THE DEBATE AROUND BLOCKCHAIN AND CYBERSECURITY

LOGISTICS 4.0

Adrien Ogee, Lead Security Technology and Innovation, World Economic Forum Centre for Cybersecurity
and Soichi Furuya, Senior Researcher, Hitachi

The Safety and Shipping Review 2019 conducted by Allianz has again identified cyber security as a significant threat. In this annual review, cyber incidents rank as the second top risk for the maritime and shipping sector. With major cyber-attacks on the rise over the last few years, like the NotPetya that affected supply chain multinational companies including Maersk and FedEx's European subsidiary TNT Express, many organizations are trying to reduce their cyber risk exposure. As the industry is also experimenting with blockchain and distributed ledger technologies to increase efficiency, what are the security implications?

MEETING IN THE MIDDLE

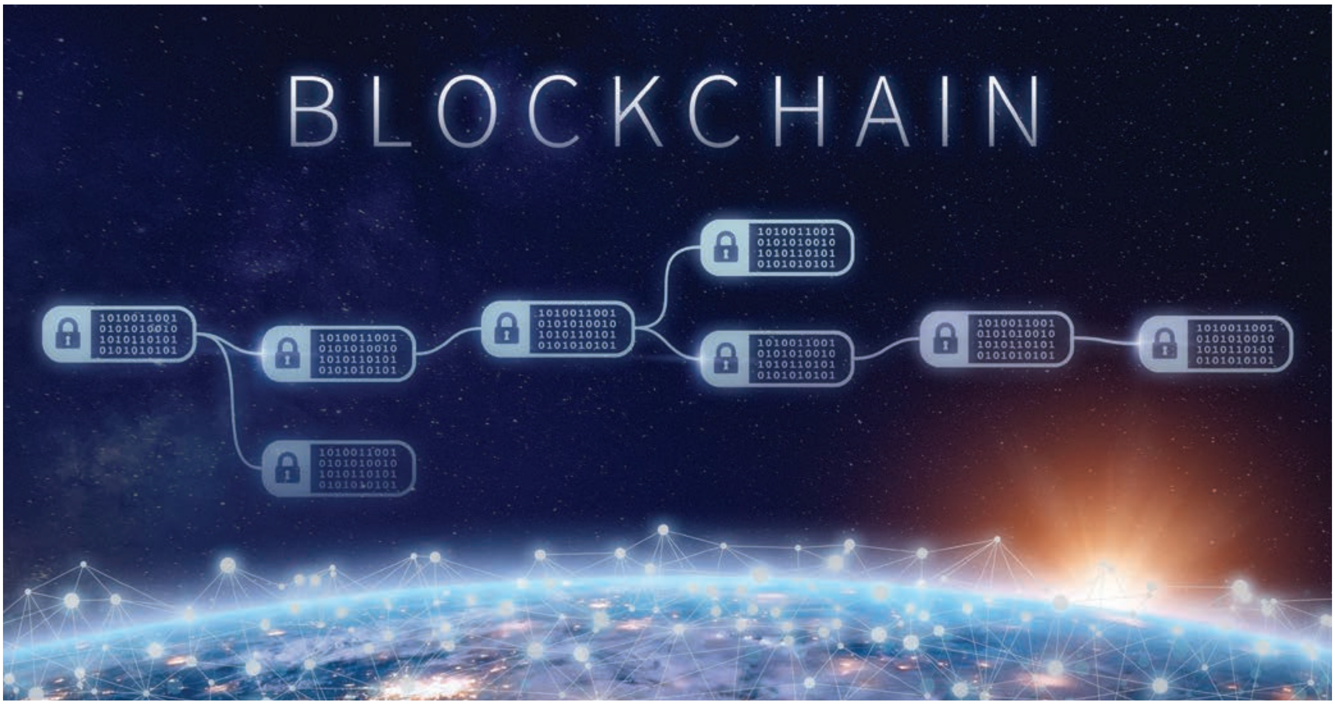
The debate around blockchain security is rather polarized. On one end of the spectrum, mostly due to the poor security reputation of cryptocurrencies, blockchain is perceived as inherently insecure and unfit for most use cases requiring privacy protections. On the other end, it is viewed as a cryptography-native and hence "unhackable" technology. The truth lies somewhere in the middle.

The belief that blockchain is inherently insecure is inaccurate, as most of the security issues reported have had more to do with overlooked traditional information security challenges than with technological flaws unique to blockchain technologies. On the opposite side, Deloitte, in its 2019 global blockchain survey, reported that over two-thirds of enterprises believe in the inherent security guarantees offered by blockchain. This line of thought is equally dangerous, for it can lead to a lack of due diligence.

Determining the facts has been problematic and abound with hyped claims and misleading terms from solution providers and others abound. This could lead to inaccurate evaluation of cybersecurity risks and an over-reliance on blockchain technology.

COMPLETE UNDERSTANDING

It is true that blockchain can improve resilience of the system. The application of consensus mechanisms provides more resiliency. Blockchain networks are also harder to take down because their distributed nature creates many targets instead of just one. However, it is very important to understand that a risk profile changes drastically by use cases, scale of deployment, and potential threats. Therefore, good security features of blockchain are deployment and design specific.



Effective cybersecurity is dependent on a sound risk management approach; from careful engineering and system design, to code review, penetration testing, user awareness and governance – using a blockchain alone generally does not add value. While there will be different security challenges in cybersecurity depending on if the blockchain is public or private, permissioned or permissionless and other variables, there are some transverse building blocks that help companies who are turning to blockchain do so with confidence.

TEN-STEP PROCESS AND SMART PORTS

"At the World Economic Forum, we created a ten-step secure deployment process for companies in the supply chain industry to consider before embarking on the blockchain journey," says Nadia Hewett, Blockchain and Distributed Ledger Technology project lead at the World Economic Forum Centre for the Fourth Industrial Revolution. The blockchain secure development process foresees ten steps, from acquiring human capital and defining security goals, all the way to monitoring, auditing and responding to cybersecurity incidents. This framework is part of the project Redesigning Trust: Blockchain for Supply Chains, led by the World Economic Forum, with participation from 100+ public and private sector entities.

The Head Strategy and Innovation at the Valencia Port Authority, Ramón Gómez-Ferrer, confirmed the importance of following such a framework, which can help highlight pinpoints such as the difficulty to ensure data confidentiality. Such findings guided the development of the blockchain proof-of-concept the Valencia Port Authority used for its Smart Port initiative .

"It is important to note that, while introducing risk management principles and various solutions to increase immunity to cyber-attacks, it is not enough. Security is a continuous process that requires constant vigilance," adds Hewett. "Additionally, distributed ledger technologies pose novel challenges to security practitioners, notably decentralized security governance. How will blockchain consortiums manage crises in a fast and effective manner, when not one but ten or fifty Chief Information Security Officers need to agree on a common mitigation plan?"

Blockchain is not a go-to technology to reduce cyber risk exposure. It brings about certain security advantages, notably around supporting data integrity and availability, but like any other technology, it also brings about a set of risks.

The long-term sustainability of any blockchain platform will necessarily require an ecosystem approach at the business layer. And this is probably the biggest challenge that blockchain poses to cybersecurity practitioners. Security has always been a centralized affair and breaking the discipline open, from egosystems to ecosystems, will require a paradigm shift.

ABOUT THE AUTHORS

Adrien Ogee advises governments and private companies on the innovative use of future technologies from an adversarial and a defender's perspective. Prior to joining the World Economic Forum, Adrien held various cybersecurity roles in the aerospace sector, the French government and the European Commission.

Soichi has overseen research and development of IT security and service design for utilities and social infrastructure operators at Hitachi. Currently he is also a Fellow, Blockchain and Distributed Leger Technology, World Economic Forum, Centre for the Fourth Industrial Revolution.

ABOUT THE ORGANIZATION

The World Economic Forum is the International Organization for Public-Private Cooperation. The Forum engages the foremost political, business, cultural and other leaders of society to shape global, regional and industry agendas. It was established in 1971 as a not-for-profit foundation and is headquartered in Geneva, Switzerland.

Hitachi: With our Mission of contributing to society through the development of superior, original technology and products, Hitachi engages in the Social Innovation Business on a global basis, putting our IT and OT (operational technologies) to use in the advanced social infrastructure systems.

ENQUIRIES

Adrien.ogee@weforum.org
+41 22 869 12 12

soichi.furuya@hal.hitachi.com
+1-669-214-6413