


CRYPTO-ASSETS: THEIR FUTURE AND REGULATION

OCTOBER 2018



AUTHORS
Douglas J. Elliott
Larissa De Lima

INTRODUCTION

Authorities around the globe face challenging questions about crypto-assets and their regulation. The right approach will depend significantly on how crypto-assets evolve. Projecting this evolution, and drawing conclusions on appropriate regulation, requires: analysis of (1) the "users" and (2) the cryptoeconomy in which they operate. (Note that "crypto-assets" is the official sector's preferred term for what has more generally been termed "cryptocurrencies," as most officials believe crypto-assets do not function effectively as currencies).

We break the users of crypto-assets into six broad groups:

- **Libertarians and techno-anarchists**, who want a currency without a government, for ideological reasons
- **Economic pessimists**, who do not trust their governments to manage their currencies
- **Seekers of anonymity**, who want to undertake transactions and investments anonymously
- **Technical users**, who find crypto-assets useful for some blockchain applications
- **Investors**, who believe crypto-asset prices will rise significantly over time
- **Speculators**, who gamble on shorter-term price movements

These market segments are large enough globally to support substantial growth of crypto-assets in the long run, regardless of market fluctuations. However, crypto-assets are particularly vulnerable to the effects of a severe crisis of confidence, since they are not backed by governments, guarantees from large institutions, or tangible assets as other currencies and quasi-currencies are. So, growth in this asset category is very likely in the long run, but not inevitable.

The cryptoeconomy has at least five defining characteristics that distinguish it from the financial economy that regulators normally oversee.

Crypto-assets:

- Are not tied to national authorities
- Power digital and borderless economies
- Do not fit neatly into any conventional asset class
- Rely on decision-making by a decentralized network of actors
- Use multiple different models to govern decision-making in these networks

Taking these two sets of points together, we reach a number of conclusions about appropriate regulation of crypto-assets:

- Regulation is necessary – crypto-assets are unlikely to disappear and there is a need for the protections and operating benefits that regulation brings
- Regulation by activity will likely work better than treating crypto-assets as one category
- New regulatory frameworks may be required to ensure stakeholder protections
- Global standards are needed
- Policymakers will need to analyze and monitor incentives within the cryptoeconomy
- Consideration must be given to how to regulate a system driven by decentralized software

For clarity, we would emphasize that blockchain, the software approach underlying crypto-assets, could thrive regardless of the future of crypto-assets. Although the technique was developed for Bitcoin, it has many other current and potential uses outside of this realm. In addition, we do not discuss central bank digital currencies here, despite some similarities to crypto-assets. Their close ties to central banks make them fundamentally different than true crypto-assets.

For those unfamiliar with crypto-assets, please see our paper, “Cryptocurrencies and Public Policy: Key Questions and Answers.”¹

1. Elliott, Douglas, Larissa de Lima and Ryan Singel, (2018). Cryptocurrencies and Public Policy: Key Questions and Answers. Oliver Wyman

The “users” of crypto-assets

There are at least four substantial market segments likely to provide long-term support for crypto-assets, in addition to speculators and investors who primarily focus on price appreciation.

Libertarians and Techno-anarchists

There are segments of the population that simply prefer a non-governmental currency for reasons of political philosophy. Conventional currencies are controlled by central banks and the governments to which they are ultimately responsible. Some people believe that gives governments too much control and, in many cases, believe that it leads to systematic problems, such as hyperinflation or excessive governmental interference in the economy. These groups are clearly a relatively small minority in percentage terms, but still represent a large absolute number.

People who deeply distrust their government’s economic management

Some people own crypto-assets for the same reason that many hold gold, as a method of storing value that avoids the risk of economic mismanagement by governments, replacing it with other risks. Some of these beliefs may appear unusual, such as expecting hyperinflation to hit the United States imminently, but some people hold similar expectations in very troubled countries where it appears reasonable to deeply distrust government management. Additionally, in many of these countries, the ability to keep direct control of assets could prove valuable, as there is precedent for sovereign states to seize assets in times of crisis or political turmoil. Anyone deeply suspicious of government policy is also likely to value anonymity to protect against expropriation or capital controls.

Seekers of anonymity

There are also many who wish to retain anonymity for their transactions. Some of these are criminals, but many others are not. For example, anyone who has beliefs that lie outside the mainstream may prefer anonymity, especially in countries with authoritarian tendencies. Others simply value privacy for its own sake. It is difficult to estimate how many people place a high value on anonymity, but it is clearly a significant number.

Technical users

For some applications of blockchain technology, it is either helpful or necessary to use crypto-assets as an internal currency. These crypto-assets may also be made available to outside buyers, including through Initial Coin Offerings that can help fund the activities of the sponsoring organization. We also include in this group those who may use or plan to use crypto-assets due its technological advantages (for example. efficiency in payments) rather than the motivations described above. We will not discuss this further, except in passing, due to the technical complexity and variability among uses. It is difficult to estimate the size

of demand from this set of users, as it depends on many factors, including the rate of take-up of blockchain applications in the future, which is the subject of lively debate.

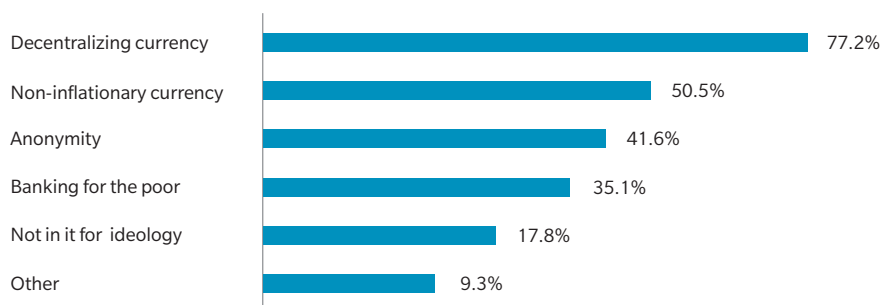
There are existing ways for most of these market segments to achieve their objectives, such as using cash to protect their anonymity or holding gold as a quasi-currency, however crypto-assets are more portable and lend themselves to electronic transactions. Additionally, crypto-asset growth and expansion can be a self-reinforcing phenomenon, as those that have found value in crypto-assets are more likely to be invested in their continued success.

Why do we focus on these four segments and not the very substantial community of speculators and investors that appears to be driving pricing in these markets today? Simply because the long-term future of an asset class tends to be driven more by the underlying value provided to various market segments than by short-term movements in views of valuation. As Warren Buffett has said about the stock market, “in the short term, it’s a popularity contest; in the long term it’s a scale”, with values based on a company’s “weight”, meaning the value of its net assets and earnings. If there are not users of crypto-assets who perceive a direct value to themselves, speculative and investment impulses are unlikely to support these assets in the long run.

How closely does this conceptual framework of users match the actual make-up of crypto-asset holders? There is little market or survey research available publicly about crypto-assets, but an interesting unscientific poll of crypto-asset holders found the results shown in Exhibit 1 below, which match up well with our user groups.

Exhibit 1: Survey results from poll of crypto-asset holders

% OF PARTICIPANTS WHO ARE IN CRYPTO
ARE YOU INTO CRYPTOCURRENCIES FOR IDEOLOGICAL REASONS? IF SO, WHICH ONES?



Source: Biehl, Z. and More, R. (2018). A Big Cryptocurrency Survey Was Conducted on Reddit, and the Results Are Fascinating – Invest In Blockchain. [online] Invest In Blockchain. Available at: <https://www.investinblockchain.com/reddit-cryptocurrency-survey/> [Accessed 5 Sep. 2018].

Our market segment analysis could theoretically be rendered irrelevant if governments try to kill or very sharply limit crypto-assets. However, they would have to make a strong, persistent, and global effort to succeed. We do not believe it likely that they will do so. Regulation is certainly coming and some jurisdictions appear poised to strongly discourage crypto-assets. But, these steps would not kill crypto-assets and their effectiveness would be sharply limited if there is not global consistency. In practice, while some nations have strong doubts about crypto-assets, there are others who are actively promoting them.

What makes crypto-assets different?

Crypto-assets are unique in that their existence and operation is governed by a fundamentally different set of constraints than for conventional financial instruments. This requires regulators and policymakers to understand the key design features of crypto-assets which will directly impact future regulation. A number of such considerations are described below.

Crypto-assets are not tied to national authorities

The original role of crypto-assets was as a currency or quasi-currency. Unlike crypto-assets, conventional currencies are closely tied to national governments and central banks, even if these currencies are sometimes used outside of those borders, as is the case with “Eurodollars.” National authorities make decisions about fiscal, monetary, and foreign exchange policy that affect the intrinsic value of these currencies. In contrast, the value and supply of each crypto-asset is managed by its community. No government regulation or guidance currently exists around managing crypto-asset supply and most crypto-assets are not based within any one specific jurisdiction.

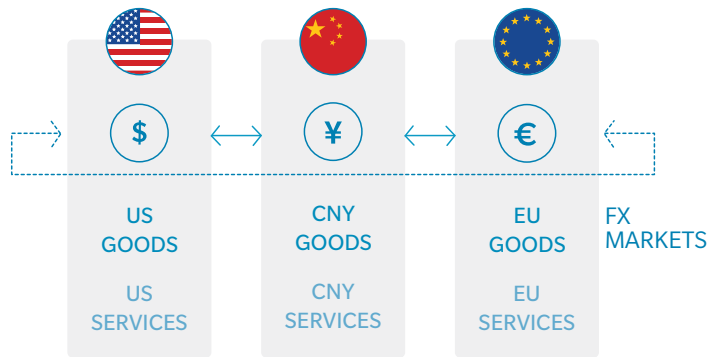
Crypto-assets power digital and borderless economies

As more peer-to-peer (non-intermediated) transactions are conducted between individuals spanning the globe, network effects grow and redraw economic boundaries. Different agents within the crypto-economy can span multiple geographies (for example, developer teams, miners, exchanges and users may all be in different countries). This will make it increasingly difficult to apply traditional regulatory and policy strategies to control them, as by design there will never be a single sovereign state that is responsible for oversight at all times (See Exhibit 2 below).

Exhibit 2: Traditional economies vs. Crypto-economies

TRADITIONAL ECONOMIES

Economies are determined based on geographic location and common social/political views



Economic exchange mediated by fiat currencies (fiat) managed centrally through a central bank and through FX markets

VS

NEW DIGITAL ECONOMIES

Economies can be constructed based on any set of goods and services

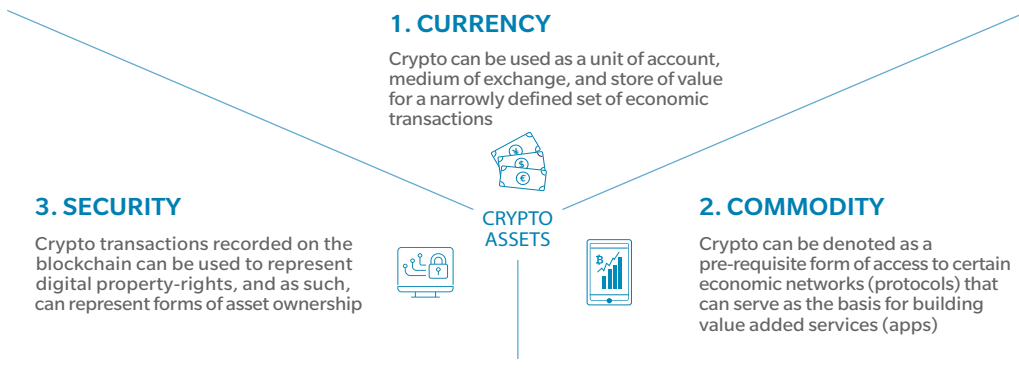


Economic exchange is mediated by digital (crypto) currencies and tokens managed through decentralized consensus

Crypto-assets do not fit neatly in any conventional asset class definition

Complicating the design of regulation and policy is the fact that different crypto-assets can exhibit features of a currency, commodity or a security. At a minimum, many crypto-assets are used to facilitate payments in an economic transaction. From there, divergences can exist depending on the purpose of the crypto-asset. Some focus on being global stores of value (like Bitcoin); others are digital commodities (raw inputs) required for building decentralized applications (like Ether). There is also an entire class of crypto-assets aimed at broadly representing claims on an issuer or digitizing property rights onto the blockchain, making any good or service “tradeable”(Exhibit 3).

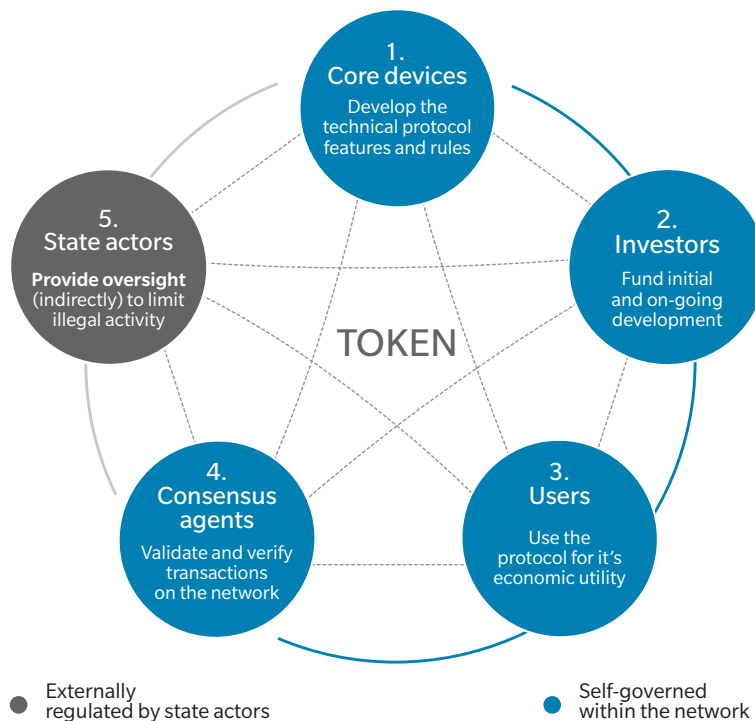
Exhibit 3: Characterizing crypto-assets



Decision-making relies on a decentralized network of actors

Governance of many crypto economic systems are more decentralized than conventional trust-based intermediary systems. This means that there is rarely a “single entry point” to engage with a network to influence or change outcomes. Crypto-economic systems rely on decentralized consensus – which means that decisions are not made by any central authority, but rather by a network of stakeholders based on different mechanisms for achieving consensus. Influencing behaviors and the direction of a crypto system requires changing the complex web of economic incentives and norms inherent in these systems (Exhibit 4).

Exhibit 4: Governance web of crypto-economic networks



There are multiple different governance models for decision-making

There is active and ongoing innovation in how the network of stakeholders in a crypto-economic system come together to make decisions, and no single model has emerged as the best or only way to ensure alignment with user and investor interests.

Crypto-assets rely on consensus on multiple levels to avoid the need for a trusted third party. A consensus mechanism (or “protocol”) is a distributed algorithm for a group of consensus agents (also called “miners”) that will ensure that all miners agree on the same state of the blockchain. Consensus mechanisms are implemented by rewarding miners for validating and verifying transaction networks, which they do via Proof-of-Work or Proof-of-Stake mechanisms. However, consensus is a factor not only at the protocol level, but also at a governance level. Developers may identify a way to make the protocol more efficient or fix a bug, but the improvement will only go into effect if consensus agents adopt and implement the change. Each crypto-asset has its own governance model for how developers, consensus agents, investors and users come together to agree on what changes are made, as well as how and when these changes are implemented.

There are multiple approaches to governance, some are fully decentralized while others depend on a higher level of centralization. Governance is said to be “on-chain” when the mechanisms for changing the protocol are based on rules and voting mechanisms embedded in the protocol itself. This is the approach adopted, for example, by Tezos. On the other hand, many crypto-assets, including Bitcoin and Ether, have “off-chain” governance, which may involve the addition of new stakeholders and influencers in the governance process. For example, the Ethereum Foundation helps convene meetings between stakeholders to reach agreement.

Decentralized decision-making creates new opportunities and challenges for dealing with risks

Consensus-driven governance models mean the crypto-asset can evolve in any way stakeholders choose to. This offers new ways of dealing with risks and potentially helping achieve policy goals. For example, if there is a hack or illegal activity is identified, the community can collectively decide to alter the transaction history and reverse the damage.

However, these models also create new risks and challenges. The distributed nature of decision-making makes it hard to define who is responsible for any harm that occurs. For example, should developers be made liable in case protocol vulnerabilities are exploited in a hack or should consensus agents be held liable if they do not implement a change that remedies a vulnerability? If there is lack of consensus on changes to the protocol, a fork may occur, creating two separate versions of the crypto-asset. Proponents of each side of the debate may then continue to develop these versions separately, but given the importance and value of network effects, communities may ask policy makers for additional mechanisms for resolving disputes.

Regulations will need to be put in place

If crypto-assets are indeed here to stay, governments need to determine how best to regulate them and to govern their connections with the conventional financial system.

Policies would be needed regarding:

- Anti-Money Laundering, Know Your Customer regulation and Combating the Financing of Terrorism
- Investor protection
- Consumer protection
- Stability of individual financial institutions
- Stability of the financial system
- Taxation

Please see “Cryptocurrencies and Public Policy: Key Questions and Answers” for a longer explanation of the potential regulatory options in these areas.

Several overarching issues will determine the nature and success of regulatory approaches.

Regulation by activity will generally work better than by broad category

Some countries have written, or are thinking of writing, rules specifically for crypto-assets as a category. However, the wider trend is to regulate crypto-asset activities in the same way as fundamentally similar financial activities that already exist – especially for activities that exist at the intersection of the financial and crypto economy. For example, nations are beginning to require digital wallets and crypto-asset exchanges to follow broadly the same “Know Your Customer” and Anti-money laundering rules as apply to other financial institutions.

This generally appears to us to be the superior approach, both for consistency and because technological changes and business innovations may shift products and services into or out of the coverage of definitions of crypto-assets employed by regulators and policymakers. Some of this shifting is likely to be deliberate regulatory arbitrage while other shifts will be triggered by other business considerations.

In addition, regulatory objectives differ depending on the purpose and nature of the asset being regulated. Given the differences in crypto-assets, this naturally leads to varying regulatory objectives and approaches.

However, some new regulatory frameworks may be required to ensure stakeholder protections

Looking at a historical analogy, the creation of publicly traded firms as a concept is what ultimately led to securities regulation. A public firm’s decisions are made by management, with oversight by a board of directors, creating a framework for duties and responsibilities

to consumers and investors. In the case of crypto-assets, decentralization means there are a multitude of stakeholders with co-responsibility for decisions, which may ultimately require a new regulatory framework to ensure user and investor protections, as well as the protection of new types of stakeholders (developers and consensus agents).

Global standards are needed

Crypto-assets are inherently global in nature, especially given their electronic nature and their strong attempts to preserve anonymity. Although regulation and tax policy are always likely to remain at the national level, there is a clear need for standards that would apply across the globe or at least in the major economies. Crypto-asset transactions can flow easily away from jurisdictions that punish them towards ones that favor them. Even if jurisdictions choose overall approaches that are equally favorable on average, differences in the specifics could lead to substantial arbitrage or other unintended consequences. Recognizing the need to jointly examine crypto-assets, G20 leaders have convened a work stream on the topic, as have other global bodies such as the Financial Stability Board and the International Organization of Securities Commissions. Considerable further work will be needed through these and other channels to achieve the necessary global coordination.

Policymakers should study and monitor network incentives to understand how crypto-powered systems will evolve

Crypto-economic networks are dynamic systems that evolve based on the design of their embedded incentives. While direct intervention and regulation may not be possible for some networks, it is nonetheless important to stay attuned to how the governance models and underlying incentives change. The complexity and power of incentives should not be taken lightly. For example, the Proof-of-Work incentive system for the Bitcoin network consisted of a 10 page paper. When released into the world, the Bitcoin network self-assembled to have a total market capitalization in the hundreds of billions of dollars, along with a globally distributed ecosystem of miners, investors, core developers and users.

Consideration must be given to how to regulate a system driven by decentralized software

As a simplification, regulation has always been about controlling the actions of people, whereas the automatic and decentralized nature of crypto-assets can make it hard to point to a single responsible party to regulate. It will clearly be possible to regulate the interfaces between the crypto-economy and the wider conventional economy, such as applying Anti-Money Laundering regulations to digital wallets and crypto-exchanges. However, actions that take place entirely within the crypto-economy will represent a tougher challenge, especially when apparently driven by the automatic application of computer code. That said, there are some similar challenges in the regulation of algorithmic trading, for example, so this is not unique to the crypto-economy.

How will stronger regulation change user demand for crypto-assets?

Crypto-assets are currently relatively lightly regulated and not all of this regulation has been effectively applied to date, so it is reasonable to wonder whether the crypto-economy can survive extensive regulation and what changes in user demand or market structure would occur. User demand is best considered category by category.

Libertarians and techno-anarchists

The desire to avoid governmental control makes this user group somewhat allergic to increased regulation, although improved market integrity and safety would be valuable to them as well. (No user group likes fraud and price manipulation.) Taken as a whole, such regulation is unlikely to drive away a large portion of this user group. Most importantly, regulation is unlikely to affect the rules governing the “money supply” of a crypto-asset, such as Bitcoin’s rules on how often a new Bitcoin is created. Taking the money supply out of government control is perhaps the single largest driver of the ideological support by this user group for crypto-assets. That said, the current feeling that crypto-assets are almost entirely untouched by governments would lessen as new regulations come in and with it the close affinity of this user group to crypto-assets.

People who deeply distrust their government’s economic management

Similarly, as long as regulation did not touch the “money supply” of crypto-assets, most of this user group is likely to remain loyal. However, increased regulation will raise the perceived risk that expropriation or capital controls could be put into place effectively. This factor would reduce the safe haven value for this user group, so one would expect some reduction in demand.

Seekers of anonymity

This is the group that might show the strongest drop in actual demand compared to its potential as a result of greater regulation. Seekers of anonymity generally are looking for anonymity from the government, so government-imposed regulations that make it easier to track their transactions would be highly disliked. However, one must bear in mind that there are extensive regulations on transactions in US dollars or Euros and yet these remain the favorite transactional instrument for criminals and many others who highly value anonymity. One would certainly expect that new crypto-assets and new techniques would be developed in an attempt to reduce the effectiveness of regulations intended to pierce the veil of anonymity. This will be perceived as less necessary to some in this user group if governments appropriately implement a reduction of anonymity with some continuing privacy protections.

Technical users

Regulation could provide a significant impetus towards new technical uses, including in the payments space, by providing greater clarity on governance of crypto-assets and paving the way for greater interconnections with the larger financial system. In addition, of course, they would benefit from improved market integrity.

Investors and speculators

New regulation could sharply increase the demand from investors, particularly institutional investors. There is known to be very considerable interest in moving into this sector, on at least an experimental basis, once the normal infrastructure of financial markets is developed, especially sound custody arrangements for holding the crypto-assets. That infrastructure will not develop without solid, effective regulation.

Although it is always hard to predict the future, it appears that most crypto-asset advocates believe that stronger regulation will actually increase the total market size of crypto-assets, rather than causing users to flee. At the same time, it seems likely that stronger regulation will help force the industry shake-out that will eventually occur anyway. It is improbable that the world needs nearly as many crypto-assets for general purposes, as opposed to specific technical uses, as exists today.

CONCLUSIONS

Crypto-assets appear to be here for the long run, barring a catastrophic loss of trust from their users, which means that regulation needs to be developed to protect stakeholders and the larger financial system from various risks. This regulation should be shaped by an understanding of the nature of the cryptoeconomy and of the user groups within it. Hopefully this paper will serve as a useful contribution to this wider and longer conversation, which is still in its early stages.

ABOUT THE AUTHORS

Douglas J. Elliott

Partner in the Finance & Risk and Public Policy and Corporate & Institutional Banking Practices

Phone: +1 646 364 8444

Email: douglas.elliott@oliverwyman.com

Larissa De Lima

Engagement Manager in the Corporate & Institutional Banking Practice

Email: larissa.delima@oliverwyman.com

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS

+1 212 541 8100

EMEA

+44 20 7333 8333

ASIA PACIFIC

+65 6510 9700

www.oliverwyman.com

Copyright © 2018 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.