BLOCKCHAIN FOR BUSINESS: APPROACHES TO RISK MANAGEMENT

Sponsored by Cyber Talk

Introduction

Blockchain is considered a major technological breakthrough and adoption of blockchain ledger technology can be a strategic business enabler. Blockchain can help address data management issues around communication, verification, security and privacy. The technology is also lauded for its potential to reduce costs and to unlock economic value.

Blockchain solutions are not limited to cryptocurrency exchanges. Numerous applications for blockchain exist that span beyond cryptocurrency. To leverage the benefits of blockchain, a strategic approach is needed across all aspects of technological adoption, deployment, maintenance and security.

The primary focus in this piece is security. While blockchain is widely perceived as highly secure, blockchain continues to require a comprehensive approach to risk management.

In 2016, a blockchain-based design flaw enabled a hacker to disappear with $67 million.[1] This highlights the fact that cryptographic protocols retain limitations. In addition, security is as much about people, policies, and processes as it is about the technology.

If you have billions of dollars' worth of proprietary data or assets stored on blockchain, it pays to be careful when it comes to security.

[1] "The Ether Thief" by Matthew Leising, Bloomberg, 13 June, 2017
https://www.bloomberg.com/features/2017-the-ether-thief

THE BUSINESS CASE FOR BLOCKCHAIN

Blockchain can deliver immense value for businesses, as it can address a variety of pain points -as denoted on the right-hand side of the page- and it can also lead to cost reductions, faster transactions, and innovation.

REAL-WORLD SCENARIOS

Blockchain is actively transforming enterprises around the globe. Blockchain ecosystems have shown strongly positive outcomes within the financial services, food distribution, government, and retail sectors, among others.

Safeguarding the Food Supply Chain.

Blockchain-based platforms are empowering food growers, processors, distributors and retailers to make food safer; saving resources, reducing waste, and keeping human hearts and minds healthy. Via blockchain-based technologies the food supply chain is reinventing processes and best practices to create a more sustainable future.

Shipping Improvements.

Remember the international shipping delays of 2020 and 2021? The world runs on a tightly timed set of logistics, a must-function set of networks, automatic scheduling systems, critical business relationships and closely followed international agreements. The slightest deviation in any of these areas can lead to significant shipping disruptions. Blockchain-based platforms have enabled shipping groups, ports, customs services and others to optimize shipping services and to reduce the likelihood of disruptions.

Reducing Banking Inefficiencies.

Within the banking sector, institutions are using blockchain-based platforms to facilitate faster and lower-cost transactions among small-and-medium-sized enterprises.

Nonetheless, blockchain isn't considered a short-term technology and business leaders are encouraged to take the time to carefully consider whether or not it genuinely adds value to the business.

Use of Blockchain Within Businesses Permits:

- **Communication.** User groups can see one another's activities and transactions as permitted through set permissions..
- **Verification.** After a "block" is approved, the block is automatically replicated across the legers for all relevant parties. Each user group can see a single reliable record of participants' transactions.
- **Security.** Although "blocks" may be continuously added to the transaction chain, blocks cannot be removed. In this way, participants are prevented from tampering with records.
- **Privacy.** In order to create blocks, participants must be authorized. Only trusted partners can be granted participation rights.

BLOCKCHAIN SECURITY

For organizations that expect to adopt blockchain or that have already adopted the technology, preemptively addressing blockchain security helps protect people, processes, the technology itself and integrated assets in order to ensure sustained business development. Risks associated with blockchain solutions can be grouped into three different categories:

1. **Operations and governance.** The decentralized nature of blockchain means that organizational use-cases require strong governance policies, along with robust identity and access management.
2. **Processes.** Inherent within blockchain architecture and operations are various processes that present risk.
3. **Technological implementation.** Because there is always technology surrounding blockchain-based systems, some level of technological risk will persist in indefinitely.

SECURING BLOCKCHAIN SOLUTIONS

Develop a Risk Model

Develop a risk model that explores governance, policy, process and technology-related risks. Identify traditional threats that could potentially affect your blockchain technology. In addition, identify blockchain-specific threat vectors. Outline risk scenarios and then assess them based on probability and potential impact.

Know Your Data

Take inventory of the data on your blockchain platform, and understand the sensitivity and business value of that data.

> In 2016, an infamous hacker exploited a blockchain-based design flaw and disappeared with $67 million.[1]

Adopt a Data Classification Strategy

Separate data into various categories (for example, legal, financial, routine business, and technical) so that relevant security controls can be applied. Re-examining and reinforcing data security on a regular basis is critical.

Secure Blockchain Transactions

Develop, define and enforce proper endorsement policies on blockchain-based business contracts. Endorsement policies provide criteria that enables the leger to assess the validity of a transaction. These kinds of policies should be bound to a smart contract that can quickly determine the security of the business network, and contract-related data. Policies should be scoped and specified on a namespace and ledger key level.

---

[1] "The Ether Thief" by Matthew Leising, Bloomberg, 13 June, 2017
https://www.bloomberg.com/features/2017-the-ether-thief

Identity and Authentication

When it comes to securely storing blockchain data, enforce identity and access controls. Create policies that offer the right level of access to the right persons. New users should be properly on-boarded to platforms, and in a similar vein, departing employees should be carefully off-boarded. In addition, put audit logs in place, which can alert the operations team to any unexpected behaviors.

Safely Storing Crypto Keys

Leverage and enforce the hardware security model (HSM), which helps to secure blockchain identity keys. Multi-organization blockchain-based groups may also want to ensure that each organization retains its own partition in the HSM, where key storage occurs. The use of blockchain identity keys ensures the security of security keys.

Follow API security best practices

To safeguard API-based exchanges, ensure that API security best practices are applied. Consider using an industry standard, like OAUTH to help standardize interactions and to secure API keys simultaneously.

General infrastructure security

An organization's general level of infrastructure security affects security for its blockchain-based platforms. All software and hardware connected to the blockchain technology need to be secure.

Conduct vulnerability assessments

At every phase of security deployment, ensure that your organization takes the time to conduct vulnerability assessments. These assessments should occur across levels and systems, and can prevent intruders from testing your controls for you.

Conclusion:

Blockchain has the potential to become a business disruptor and to generate new digital transformations. Exciting applications for blockchain have been identified in industries ranging from agriculture to finance. As the technology continues to evolve, applications will mature.

Although blockchain maintains a reputation as a highly secure technology, protecting blockchain is still a business imperative that will drive operational efficiencies, and assist with growth. Because security standards for blockchain do not yet exist, setting standards for and following best practices within your own organization is key.

For more information about blockchain security, smart contracts security, or cryptocurrency security, please visit Check Point's thought leadership website, CyberTalk.org, and/or reach out to your local Check Point sales representative.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

© 2022 Check Point Software Technologies Ltd. All rights reserved.