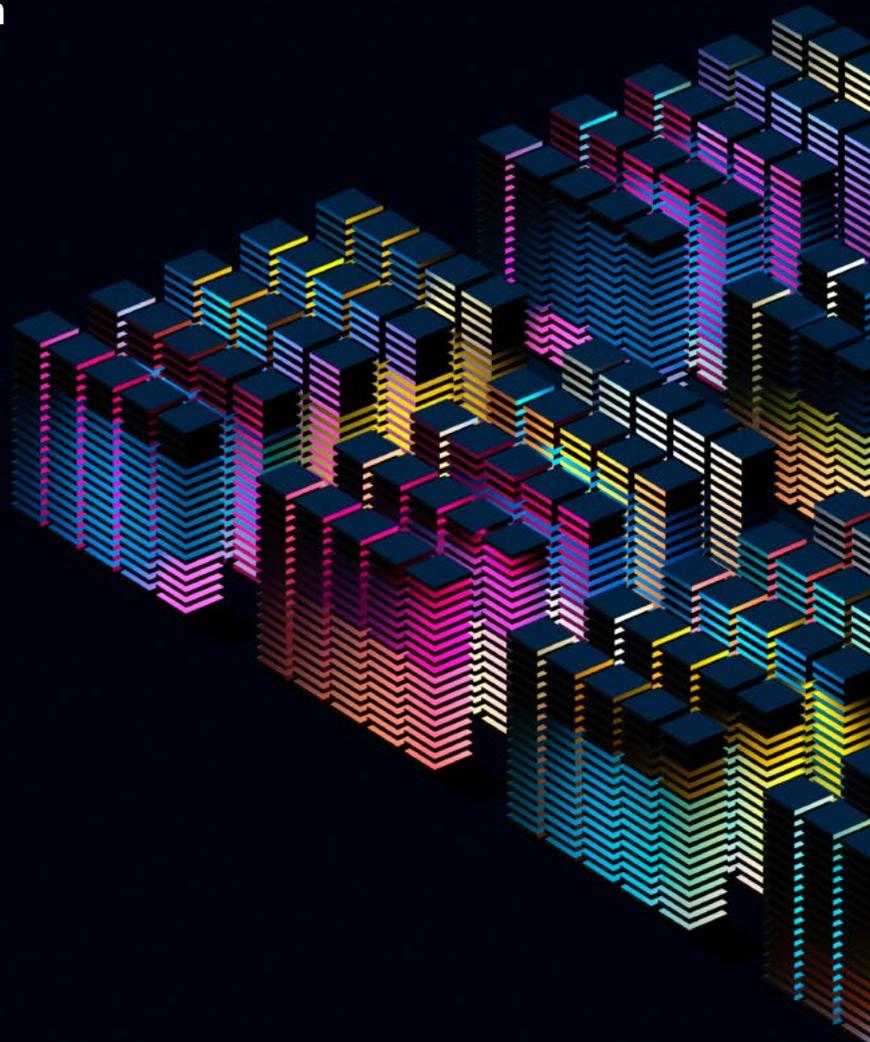




Investing in Virtual Assets

**How Virtual Assets
and associated Service
Providers have become
ready for institutional
investment and growth**



March 2021

[KPMG.com](https://www.kpmg.com)

Foreword

For a number of years, the Virtual Assets industry has been buzzing with potential. However, to move from operating ‘on the fringes’ to being ‘fully endorsed by institutional investors’ with a chance to sustain significant growth, the sector must continue to drive optimal operational excellence to be in line or similar to with Financial Services (FS) industry standards.

By virtual assets, we are referring to “a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes”¹ Examples are cryptocurrency or asset-backed tokens. Since our last deep-dive report in 2018, many Virtual Assets Service Providers (VASPs), such as virtual asset exchanges and virtual assets custodians, have leapt forward on their path to institutionalization.

The industry has demonstrated great innovation in creating new products and new asset classes, and exciting players have appeared – blissfully unburdened by legacy processes and infrastructure. Thanks to these moves, there has also been an uptick in interest and focus from regulators and institutional investors towards the industry.

The next step for VASPs, if they want to pursue and sustain growth, is to incentivize the FS industry to engage more closely, and to deliver what business-to-business (B2B) customers need and want. This requires VASPs to have operations that are streamlined, scalable and compliant – and all without losing speed and agility.

KPMG has identified four pillars that will support VASPs in this process, outlined in the table below.



Customer

Evolving B2B Customer Engagement – digital first institutional services



Compliance

KYC best practice and onboarding
AML and CTF



Operations

Clearing and settlement
Custody and asset management



Governance

Risk management and operational controls

In this report, we share our insights into how VASPs can drive these areas to accelerate institutionalization. We finish by looking ahead to what we might see next from this dynamic industry – including how established FS organizations are in fact creating their own virtual asset offers.

The KPMG team involved in this report spans four continents. We were kindly supported by contributions from organizations and individuals working in the Virtual Assets industry, financial services, government and industry associations. We are grateful for their time and insights.



Laszlo Peter
Head of
Blockchain
Services,
Asia Pacific

1 <https://www.fatf-gafi.org/glossary/u-z/>

Contents

1	Executive Summary	1
2	Evolving Customer Engagement: digital first institutional services	2
3	Reliable Regulatory Compliance: KYC best practice and onboarding	4
4	Reliable Regulatory Compliance: AML and CTF	6
5	Scaled and Stable Operations: clearing and settlement	8
6	Scaled and Stable Operations: custody and asset safekeeping	10
7	Robust Governance: risk management and operational controls	13
8	Closing Outlook	15
9	About KPMG	16
10	Abbreviations	17

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Authors and Contributors

KPMG Australia

Laszlo Peter, Head of Blockchain Services, Asia Pacific

Max Soyref, Associate Director, Blockchain Services

Peter Xing, Associate Director, Technology, Markets & Growth

Joshua Maloon, Consultant, Technology, Markets & Growth

Kim Quinones, Consultant, Technology, Markets & Growth

KPMG China

James O'Callaghan, Partner, Regulatory Technology Advisory

Benjamin Usinger, Associate Director, Crypto Advisory Services Lead

James Harte, Director, Financial Services Strategy

KPMG Switzerland

André Guedel, Head of International Headquarters

KPMG in Cayman Islands

Andrew Schofield, Partner, Head of Digital Assets

Gautam Ganeshan, Director, Digital Assets

Jonathan Sy, Director, Audit, Asset Management

KPMG Japan

Masatake Toyota, Director, Lighthouse of KPMG Ignition Tokyo

KPMG in Malta

Juanita Brockdorff, Partner, Tax Services

Christopher Azzopardi, Director, IT Assurance

Mark Curmi, Director, Banking, Financial Institutions and VFA Advisory Services

Matthew Scerri, Associate Director, Digital Solutions

Trudy Muscat, Senior Manager, Tax Services

Quotes, Interviews and Client Contributors

Australian Federal Government

Chloe White, National Blockchain Roadmap Lead, Digital Economy and Technology Division, Department of Industry, Science, Energy and Resources

BC Technologies Group

Hugh Madden, Chief Executive Officer

Usman Ahmad, Chief Information Officer

Nathan Simmons, Chief Compliance Officer

Blockchain Australia

Steve Vallas, Chief Executive Officer

Independent Reserve

Adrian Przelozny, Chief Executive Officer

Duncan Tebb, Chief Operating Officer

National Australian Bank

Lisa Wade, Director, Digital, Innovation and Sustainability

OSL

Wayne Trench, Chief Executive Officer

Matt Long, Head of Distribution and Prime

Volt Bank

Alexander Maron, Head of Operational Risk

100x Group

Vivien Khoo, Chief Operating Officer

Ben Radclyffe, Commercial Director



BC TECHNOLOGY GROUP LIMITED
BC 科技集團有限公司



ASIA'S LEADING
DIGITAL ASSET
PLATFORM



1 Executive Summary

Virtual Asset Service Providers (VASPs) are continuing to disrupt and mature, and are eyeing opportunities to scale up and institutionalize within the Financial Services (FS) landscape, as this is where the real potential lies for growth.

Regulatory bodies are now taking the industry seriously, while institutional investors are shifting from keeping a watchful eye, to actively engaging with the most professional players. In fact, some established FS institutions are taking things a step further, and are preparing their own virtual assets service offerings.

This KPMG report considers the recent evolution of the industry, and looks ahead to the operational changes that VASPs need to implement to succeed at institutionalization. Success will be dependent on VASPs achieving superior customer engagement, regulatory compliance, scalable and stable operations, and robust governance.

By delivering an optimal customer engagement experience, VASPs can streamline participation for institutional players. Drawing on evolving regulations, they can increase security through strict customer onboarding and Know Your Customer (KYC) programs, while through Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) practices, they can build trust.

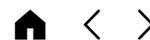
Reliable policies and procedures will help prepare VASPs to scale and meet the expectations of large institutions. Embracing automation technology for ongoing monitoring, review and improvement will provide assurance to regulators, who are evolving their risk appetite in each jurisdiction.

As the industry and its ecosystem grows, custody and safekeeping services will emerge as a prerequisite of institutional investment. VASPs need to offer secure custody solutions of their own, or ensure application programming interface (API) integrations are in place for seamless connectivity to third party custody providers.

Finally, strong governance and risk management must start at the top with experienced leadership, supported by governance bodies and sophisticated risk management frameworks across customers, vendors and internal staff.

If VASPs surge ahead in these areas, we see significant potential for them to deliver to institutional demand, and forge long lasting value propositions.

Whether a 'native VASP', or a traditional FS organisation moving into the space, collaboration is the key to success. Rather than a 'build it yourself' approach, the best results will come from a strong and scalable ecosystem, together shaping and seizing the opportunities in this fast-growing market.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

2 Evolving Customer Engagement: digital first institutional services

For VASPs to institutionalize, they have to put optimal B2B customer engagement at the center of every move – across every area in the below chart:

Client Facing Functions

		
Engagement Channels	Engagement Management	Sales and Operations
Online	Relationship Management	Marketing Sales
Mobile	Information Management	Customer On-Boarding
Assisted	Segment Management	Customer Analytics

At a channel level, practical online interfaces, structured onboarding experiences, and strict security features should be standard.

The next step is engagement management, and in particular, meeting the more specific needs of institutional investors and money managers. This group needs assurance that VASPs have adequate risk management, governance, expert analysis, audit trails, and technical execution. They also want the right level of support to orchestrate and execute on their investment decisions. Ben Radclyffe, Commercial Director, 100x Group, says this could be in the form of a 'middle layer of expertise', akin to the role of a broker in FS.

Finally, in the sales and operations space, VASPs can exploit state-of-the-art data analytics to support their workforce in making insightful decisions.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations



Some other ways to drive an optimal B2B customer experience include:

Streamlining large orders: Institutional investors often face challenges in placing large orders, especially in markets with lower liquidity. Orders have to be broken down and split over multiple exchanges, which is a difficult process. This is where over the counter (OTC) desks and liquidity providers can help, as they can source and pool virtual assets to fulfil larger block orders in a more personalized way. There is an opportunity for OTC and liquidity related service offerings to be developed as part of a broader ecosystem, to ensure long-term growth and sector stability.

APIs when scaling: As VASPs scale in size, they need to standardize processes, and this is where a robust API-based (application programming interface) infrastructure can be beneficial. APIs allow access to value-adding software, opening up additional capabilities while keeping the customer experience streamlined. For example, traditional FS providers have entire teams dedicated to, or have outsourced, the confirmation process (validating transactions), given the large volumes of requests and monitoring effort needed. As VASPs face a larger demand for confirmation services, a good solution may be to apply a read-only API, where an exchange user can provide the API key to an auditor, who can then request and review the data.

Communicating insights: A key part of growth is communicating with customers and taking them on the journey, and VASPs are getting more sophisticated in their approaches. VASPs are sharing expert insights, research and thought leadership via their websites and social media channels. Several players (e.g. Binance Research and Huobi Research) have started sharing in-depth analysis of virtual asset research projects, enabling people to follow and understand progress. In line with this, it is interesting to observe a shift in how traditional finance media is reporting on the industry, with publications such as Bloomberg and Forbes increasingly covering Virtual Assets industry developments and market prices.

Institutional competitors

Chloe White, National Blockchain Roadmap Lead for the Digital Economy and Technology Division at the Australian Federal Government Department of Industry, Science, Energy and Resources, says there is both innovation and competition on the horizon for VASPs.

“Early signs suggest that global financial services firms are becoming more open-minded to building crypto-asset functionality into their platforms, preparing to potentially encroach on the market share of digital currency exchanges. In the future, we can expect to see digital currency exchanges continue to innovate and broaden their business models in response. Their agility and greater appetite for risk will allow them to remain at the forefront of crypto-asset experimentation for some time, but they will also need to expand their customer base, including targeting businesses and institutions, to remain competitive in a world where large global corporations are exploring creating digital wallets and issuing tokens at scale.”



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

3 Reliable Regulatory Compliance: KYC best practice and onboarding

In recent years, maturity of regulation has brought a number of advantages to the Virtual Assets industry. For example, two significant supra-regulatory bodies, the International Organization of Securities Commissions (IOSCO), and the Financial Action Task Force (FATF), have assisted regulatory authorities with evaluating how virtual assets work with regulatory frameworks around the world. As a result, we have seen many relevant FS jurisdictions issuing considerations, rules or conditions for VASPs.² This helps to bring legitimacy to the sector in the eyes of institutional investors.

Hugh Madden, Chief Executive Officer, BC Technology Group, the HKEX-listed parent company of digital asset firm OSL, says:

“A strong compliance program is mandatory for licensing, and provides a clear advantage over unregulated competitors when addressing the professional and institutional client segment.”

Customer due diligence

Most regulations and licensing regimes focus on robust customer due diligence and monitoring programs for the purposes of Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) compliance.

A key part of this is having a robust Know Your Customer (KYC) program, and in recent years, many VASPs have adopted some elements of a KYC program and practice. This uptake increased after global regulators clarified their expectations for ‘*risk-based customer due diligence*’ in the June 2019 declaration from the FATF.

Risk based customer due diligence and KYC programs are often executed as a set of policies and processes that aim to set boundaries around the type of customers an organization will and will not accept. Historically, many VASPs have met minimum KYC standards by establishing basic customer data collection practices, or integrating third-party solutions to support identity collection and verification (ID&V). This approach is influenced by the retail heritage of many VASPs.

² <https://www.forbes.com/sites/sarahhansen/2018/06/20/forbes-guide-to-cryptocurrency-exchanges/#4d447e025722>

³ <http://www.gov.ky/portal/pls/portal/docs/1/12964483.PDF>



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

However, when catering for institutional investors, a KYC program can only be a first step towards a risk-based Customer Acceptance Policy. ID&V procedures must be matched by a set of screenings and checks that result in a graduated level of due diligence and risk management. These checks may include Politically Exposed Person (PEP) screenings and suitability assessments to assess the fit of an investor with the products offered.

This process can be complex for corporate and institutional clients, and is no different to the onboarding at traditional FS organizations. It requires up-to-date documentation for the organization and all parties engaging with the service.

Institutional onboarding

A good practice for institutional onboarding is an online-based process guided by a relationship manager, to deliver outstanding customer service in the first touchpoints. The goal is to provide a frictionless user experience and avoid recreating the same process every time a customer signs up. This is especially helpful for customers from larger institutions that may have multiple accounts for different products with one service provider. Part of this needs to be a risk-level driven feature, which allows customers to do certain things with a (reduced) level of KYC. To access higher-risk functionality or more complex products, the system will ask for additional information.

Ongoing monitoring

Some organizations are adopting highly detailed customer risk profiles, such as profiles broken down into peer groups for a more granular risk scoring of customers. This grading takes into consideration the customer's activity and trading patterns, as well as relationships between master and sub-accounts, for example.

VASPs that apply this practice have been able to further automate their checks, calibrate alert thresholds, and improve the customer onboarding and due diligence process.

Ultimately, this level of customer due diligence should not be triggered upon onboarding only. A well-established regime will feature ongoing monitoring, review and adjustment at key trigger points in the customer lifecycle.

Policy first, process second

Technology is an important component of an effective KYC program and the safe onboarding of new customers. However, it is prudent to adopt a 'policy and procedure first' approach, then apply processes, as the FATF's KYC requirements may differ from jurisdiction to jurisdiction. Therefore, policies and procedures that consider diversity of jurisdictional needs, and adjust to local requirements for data collection are key.

How Volt Bank is 'knowing its customers'

Neo-banks (digital-only banks) are playing an important role when it comes to the immersion of new and emerging financial products into everyday banking. However, they are also a high target for fraud and cybercrime – and therefore offer good lessons to VASPs looking to increase security.

For example, Australian neo-bank Volt Bank is continually bolstering its KYC program and security protocols to protect against undesirable customers and activity.

Alexander Maron, Head of Operational Risk, Volt Bank, says,

"Volt is focusing on balancing a frictionless onboarding experience with robust KYC protocols. Open Banking is also expanding opportunities for verification procedures, allowing FS providers to improve their customer risk ratings. Australia's new Open Banking system is strengthening information sharing, with the ability to rapidly pull customer information from multiple sources via third-party providers."



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

4 Reliable Regulatory Compliance: AML and CTF

In the 10 years since inception, virtual assets have often been associated with the risk of illegitimate transactions and the shadow economy. While a majority of virtual asset holders acquire and use the assets for legitimate reasons, this association been hard to shake.

This perception is why many regulatory bodies, including the FATF, have been attempting to introduce greater AML and CTF scrutiny to the sector.

The FATF's guidance and requirements for VASPs to address AML and CTF risks are on par with those by the Society for Worldwide Interbank Financial Telecommunication – which most people know as a 'SWIFT code' and enables seamless payment between international banks. This means VASP standards should equal other regulated FS institutions. However, AML/CTF is often looked at as just another third-party system to be integrated, rather than a foundation for organizational strategy on tackling money laundering and terrorism financing risks. To overcome this, a good practice we have observed is to conduct a combined 'customer and product risk assessment', defining the likelihood and impact of AML/CTF risks based on the target customer segment and products offered.

In-house accountability

All regulatory policies and procedures must be supported by clear accountability within each organization. It is therefore positive to see that significant investment and recruitment is happening at VASPs related to compliance. We are now seeing many compliance and governance functions headed by senior officers with long-term experience in areas such as AML/CTF programs in traditional FS institutions.

Under this leadership, all staff members should be part of a regular training regime to ensure a clear understanding of AML/CTF requirements. Ongoing review and audits should be implemented to ensure key risks are identified and mitigated, and compliance remains intact.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

Monitoring tools

Once policies and leadership are defined, supporting technology can be tailored to help address customer and product risks. Many VASPs have implemented third party transaction monitoring and alert solutions that have been designed specifically for the industry.

Duncan Tebb, Chief Operating Officer, Independent Reserve, says:

“We have implemented new and very strict processes for ongoing improvements in our AML and KYC capabilities. Not surprisingly, there are still gaps in the data we capture from third party vendor solutions and we are using a number of vendor integrations as well as new, in-house built solutions, to strengthen our procedures and reduce various AML/CTF related risk vectors.”

At KPMG, we have observed the same challenge with third party AML/CTF services. While some virtual asset specific risks, such as high-risk wallets or high-risk transactions, can be analyzed and flagged through these services, some unusual customer behaviors are not picked up. Therefore, VASPs should implement an effective monitoring system that connects with necessary third-party monitoring systems for a more holistic approach.

The Travel Rule

Another area for a strong AML/CTF approach is to follow the FATF’s Recommendation 16, also known as the Travel Rule, requesting that the originators and beneficiaries of all transfers of virtual assets must exchange identifying information such as their name, account number, and address.⁴ This rule must be complied with by all licensed and regulated VASPs in any of the 38+ FATF member jurisdictions.

However, the rule also poses challenges. This is because VASPs have not yet had a widely accepted industry service like SWIFT that has mandatory data fields to ensure compliance with the rule, while protecting client and business relationship information.

Therefore, the industry has established several cooperative efforts, including the now broadly accepted IVMS101 (inter-VASP messaging) to streamline data collection across different jurisdictional requirements. In addition, VASP’s and traditional FS institutions are collaborating to build messaging solutions such as the Travel Rule Protocol.⁵ No single solution will suffice, and therefore, there is a need for interoperability and multi-party service integration.

From a customer perspective, we expect to see significant impacts to the onboarding and deposit and withdrawal experience, because additional information and documentation could be required with each transaction.

Accurate reporting

As regulations for digital assets evolve, users of virtual assets exchanges need to be able to obtain accurate reporting of their digital asset holdings and activities for their respective jurisdictions (e.g. for tax reporting, which can be done with the help of KPMG Crypto Tax Estimator). VASPs need to be able to provide their customers with data such as the original cost basis of an asset, sales proceeds, realized gains/losses, and deposits and withdrawals. In certain jurisdictions, exchanges may be required to provide this information directly to the relevant tax authority.

Overall, it is clear that there are some substantial regulatory compliance challenges for VASPs, however, investment in compliance, and particularly in AML/CTF programs, will be a significant competitive differentiator. Getting this right should be an attractive drawcard for institutional investors.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

⁴ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>

⁵ <https://www.travelruleprotocol.org/>

5 Scaled and Stable Operations: clearing and settlement

Following customer engagement and regulatory compliance, scaled and stable operations are vital on the path to institutionalization. A fundamental focus must be on clearing and settlement, which are among the most critical day-to-day operations for VASPs.

Virtual assets have brought a significant simplification to the processes of clearing and settlement, thanks to the nature of the underlying distributed ledger design used, commonly known as blockchain. The distributed ledger design offers immutability, irrefutable ownership, removal of novation of transactions, and instant data reconciliation. These factors have redesigned the way assets can be transacted and invested in. For example, unlike traditional payment or investment activities, virtual asset trading and settlement happen in near real-time and almost simultaneously. This helps to eliminate the counterparty-risk associated with middlemen and boosts liquidity through reducing settlement times.

Settlement types

There are two common types of settlement involving virtual assets: payment or exchange of virtual asset to virtual asset; and payment or exchange of virtual asset to fiat (and vice versa).

1 Payment or exchange of virtual asset to virtual asset

Virtual asset exchanges are centralized platforms that connect buyers and sellers of a virtual asset. They automate the matching and execution of trades. Usman Ahmad, Chief Information Officer, BC Technologies Group, explains that on the exchanges, trades are matched and confirmed instantly through an account movement within the exchange platform. This is a non-public record, and the appropriate funds are reflected in the client's account. When a client deposits or withdraws those assets (either through the exchange or through a designated custodian), the aligned blockchain ledger, such as Bitcoin chain or Ethereum chain, is updated with a public record. This instant settlement helps to eliminate risks such as counterparty, market, settlement, and credit risk, but shifts the degree of trust clients must place to the exchange and its operations.

However, new risks also arise. For example, the failure of the exchange to secure the traded assets, the inability to pre-fund trades, or the inability to move assets fast enough from a secure offline wallet to a liquid online wallet for settlement on the blockchain ledger. Therefore, thorough due diligence on the exchanges that investors use is critical.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

Decentralized Finance (DeFi) for clearing and settlement

For years, decentralized finance (DeFi) products were used to reduce the need to rely on a centralized clearing and settlement service. However, these platforms struggled with regulating their activity, high transaction fees, lower liquidity, and a slower speed of execution. Centralized exchanges stepped up in prominence, however, 2020 has seen a significant return of volumes in decentralized exchanges. That said, we expect that increased regulatory scrutiny will drive growth of fully centralized exchanges, while decentralized exchanges may co-exist in a regulatory ‘grey zone’. Still, the rapid speed of innovation in DeFi means that services may arise that are suitable to the relevant regulatory compliance.

2 Payment or exchange of virtual asset to fiat (and vice versa)

Virtual asset to virtual asset clearing and settlement are executed by the VASP platforms and blockchain technology without further intermediaries. However, for most investors, the starting point to virtual assets is using traditional fiat money – a step referred to as ‘on-ramping’. Commonly, virtual asset exchanges are the bridge between fiat systems and virtual assets – also referred to as ‘clearing funds’. On the other side are traditional FS institutions such as banks or traditional payment providers which provide the ‘funds movement’ infrastructure.

A challenge for VASPs is that many global banks are not yet fully servicing VASPs, so often they can only open bank accounts with virtual or ‘challenger’ banks.

Adrian Przelozny, Chief Executive Officer, Independent Reserve, says:

“It is for this reason that many virtual asset exchanges are looking elsewhere for financial services support. Examples of where liquidity support may come from includes alternative finance options such as asset or cash-backed tokens, whereby direct transfer of ownership will be limited and provide much needed assurances.”

We expect that opportunities will emerge as both traditional and challenger banks realize the potential of servicing participants in the Virtual Asset industry. For example, in the US, JP Morgan has started on-ramping with virtual assets Coinbase and Gemini.⁶

Stablecoin tokens

Due to the early challenges with transactions between virtual assets and fiat currencies, ‘stablecoins’ have emerged. Stablecoins are virtual assets with the promise of a fixed exchange rate (usually in fiat currencies), and are underwritten by collateral that is held by the stablecoin creator or ‘minter’. Collateralization is conducted via normal banking transactions, alongside the respective minting or destruction of the equivalent value in stablecoins.

Stablecoins open up opportunities for both VASPs and banks, enabling a fully regulated and audited deposit taking institution (DTI) to act as an independent custodian of the traditional assets. The ‘minter’ of a stablecoin has to hold the equivalent collateral with a DTI. Some banks are entering this space, for example with JP Morgan offering its JPM Coin as a USD-collateralized stablecoin.

In future, as VASPs and traditional FS institutions move into each other’s space, regulators could apply the same standards and frameworks across traditional and virtual assets. This would make collaboration easier, and smooth the fiat-to-virtual asset settlement friction observed today.

Lisa Wade, Director, Digital, Innovation and Sustainability, National Australia Bank, says that working with VASPs is a great collaboration opportunity.

“Banks like NAB will continue to exist because they have established their operations through credible risk management, rigorous approach and structures to finance, regulation and compliance. By blending the infrastructures that VASPs are developing with the established foundations banks have set, together, banks and VASPs will pave the way in building the future ecosystem of finance.”



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

⁶ <https://www.wsj.com/amp/articles/jpmorgan-extends-banking-services-to-bitcoin-exchanges-11589281201>

6 Scaled and Stable Operations: custody and asset safekeeping

The term ‘custody’ in the context of virtual assets refers to the management and safekeeping of the cryptographic private keys that virtual asset owners use to execute virtual asset transactions. Whoever controls these private keys can sign transactions and change the amount of assets owned in near real-time – effectively controlling the asset.

Therefore, custody plays a very important role on the path to institutionalization, with VASPs needing to offer their own custody approach, or engage with secure custody providers.

Usman Ahmad from BC Technologies Group says:

“The evolution of the custodian model in virtual assets is still developing, and there is a need for more independent, trusted parties to hold assets outside of a trading venue. Recently, more trusted custodians have emerged in the market to meet this need – a key indicator of ongoing wide-scale institutional adoption of the asset class.”

Challenges for custody providers

Custody providers for virtual assets face a number of challenges, and are working in different ways to overcome them. For example, every participant in the virtual asset market needs a way to safely store and move their assets. In traditional FS, participants often rely on third parties to store and move assets safely. Yet, virtual assets are different in two ways:

- 1 Direct access:** Virtual assets were designed to provide owners with full control over them, without the need for centralized middlemen that record ownership or transactions.
- 2 Ownership and bookkeeping:** Virtual assets exist and are recorded only in the virtual space without a local register of ownership. This means whoever has control over the asset, specifically the private key, has ownership by design. It requires local contract law to record changes to this arrangement, i.e. between a custodian and the asset owner.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

As a consequence of these differences, three solutions have emerged:

- 1 Self-custody solutions:** These leverage direct access to the asset (referenced as ‘access to the private key’), through either software and hardware to store the assets. Solutions are differentiated between ‘hot’ and ‘cold’ storage, whereby hot indicates that the ‘wallet’ has direct access to the internet, and cold indicates ‘air-gapped’ computers, without internet access and often kept in a protected location. Examples of self-custody are Hardware Security Modules (HSM) in a data center, to simple USB stick or mobile wallets with pre-configured software.
- 2 Exchange-hosted wallets:** Some exchanges offer ‘hosted wallets’, which are commonly used for asset storage by retail investors and traders. Exchanges took on this role to smooth out trading activities, and over time have strengthened their service and safety. The retail investor does not have an actual wallet, and does not have access to private keys, like in the case of self-custody solutions.
- 3 Independent full-service custodians:** These service virtual asset exchanges and institutional investors that want to safely keep a large amount of assets and operate across multiple jurisdictions. They store the assets both hot and cold, and may also offer regulatory compliance services and tax reporting.

Asset safekeeping

To prepare for large-scale adoption, VASPs will need to increase the maturity of asset safekeeping. It is important to have more than ‘cold storage’. Instead, a combination of secure vaulting and cryptographic hardware with a governance model, robust terms of service, independent reviews (audit), and value-added services that create multiple layers of security are needed.

This will help:

- Protect the asset against hacking and other cyber security risks
- Prevent physical access or stealing of the vault or wallet hardware
- Back-up the asset as safe as the originals
- Prevent single points of failure by a clear separation of duties
- Offer insurance in case the asset is being compromised
- Manage liquidity and 24-hour access to the asset if needed
- Continuous compliance with local and global regulations

Adrian Przelozny from Independent Reserve, says:

“In an industry where asset safekeeping is of ultimate importance and any breach can completely destroy a business like a crypto exchange, organizations would invest significant effort and capability to not only develop, but constantly enhance their asset custody solutions.”

OSL’s approach to custody

The safe custody of assets is a hot topic for VASPs, including one of Asia’s largest, Hong Kong-based OSL, which provides virtual asset custody services to clients, along with trading and technology services.

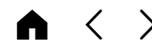
Usman Ahmad, Chief Information Officer of BC Technologies Group, OSL’s parent company, says OSL has developed a multi-level framework to protect clients’ assets, to understand attack vectors, and to mitigate threats through cyber security protocols.

Steps include putting customer deposits into a ‘frozen wallet’ which restricts withdrawals to approved internal wallets only, separation of customer assets, and a scalable ledger to reconcile customer transactions against the external blockchain. OSL has also put

in place clear segregation of duties and is being audited independently.

As threats sometimes come from unknown sources, such as sanctioned individuals that try to route transactions through OSL services, OSL has implemented a large-scale AML/CTF monitoring program for all assets in its custody.

Lastly, insurance is an important mechanism to increase consumer confidence in the safeguards and controls that have been put in place. As the insurance industry continues to mature in the Virtual Assets industry, Ahmad expects to see an evolution in insurance products and offerings that will ultimately underpin custody and asset management.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

More insights on risk

We have outlined a set of solutions on how to prevent against the physical and digital risks in virtual assets. If you are interested to know about this topic, you can read *Cracking Crypto Custody*, KPMG LLP (US) (2019).

Terms of service

VASPs need to have clear legal agreements, or 'terms of service', with custody services providers, and these must reflect the operating locations of the custody business. These terms should emphasize compliance with local regulations of factors such as KYC programs and AML, location of private key storage, and have a clear reference to the property and insolvency law that applies to assets in case of a defaulting custodian.

Insurance

Insurance is often seen as a 'holy grail' for the investor's protection; however, both the attainment of sufficient coverage and any eventual payout depend on the custodian's ability to achieve high standards of asset protection. Insurance policies are often brokered individually, for a limited period, and covering specific systems and incidents only. Due to a lack of 'vanilla policies', industry standards, regulation on custody best-practice, and generally poor historic data sets, fees of 1 percent p.a. of the amount protected are common, making insurance expensive.

Przelozny says:

"The lack of institutional-grade infrastructure and industry standards also hinders custodian services affordability, as insurers remain hesitant to participate. While certainly a challenge, we believe the development of comprehensive guidance from regulators and government agencies in the near-term will increase the attractiveness of virtual assets, driving insurers and third-party providers to expanding their service offerings to meet the needs of institutional grade retail investors."

Some custodians have been able to obtain insurance policies and offer insurance to their customers. The natural evolution would be for VASPs to likewise offer insurance to users, as this would instill confidence, and further assist institutional investors with the due diligence process.

Over time, we expect the custody choices for investors to become easier due to standardization of the industry and the emergence of certification programs. It will be helpful to have more support for institutional investors in their decision making and risk assessment in picking a custody solution that suits their needs best.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

7 Robust Governance: risk management and operational controls

The final operational pillar that supports institutionalization of the Virtual Assets industry is governance. VASPs are often fast growing, technology driven, and agile organizations. Therefore, it is critical to implement robust governance structures for sustainable operations. Strong internal governance helps with oversight and policing of internal processes and policies.

Similar to traditional FS organizations, a robust governance infrastructure should have 'three lines of defense'. A first line would be implementing management and internal controls; a second strengthening security, financial controls, risk mitigation, and inspection and compliance obligations; and a third would both internal and independent audits.

Here are some factors to consider within these areas:

Experienced leadership: VASPs must have experienced risk and compliance senior management in place, be aware of the risks to the business, and how they are to be managed.

Governance bodies: VASPs need a governance body, as well as a risk and audit committee, to help implement robust risk management, compliance, and internal control functions. This includes setting up a board and committees, defining the organization's values, and establishing a risk culture to drive and reward the right behaviors.

Third party risk mitigation: Given the digital-first nature of VASPs, they often rely on third parties to enable certain functions. This outsourcing needs to be clearly included in the governance framework and controls. This requires robust vendor management, thorough due diligence of the vendor, and regular reviews of performance.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

Information control: VASPs should consider the risks and controls around disclosure of information, especially around the handling and safekeeping of customers' assets. VASPs need to explain to their customers relevant aspects of their operations to establish trust and confidence, without introducing risk by over-disclosing operational secrets.

Relationship management: Fast and effective responses to customer enquiries are critical, as is more formalized interaction with major stakeholders and regulators.

Insider risk management: A major risk often comes from those working in, or close to the organization, and their access to privileged information. For example, hacks can involve collusion and interpersonal behavior. Therefore, it is critical that people have strongly separated duties, clear responsibilities, and the necessary competences to execute their work. Organizations should establish internal audit and whistle-blower functions. The operational team should include members with different backgrounds and areas of expertise. VASPs need to foster collaborative environments in which compliance and risk-focused roles work together.

Embracing automation

Automation technology is a significant way to help organizations effectively manage risk and operational controls as they scale. VASPs often use automation for system scans, trading balance audits, and transaction monitoring.

However, it is important to make sure the automation tools are set up to act independently and flawlessly. This requires robust specification documents, rigorous test results, and diligent Software Development Lifecycle (SDLC) governance. This also helps regulators and institutional investors to trust the processes.

Institutional investors and regulators will want assurance on the accuracy of automation controls. Professional services organizations can perform an independent assessment, in addition to the assessment performed by regulators.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

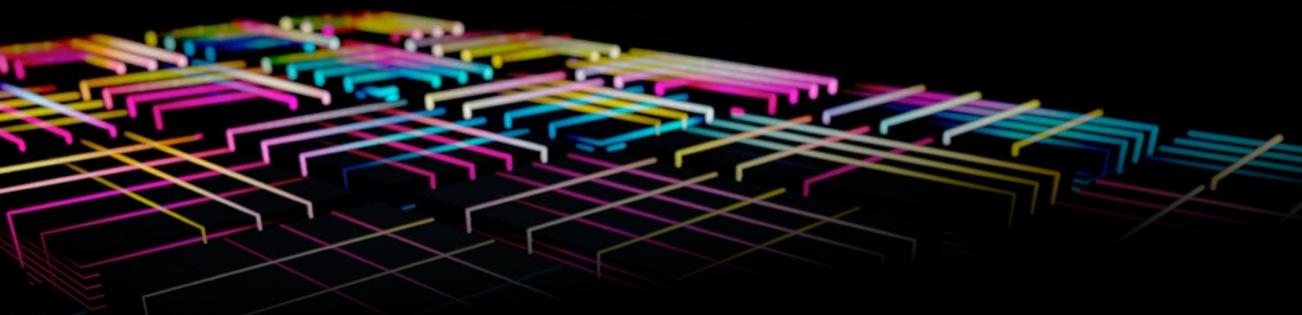
Robust Governance

Closing Outlook

About KPMG

Abbreviations

8 Closing Outlook



In March 2020, the COVID-19 pandemic led to a virtual asset ‘flash crash’. However, while traditional stocks continued to suffer severe volatility, virtual asset markets recovered within just a few weeks. This was a proof point for VASPs, as it showed their resilience to rapid market movements.

In fact, just a few months later, we saw major announcements with regards to the institutionalization of the industry with JP Morgan US announcing it will bank virtual asset exchanges Coinbase and Gemini, and the Hong Kong Securities & Futures Commission (SFC) issuing its first in principle virtual asset trading licenses to OSL. These are signs of a new era where VASPs become part of the traditional FS ecosystem.

In the next 1-2 years, we expect to see more VASPs follow the institutionalization route. New organizations will innovate with new business models and fast product development. Meanwhile, traditional FS institutions will add to the competition, setting up their own virtual asset services. An example is Standard Chartered’s venture arm, SC Ventures, which offers virtual asset custody out of Singapore. This is amplified by the news of the development of new digital currencies across many jurisdictions, particularly the Central Bank Digital Currency (CBDC) projects in various stages of maturity around the globe. In fact, some governments have also announced their plans to take part, with China’s digital Yuan a prominent example.

There are multiple other trends to watch out for – such as tokens that allow for fractional ownership of less liquid assets (i.e. real estate, carbon, IP or art), driving liquidity premiums and diversification. Other trends include additional services such as professional brokerage services and investment banks dedicated to virtual assets.

In summary

This report outlined many of the operational steps required to make VASPs mature enough for institutionalization. For VASPs to succeed, customer engagement, regulatory compliance, clearing and settlement, custody and governance are all vital to optimize. At KPMG, we are excited to follow this development and support our clients on their institutionalization journey.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

9 About KPMG

KPMG is a global organization of professional services firms providing Audit, Tax and Advisory services. We operate in 147 countries and territories and have more than 219,000 people working in member firms around the world. We lead with a commitment to quality and consistency across our global organization, bringing a passion for client success and a purpose to serve and improve the communities in which member firms operate.

KPMG firms are collaborating with innovators, corporates, industry associations and governments to understand the impacts and opportunities in the Virtual Asset industry.

KPMG firms are working with some of the leading global VASPs to help them to develop business strategies, conduct risk and technology assessments, define compliance frameworks, and advise them during regulatory applications.

Leveraging our insights and experience, we have developed API-based solutions specific for virtual assets, including a suite of transaction monitoring and compliance tools KPMG Chain Fusion, and an online tax estimation and computation tool: KPMG Crypto Tax Estimator.

In addition, we assist traditional FS organizations and challenger banks to grow a footprint in the Virtual Asset industry. Depending on jurisdiction and associated regulatory frameworks, we may also provide audit services to VASPs and investors.



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

10 Abbreviations

AML	Anti-Money Laundering
API	Application Programming Interface
B2B	Business to Business
CBDC	Central Bank Digital Currency
CTF	Counter Terrorism Financing
DeFi	Decentralized Finance Products
DTI	Deposit Taking Institution
FATF	Financial Action Task Force
FS	Financial Services
HSM	Hardware Security Modules
ID&V	Identity Collection and Verification
IOSCO	International Organization of Securities Commissions
IVMS101	Inter-VASP Messaging
KYC	Know Your Customer Program
OTC	Over the Counter
PEP	Politically Exposed Person
SDLC	Software Development Life Cycle
SFC	Hong Kong Securities & Futures Commission
SOC	Service Organization Controls
SWIFT	Society for Worldwide Interbank Telecommunication
VASPs	Virtual Assets Service Providers



Executive Summary

Evolving Customer Engagement

Reliable Regulatory Compliance: KYC best practice and onboarding

Reliable Regulatory Compliance: AML and CTF

Scaled and Stable Operations: clearing and settlement

Scaled and Stable Operations: custody and asset safekeeping

Robust Governance

Closing Outlook

About KPMG

Abbreviations

Australia**Laszlo Peter****T:** +61 2 9455 9018**E:** laszlopeter@kpmg.com.au**Max Soyref****T:** +61 2 9335 8827**E:** msoyref@kpmg.com.au**Bahrain****Manav Prakash****T:** +973 17224807**E:** mprakash@kpmg.com**Canada****Frankie Davenport****T:** +1 416 777 8047**E:** frankiedavenport@kpmg.ca**Cayman Islands****Andrew Schofield****T:** +13458152634**E:** aschofield@kpmg.ky**Gautam Ganeshan****T:** +13459144481**E:** gautamganeshan@kpmg.ky**China****Benjamin Usinger****T:** +85226857920**E:** benjamin.usinger@kpmg.com**James Harte****T:** +85221402876**E:** james.harte@kpmg.com**Cyprus****Konstantinos Botsaris****T:** +35722209220**E:** Konstantinos.Botsaris@kpmg.com.cy**Finland****Annika Tanttinen****T:** +358207672032**E:** annika.tanttinen@kpmg.fi**France****Catherine Philippe****T:** +33155688809**E:** cphilippe@kpmg.fr**Germany****Timo Purkott****T:** +49 69 9587-1533**E:** tpurkott@kpmg.com**India****Abhishek Gupta****T:** +918068335502**E:** ak Gupta@kpmg.com**Israel****Jonathan Bellish****T:** +97236848000**E:** jbellish@kpmg.com**Italy****Giovanni Colucci****T:** +3906809711**E:** GColucci@KPMG.IT**Japan****Kenji Hoki****T:** +81335485125**E:** kenji.hoki@kpmg.com**Masatake Toyota****T:** +81335485144**E:** masatake.toyota@jp.kpmg.com**Luxembourg****Said Fihri****T:** +3522251517892**E:** said.fihri@kpmg.lu**Malta****Juanita Brockdorff****T:** +35625631029**E:** juanitabrockdorff@kpmg.com.mt**Matthew Scerri****T:** +35625631270**E:** matthewscerri@kpmg.com.mt**Mexico****Jose Luis Gonzalez****T:** +525552468300**E:** josegonzalez7@kpmg.com.mx**Netherlands****Dennis de Vries****T:** +31206 567451**E:** deVries.Dennis@kpmg.nl**Panama****Glenn Tjon****T:** +5072080700**E:** gtjon@kpmg.com**Russia****Nikolai Legkodimov****T:** +74959374444**E:** nlegkodimov@kpmg.ru**Saudi Arabia****Farhan Syed****T:** +97144248985**E:** farhansyed1@kpmg.com**Singapore****Jan Reinmueller****T:** +6565071581**E:** jreinmueller@kpmg.com**South Korea****Mun-Gu Park****T:** +82221120573**E:** mungupark@kr.kpmg.com**Switzerland****Andre Guedel****T:** +41 58 249 28 24**E:** aguedel@kpmg.com**United Arab Emirates****Paritosh Gambhir****T:** +97144030495**E:** pgambhir3@kpmg.com**United Kingdom****Antony Ruddenklau****T:** +44 207 6942224**E:** anton.ruddenklau@kpmg.co.uk**United States of America****Arun Ghosh****T:** +1 617 988 1628**E:** arunghosh@kpmg.com**Salvatore Ternullo****T:** +1 617 988 1153**E:** sternullo@kpmg.com**KPMG.com**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit home.kpmg/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, "we," "KPMG," "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

March 2021. 5695746691SV