Securing the Blockchain

16 May 2017

Two high profile blockchain incidents prompt comprehensive risk framework for secure and resilient implementation. Organizations can no longer turn a blind eye.

Highlights

- Recent incidents: What happened and how?
- Is blockchain fundamentally flawed?
- Securing the chain
- KPMG’s blockchain security and risk framework

Eamonn Maguire

KPMG in the U.S.

Kiran Nagaraj

KPMG in the U.S.

Related content

Transformation Insights from the CEO Outlook Report

Business transformation is one of the most critical issues facing CEOs today.

Nexus between regulation and technology

How RegTech allows greater strategic advantage, reduce cost and harmonize coordination.

No room for complacency

Insurers' need for better cyber security

To date, much of the blockchain frenzy has centered on its vast transformative potential with many organizations focusing 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. 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 examine two recent high profile blockchain incidents in which the attackers exploited security vulnerabilities while the blockchain networks and their underlying infrastructure continued to function as intended.

Recent incidents: What happened and how?

The Decentralized Autonomous Organization (DAO) incident

In June 2016, approximately US$50 million in assets was drained from a newly formed digital

venture capital fund, the DAO, due to an unintentional flaw in the codes. Ethereum, the blockchain technology that The DAO was built upon, was not compromised in any way. The vulnerability published showed that while the split function worked correctly, it allowed participants to call another split before the first split was finished. The attacker simply took advantage of the design and the knowledge that the blockchain technology itself actually works.

The Bitfinex breach
In August 2016, the Hong Kong-based Bitfinex crypto currencies exchange suffered a breach in which almost 120,000 Bitcoin were removed from customer accounts. Similar to the DAO example, the attack exploited security vulnerabilities within individual organizations and service providers, while the blockchain network remained fully functional and operated as intended.

Is blockchain fundamentally flawed?

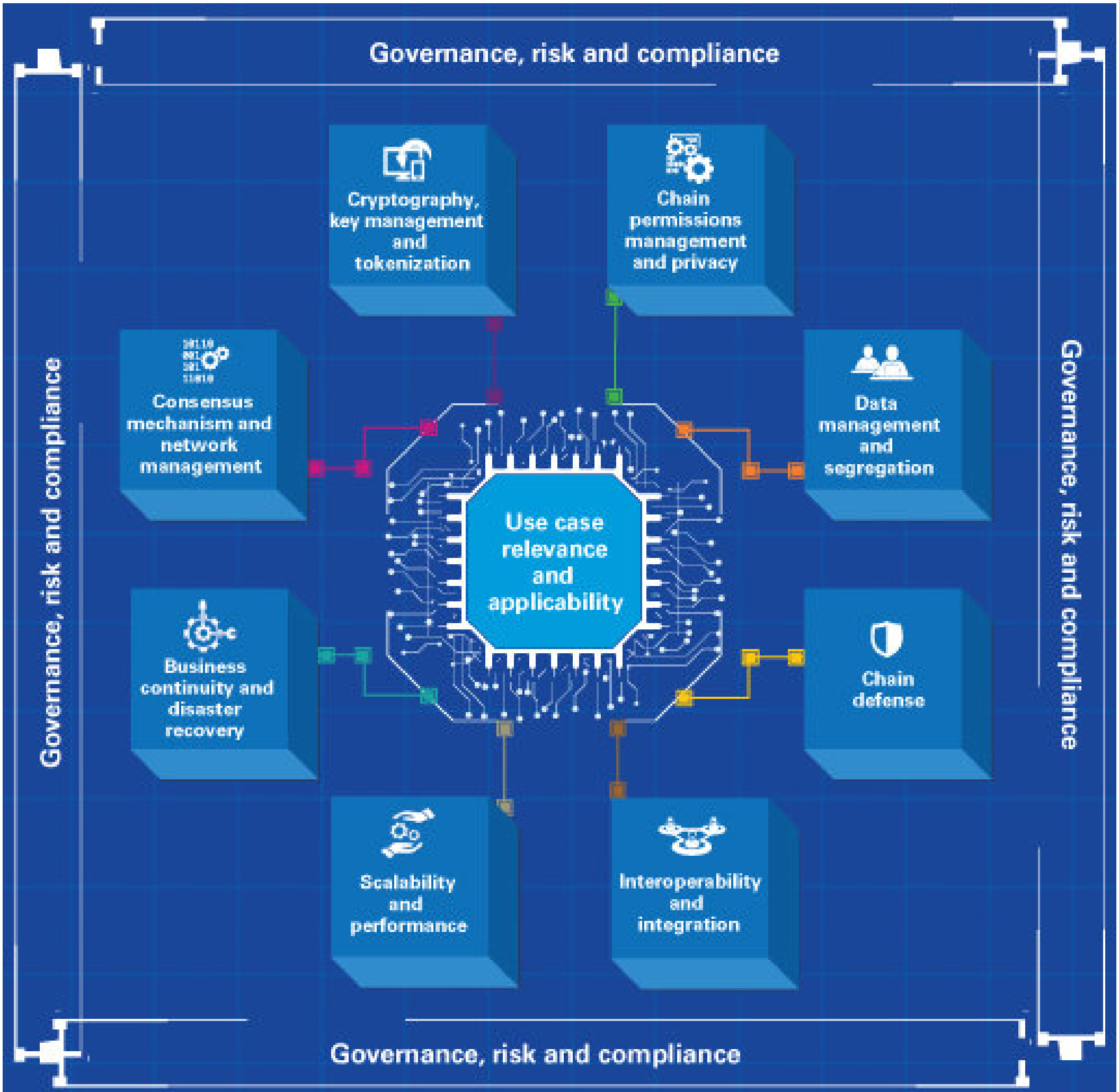
No, the underlying foundation and architecture is not fundamentally flawed. In both incidents, the attackers exploited security oversights within individual organizations, while taking advantage of the fundamental strengths of blockchain technology. Given the underlying infrastructure can still be considered reliable, we should focus on how organizations can build and benefit from blockchain solutions that are secure and resilient.

Securing the chain

In each instance, many of the vulnerabilities could have been addressed during the design or testing phase. We believe 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.

In the report, we provide a blockchain security and risk framework based on leading practices to enable a critical line of questioning to ensure your blockchain implementations are secure and resilient. The leading practices underpinned by this framework can be integrated with your existing security and risk management capabilities and frameworks.

KPMG’s blockchain security and risk framework



Learn more about the risk framework in the publication, and contact your KPMG advisors to discuss how you can mitigate security threats and technology risks to establish a secure and resilient blockchain.

Distributed Ledger Services at KPMG: Seize the potential of blockchain today

Blockchain technology is set to disrupt financial services, but also has potential for significant value.

Connect with us

- Find office locations
- Email us
- Social media @ KPMG

Request for proposal

Submit

Save, Curate and Share

Download PDF (939.5 KB)




Submit RFP

Find out how KPMG's expertise can help you and your company.