



Securing the chain

KPMG International

kpmg.com/blockchain360



Foreword

It's no secret that blockchain¹ is a potential game changer in financial services and other industries. This is evident by the US\$1B investment² in the technology last year alone. Or the fact that you don't have to look very far for blockchain use cases, which are as diverse as a foreign exchange market in financial services to the pork supply chain in consumer retailing. Some even see blockchain as a "foundational" technology set to disrupt, enable and change business processing, as we know it across industries.

To date, much of the blockchain frenzy has centered on its vast transformative potential across entire industries. So, organizations have focused squarely on "how" they can use blockchain for business. Yet, as more proof of concepts move toward practical implementations and cyber threats rapidly grow in number and sophistication, security and risk management can no longer take a backseat. In addition to "how", the question then becomes, "Is blockchain secure for my business?"

Simply put, it can be. But, not by just turning the key. Security will depend on a variety of factors, none the least of which requires a robust risk management framework. Consider, for example, that as many as half of vulnerability exploitations occur within 10 to 100 days after they are published according to one study³. Then add in the number of threats that are already known. Next, factor in the plethora of unknowns that accompany emerging technologies and you quickly see why a comprehensive view of your risk and threat landscape is necessary.

In *Securing the Chain*, we explore two recent incidents related to blockchain technology — what happened, how it happened and how it could have been prevented. We then apply the lessons learned from such incidents, and from security and risk management experience with other emerging technologies, to provide you with a framework that can help you identify and respond to threats for your specific blockchain implementation.

Organizations are already grappling with multiple frameworks and standards. At the risk of creating another one, the purpose of our blockchain framework is to enable a comprehensive (and critical) line of questioning to ensure blockchain implementations are secure and resilient. We fully expect organizations to take the leading practices underpinned by this framework and integrate them with their existing security and risk management capabilities and frameworks.

We believe this report will provide you with valuable insight and awareness so that you can ensure your blockchain implementation is truly secure. To discuss your organization's specific needs, please contact your local KPMG office.



Kiran Nagaraj
Managing Director
KPMG in the US



Eamonn Maguire
Global Head of Digital Ledger Services
KPMG in the US

¹ For purposes of simplicity, references to "blockchain" throughout this paper also include other Distributed Ledger Technologies (DLT), which were inspired by or built based on the underlying architecture concept of the widely popular Bitcoin.

² Finance firms seen investing US\$1 billion in blockchain this year, bloomberg news, 2016

³ Verizon 2016 DBIR <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>



Isn't blockchain inherently secure?

There is a common misconception that blockchain is inherently secure because its principles are founded on cryptography and immutability (i.e., information can be permanently stored on a public ledger without being tampered with). But despite its strengths and promise, blockchain is not inherently secure, and even a small oversight can have a significant impact.

Two recent incidents made this point clear by showing how attackers can exploit security oversights within individual organizations while simultaneously using the fundamental strengths of blockchain technology. Let's take a closer look at each.

The DAO incident

What happened?

In June 2016, approximately US\$50 million in assets was drained from a newly formed digital venture capital fund, — the Decentralized Autonomous Organization (the DAO). The DAO is a leaderless, virtual organization built within a smart contract on the Ethereum blockchain. This smart contract sets rules that provide the ability for participants to vote on which ventures would be funded using the Ether (a crypto currency similar to Bitcoin) that each participant contributes to during the creation of the DAO. The larger the contribution, the larger the number of votes each participant has. When a vote is finalized, the Ether coins are distributed to the venture's Ether wallet and are recorded as an immutable transaction within the Ethereum blockchain.

In the days prior to the attack, a software vulnerability was identified and published⁴ for the "split DAO" function.

This function was originally designed to allow participants of the DAO to transfer their account balance and branch off into a new DAO, dubbed a "child DAO" if they decided to go in a different direction with their investments after a vote. Just like in a traditional demand deposit account, the network would check the participant's balance and then transfer it to the child DAO. When the split was finished, the participant's balance in the original DAO would be zeroed out.

The vulnerability published showed that while the split function worked correctly, it allowed participants to call another split before the first split was finished. Because balances are not zeroed out until the end of the split, the attackers were able to perform the same split over and over again, nearly 200 times, until the DAO was nearly empty.⁵

What caused it?

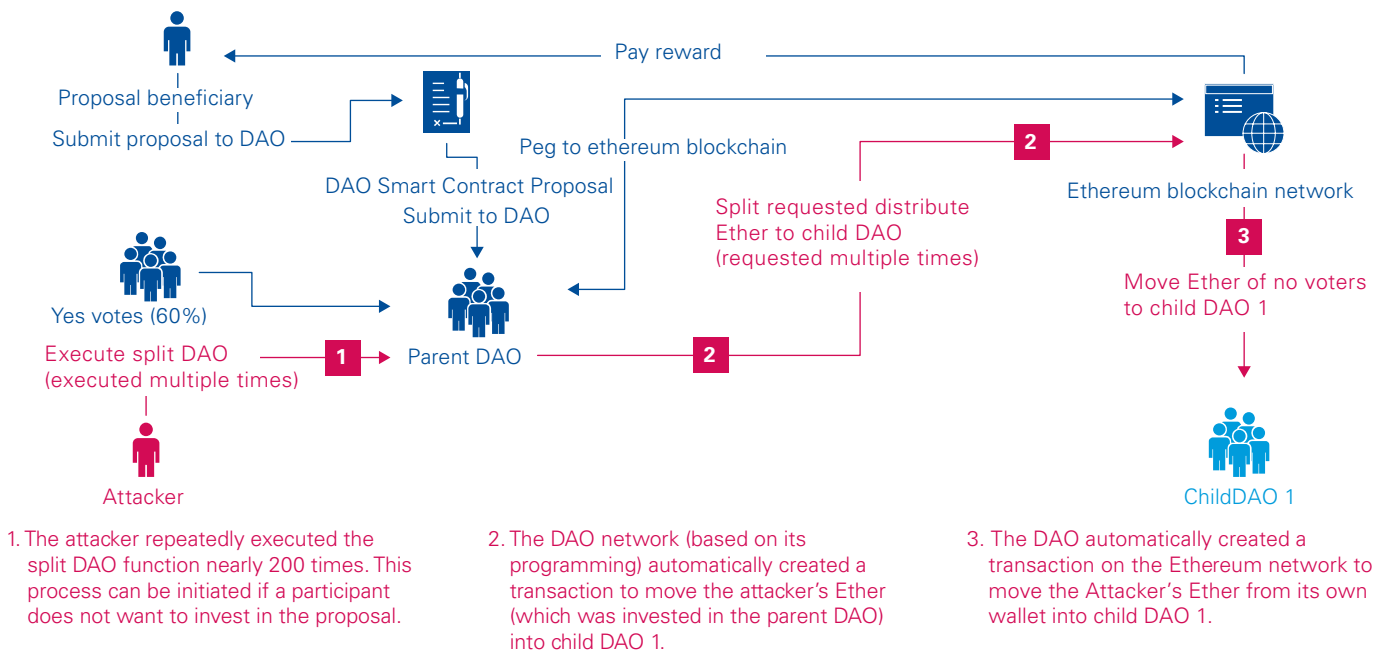
The cause of the outflow of funds seems clear: there was an unintentional

flaw in the code of the "split DAO" function of the DAO smart contract. Ethereum, the blockchain technology that the DAO is built upon worked as it was designed and was not compromised in any way. The attacker's exploit took full advantage of this design and the knowledge that the blockchain technology itself works.

Could it have been avoided?

Yes. Based on publicly available information, the hack could have been avoided if the DAO's smart contract code had undergone a thorough, formal review before going live. While easy to know the right thing to do after something has happened, these assessments, reviews and testing activities are those that any enterprise grade application is expected to go through prior to being used in production given today's cyber threat landscape.

Breaching the DAO



The attacker's Ether balance within the DAO was only checked a single time during this process, which allowed them to drain the massive centralized wallet of the DAO over many transactions.

⁴ No DAO funds at risk following the Ethereum smart contract 'recursive call' bug discovery, Stephen Tual, June 2016

⁵ Understanding The DAO Hack for Journalists, David Siegel, June 2016

The Bitfinex breach

What happened?

In August 2016, the Hong Kong-based Bitfinex crypto currencies exchange suffered a security breach in which almost 120,000 Bitcoin were removed from customer accounts. Bitfinex used a number of security measures including a multi-signature key management system, which divided private keys for each user's wallet among two different parties to reduce the likelihood of a successful breach.

What caused it?

At the time of publication of this report, the cause of the attack had not been confirmed by Bitfinex. Two of the three keys in Bitfinex's multi-signature system were held internally. The third key was held by a third-party wallet provider, BitGo. All three of these keys would be required to make a transaction. Regardless of who is at fault, systematic controls to prevent and detect analogous transactions put into place by either party could have helped minimize the losses sustained. Similar to the example above, this attack exploited security vulnerabilities

within individual organizations and the blockchain (Bitcoin in this example) network remained fully functional and operated as intended.

Could it have been avoided?

Yes, the hack might have been prevented, if Bitfinex and BitGo developers and their business side counterparts had conducted an in-depth review of security using various risk scenarios throughout the end-to-end transaction lifecycle. By performing an end-to-end review, these organizations would have a better opportunity to identify and mitigate risks, beyond just IT risks such as private key management. Once again, while hindsight is 20/20, these are standard activities that enterprise grade technology running many industries of today would have typically applied.

As these examples clearly illustrate, despite its strengths and promise, blockchain is not inherently secure, and even a small oversight can have a significant impact.

Crypto currency exchanges are organizations that help interested individuals in trading a traditional currency (e.g. USD) for crypto currencies such as Bitcoin. In the traditional sense, crypto currency exchanges operate as not only an exchange, but can also act as a broker dealer as well as a custodian. There are a number of crypto currencies in operation today, all of which are operating in a grey area when it comes to regulations.

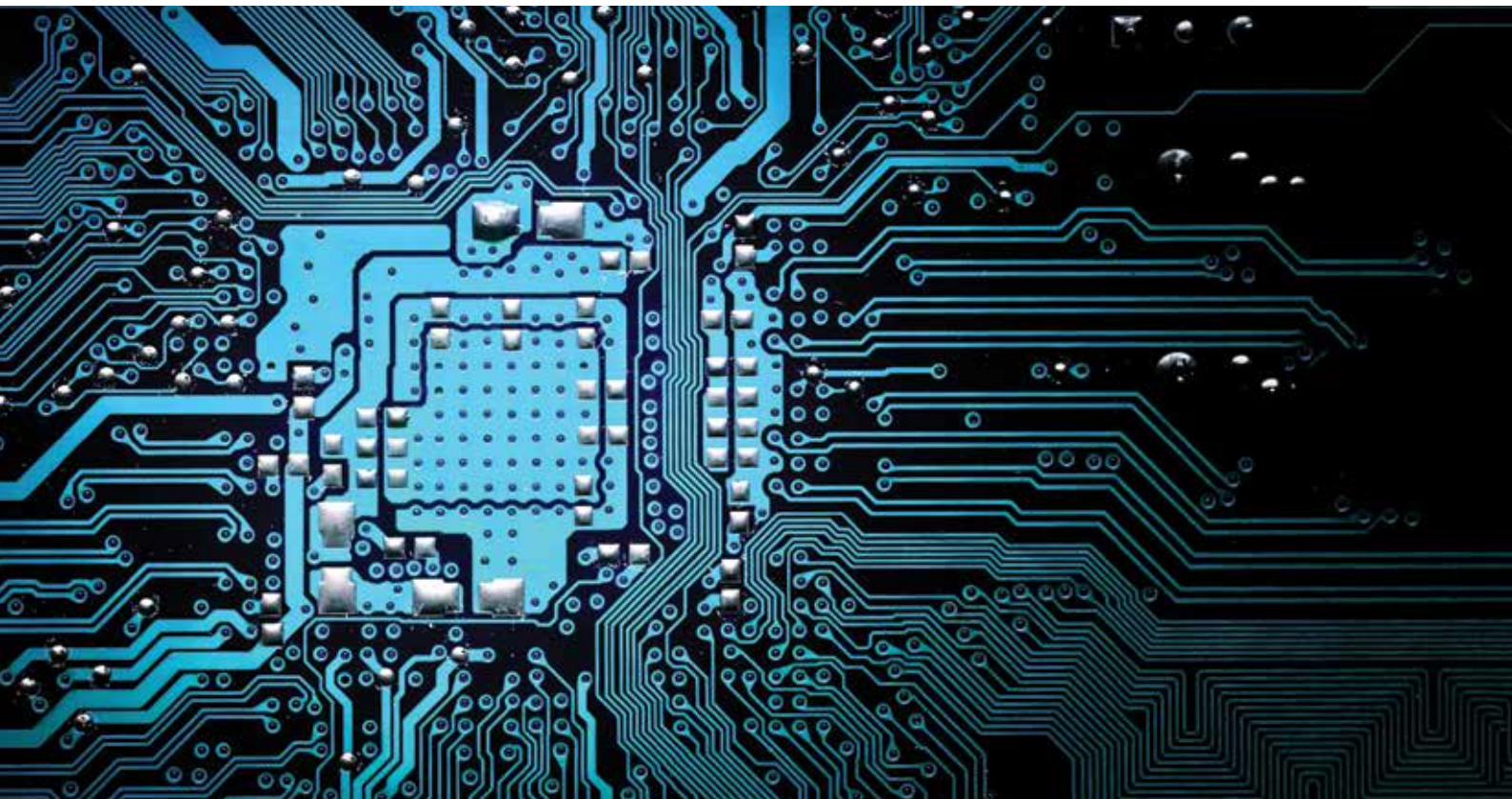


Is blockchain fundamentally flawed?

Hard forks in a blockchain indicate when a single blockchain breaks into two new independent blockchains. The original blockchain stays immutable, but future blocks after the hard fork are only part of the new fork itself.

No, the underlying foundation and architecture is not fundamentally flawed. In the case of the DAO incident particularly, there has been much debate around whether the network should permit the ability to rewrite history through a “hard fork.” On the one hand, those who lost their investment would be very happy, but on the other hand, the rules of the network would have been bent for a particular scenario and would have set a dangerous precedent for the future. Regardless of the solution chosen, the underlying architecture functioned as it was expected to.

Technical aspects of these incidents, including the potential impact on immutability of a blockchain have been widely covered by blockchain blogs and major newspapers. Given the underlying architecture and foundation can still be considered reliable, in this paper, we will instead focus on how organizations can take a more business centric approach to building blockchain solutions that are secure and resilient. Because, blockchain is here to stay and its adoption will only increase.



Lessons learned

Both incidents examined on pages 4 and 5 underscore the need for a comprehensive view of risk. In each instance, many of the vulnerabilities and design flaws could have been addressed earlier, if there was discipline applied to identify, assess

and mitigate risks during design or testing. There are lessons to be learned from these and other incidents, but also just as importantly are lessons learned from decades of security and risk management experience with other traditional and emerging technologies.

“While an understanding of prior pitfalls and challenges is helpful, a comprehensive framework is required to identify and respond to security threats and risks.”

Examples include:

Applying blockchain experience

Cryptographic key theft — an attacker with access to a private key can make fraudulent transactions, including fraudulent withdrawals.

Consensus mechanism override — a group of attackers can achieve consensus on a transaction that is beneficial only to themselves.

Anonymity — members of a public blockchain can hide their identity, making it difficult to find attackers, as in the case of the DAO hack.

Applying decades of security and risk management experience

Poor implementation — inadequate testing creates vulnerabilities in the software code.

Unauthorized access — inappropriate access to private keys or blockchain related software could be used to steal funds or information.

Identity management — personally identifiable information may be stolen or a node impersonated to obtain access to a blockchain.

Today's blockchain landscape has many different variants including public chains, private chains and a number of different consensus mechanisms. Each specific implementation or use case brings its own security and risk implications. Consider the example of anonymity above — the implication and applicability of anonymity in a public chain such as Bitcoin is vastly different from that in a permissioned chain

with a handful of nodes trading credit default swaps where all parties are known and likely bound by a traditional International Swaps and Derivatives Association (ISDA) agreement. While an understanding of prior pitfalls and challenges is helpful, a comprehensive framework is required to identify and respond to security threats and risks related to any blockchain implementation.

Securing the chain

“

The sheer excitement over this innovative technology and its promising potential has eclipsed a true focus on the possible threats and risks.”

KPMG has built a security and risk management framework which helps provide an end-to-end approach to identify and respond to security threats and technology risks for a blockchain implementation.

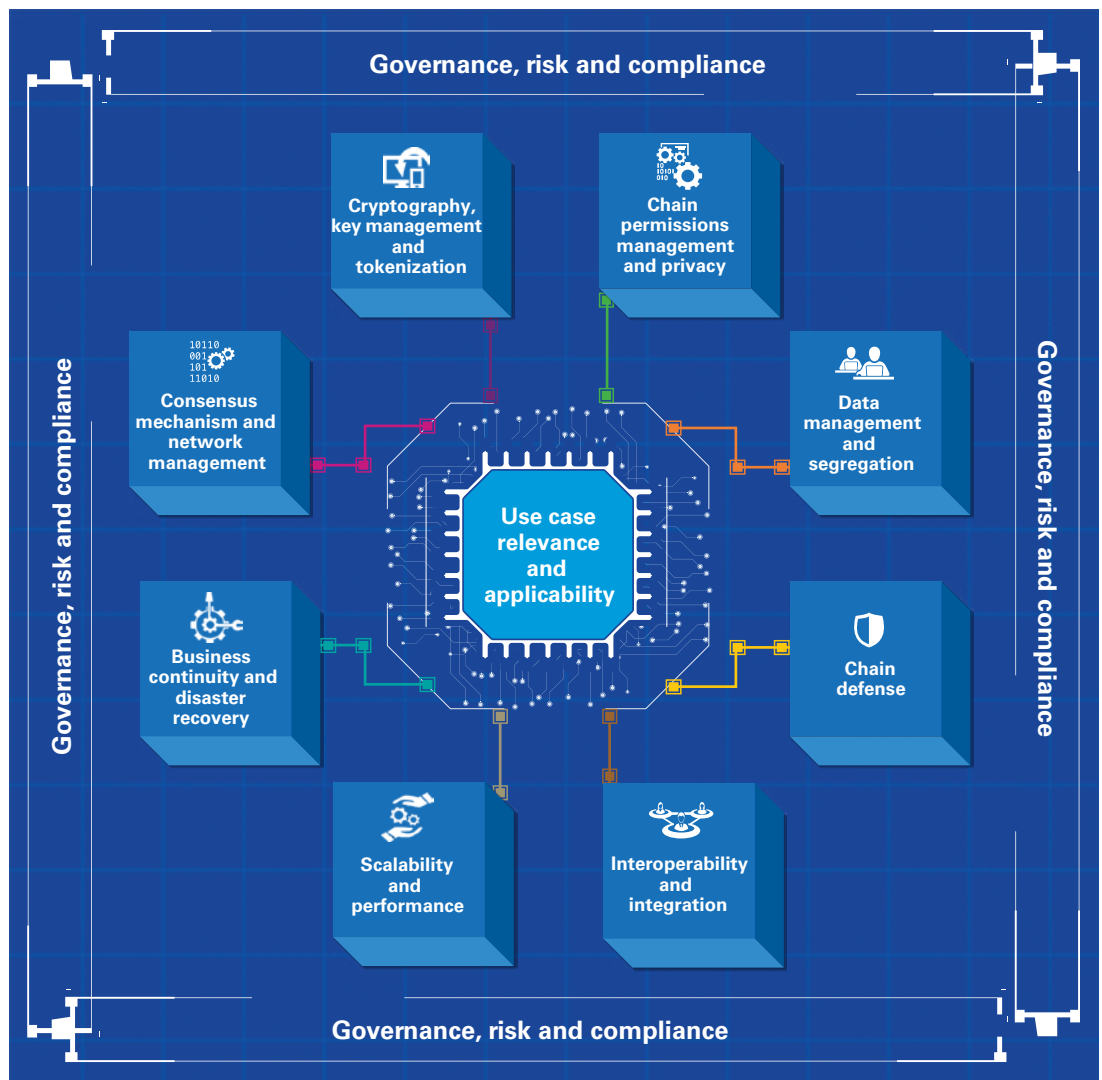
This framework was developed through the identification of leading practices across ten key dimensions that are applicable across a typical blockchain implementation lifecycle — from strategy and business case to operate and maintain.

While some dimensions within this framework such as Data management

and segregation are typically part of existing capabilities for Security and Risk departments within organizations, others such as as Consensus mechanism, Chain permissions management, and Cryptography, key management and tokenization, may be entirely new and will need to be considered for inclusion within existing frameworks and standards.

A sample of leading practices across each of the ten dimensions underpinned by this framework are included on the following page.

KPMG’s blockchain security and risk framework





Applying KPMG's blockchain security and risk framework



Blockchain security and risk framework

- | | |
|--|--|
| <ul style="list-style-type: none"> Consensus mechanism and network management Cryptography, key management and tokenization Chain permissions management and privacy Use case relevance and applicability Data management and segregation | <ul style="list-style-type: none"> Chain defense Interoperability and integration Scalability and performance Business continuity and disaster recovery Governance, risk and compliance |
|--|--|

Actions that may have been avoided

-  The Bitfinex breach
-  The DAO incident

Source: Excerpt of leading practices from KPMG's framework



Conclusion

Many anticipate blockchain will significantly disrupt and transform business models in financial services, healthcare and beyond. Yet, the sheer excitement over this innovative technology and its promising potential has eclipsed a true focus on the possible threats and risks. As blockchain continues to build significant momentum and reality sets in, companies cannot turn a blind eye to security and risk management any longer. Blockchain may even provide a false sense of security through some core features around cryptography and immutability. It is now time to apply a risk management lens.

Moving forward, we believe the security and risk considerations, including those discussed in this paper, will steer the use cases and implementations of blockchain across industries. By analyzing lessons learned from recent examples of blockchain related incidents and from decades of experience in security and risk management, organizations can be better equipped to implement secure and resilient solutions around this emerging technology.

KPMG and Microsoft alliance

KPMG and Microsoft are creating and implementing prototype solutions that use blockchain technology at joint blockchain “nodes” around the world, enabling clients to discover and test ideas based on market insights. The KPMG and Microsoft Blockchain Nodes located in Frankfurt, New York and Singapore will provide an opportunity to create and demonstrate use cases that apply blockchain technology to business propositions and processes and help organizations achieve their strategic goals.

With a priority focus on applications for financial services, the blockchain nodes will also further examine how blockchain technology can optimize business processes and models for healthcare and the public sector, and potentially other industries in the future.

To learn more, visit kpmg.com or contact your local KPMG member firm.

Authors



Kiran Nagaraj
Managing Director
KPMG in the US
E: kirannagaraj@kpmg.com



LaDarius Goens
Associate
KPMG in the US
E: ladariusgoens@kpmg.com



Sam Wyner
Manager
KPMG in the US
E: swyner@kpmg.com



Eamonn Maguire
Global Head of Digital Ledger Services
KPMG in the US
E: emaguire@kpmg.com

Acknowledgements



Dennis deVries
Lead, Digital Ledger Services
KPMG in the Netherlands
E: devries.dennis@kpmg.nl



Hardwin Spenkelink
Senior Consultant
KPMG in the Netherlands
E: spenkelink.hardwin@kpmg.nl

Related reading



Blockchain accelerates insurance transformation

This provides an overview of how blockchain can be applied to the insurance sector. We offer insight into how blockchain technologies will impact key activities across the operational ecosystem and identify areas of change for these activities throughout the enterprise. The report also features practical actions insurers and reinsurers can take now to prepare for, and get the most value from, the disruption ahead.



Consensus: Immutable agreement for the internet of value

Within computer science, consensus has become the backbone of blockchain and other distributed ledger technologies. This paper aims to provide the relevant questions to ask when deciding on whether this technology is right for your organization, and if so, what kind, and how it might best be implemented.

Contacts

Eamonn Maguire

Global Financial Services and North America Lead Digital Ledger Services

KPMG in the US

E: emaguire@kpmg.com

Phil Lageschulte

Global Emerging Technology Risk Leader

KPMG in the US

E: pjlageschulte@kpmg.com

Wei Keat Ng

Global COO Digital Ledger Services

KPMG International

E: wei.keat.ng@kpmg.co.uk

US

Kiran Nagaraj

KPMG in the US

E: kirannagaraj@kpmg.com

Charlie Jacco

KPMG in the US

E: cjacco@kpmg.com

Malik Faizullah

KPMG in the US

E: mfaizullah@kpmg.com

UK

Chris Mills

KPMG in the UK

E: chris.mills@kpmg.co.uk

Netherlands

Dennis de Vries

KPMG in the Netherlands

E: devries.dennis@kpmg.nl

Germany

Sven Korschinowski

KPMG in Germany

E: skorschinowski@kpmg.com

Singapore

Jan Reinmueller

KPMG in Singapore

E: jreinmueller@kpmg.com.sg

kpmg.com

kpmg.com/socialmedia



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.

© 2017 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by Evalueserve.

Publication name: Securing the chain

Publication number: 134352-G

Publication date: May 2017