchains is in distributing trust over many parties, that isn't where you need to start. Many applications can be developed in-house, tested within the group and expanded beyond the four walls of your business as the model is proven.

Additionally, putting everything on a blockchain to begin with is not necessarily either a wise business or technology decision. Use blockchains for what they are valuable — being a framework to establish trust — but otherwise, keep initial deployments simple with familiar technologies while leveraging the new technology for its added power.

Meet with the major players, develop some proof-of-concept tests, pilot internally and then expand with selected customers.

3. Identify and seize opportunities to build foundations

While blockchain is at the top of the hype cycle, the foundations of many disruptive technologies are built before they reach mass consumer adoption. Consequently, as the public blockchain ecosystem develops, financial institutions can help build these foundations to play key roles in the future state. The large IT multinationals that dominate global markets built their services based on underlying services created at the beginnings of the web — search, web browsers, email, e-commerce — and reshaped the consumer experience. There are a number of foundations that will be established in this future ecosystem that will be fundamental to its growth and operation and, consequently, many new business opportunities to be created.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY is a leader in serving the global financial services marketplace
Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

EYG no. 04165-161Gbl
1610-2083782 BDFSO
ED None

ey.com

Endnotes

[1] "Hacked Bitcoin Exchange Users to Lose 36%," Bloomberg, 6 August 2016 Yuji Nakamura, "Hacked Bitcoin Exchange Users to Lose 36%, Bloomberg, 6 August 2016, https://www.bloomberg.com/news/articles/2016-08-07/hacked-bitcoin-exchange-users-to-lose-36-will-receive-tokens

[2] EY's Horizon Scanner, 1 May 2016

[3] EY's Horizon Scanner, 1 May 2016