Blockchain is being introduced in an already fragile digital landscape, with reports of hacking being ubiquitous. A single cyberattack in late June last year cost Maersk up to $300 million. Maersk responded with “different and further protective measures” to contend with a “new type of malware”. This highlighted a growing problem for the shipping industry. Blockchain is hailed as a safe, robust alternative to existing systems with central points of failure. If this claim is factual, could the maritime sector be facing an inevitable transition to such solutions? As a provider of a Blockchain-based platform for trade related documentation processing, CargoX has put extensive thought into the sensible adoption of Blockchain for the maritime industry. Many of the concerns around adopting blockchain regard the peripheral points of failure rather than Blockchain as a protocol itself.

PARALLELS FROM THE EARLY DAYS OF INTERNET?

This is not the first time industries have faced these questions. In the very beginnings of the internet there existed a dichotomy of the two widely diverging attempts at cyber security that are still being used and played out on the stage of society; security either by isolation or obscurity.

In the early 90’s, companies and banks were deciding on the best way to integrate emails into their corporate structure. The innovation was met with many of the same critiques that Blockchain-based solutions for data flows are facing today; “None of our clients are using it, who are we going to transact with using Blockchain?” “The implementation looks daunting and overridden with complexities that might be risky and require scrutiny”.

But the veracity of Blockchain as a technical impetus of innovation continues to beckon us, as providers of commerce, into examining all possible modes of operation. Additionally, in the context of cyber security, it calls us to re-examine the practices of previous decades, which should serve as a testing ground from which conclusions can be derived for the creation of differing approaches to information security. Not only do systems need to be updated, but the calibration of solutions for organizations handling large transactions must be in sync with the current flows of technical evolution. This evolution sync must also encompass the minds of talented individuals who are pushing the fronts of digital boundaries — the cyber experts who are seeing a picture much more troubling than unsuspecting users do, as well as the wide range of Hacker types, some of whom simply like to discover systemic faults in new hardware and are very important in driving the discovery of the weaker elements of the current digital landscape.

CYBER HACKING... STIGMATIZED OR NECESSARY?

Barnaby Michael Douglas Jack, a hacker and cyber-security expert who famously demonstrated an ATM exploit in 2010, once commented: “Sometimes you have to demo a threat to spark a solution”. We live in a time when companies will no longer be able to rely on the good will of ‘White Hat’ Hackers, and trying to repressively fight all hacking comes at the cost of stifling innovation. This is an
element of society we simply cannot control. Last year, over 2 billion records were lost or stolen, and in many cases it takes months for the news of these attacks to reach the public. The UN estimates that 80% of these attacks are committed by ultra-sophisticated criminal organizations. If correct, this would represent one of the largest illegal economies in the world, with a capitalization of over $400 billion, greater than the GDP of many nations. To call them criminals falls short as a designation of their relevance, given the complexity of these issues.

We innovate, learn and recreate our systems, until they become so advanced that we maximize our potential as a civilization. Blockchain is only at the beginning of this larger societal pursuit of technical eminence, which would signifies an era of no further obsolescence. But today we are far from that point in time. We must consider the reality that cyber security is inadequate today. Saying "our current systems of old are impenetrable" should be weighed against the measure of rationality which is attained only by being constantly up to date. New ways of hacking, and along with it the process of discovering obsolescence of our technical solutions, are emerging with certainty and traces of the effects they have on the shipping industry.

LESSONS FROM PAST MISTAKES?
As large corporations first attempted to join the internet revolution, they did not just blindly connect straight to TCP/IP and build applications on top of it. They built firewalls, using military analogies such as perimeter security to wall themselves in. The prevailing idea was that this made their organization more secure.

Today we see a rising trend of permissioned ledgers and isolated Blockchains. The problem with private Blockchains is that at some point the system which existed in isolation gets exposed to the outside world, and it may have such low resilience that it is not immune to real world peculiarities of the internet. If it has any bugs, we will not know about them until exposing it to external variables. A public Blockchain exposed to attacks all the time however, is one where bugs are constantly found and fixed, making the system more resilient.

The digital products and services of the past few decades were designed to exist within a wall. But the problem with walls is that we cannot trade through them easily. As businesses we do commerce, and commerce cannot happen if we are walled in. We implement all modern prerequisites of cyber security, but what is the salesperson going to use on the field? A laptop, which is vulnerable to external threats or infection, which can then distribute malware within the confines of the firewall and the full trust of his colleagues.

HARD-WIRED PROBLEM?
Malicious data-harvesting is a reality all businesses must face. We tend to underestimate hackers, be they of a malicious or benevolent sort. Wireless devices are still very vulnerable to exploits. How many OEMs are still flooding the markets with obsolete Wireless Modules? And how conscientious are they in rectification of known issues, when capital losses are taken into consideration?

The design parameters of general purpose PC hardware is arguably the most concerning area of cyber security development we face today. Intel and AMD hold the vast majority of the market share, and both currently ship their hardware with back doors that have been exploited by professionals to various degrees of concern.

Modern intrusion methods enable hackers to perform exploits without the need to sneak into your offices. One of the most vulnerable devices today are printers. An exploit can be delivered to the printer via a resume, which is designed to re-write the firmware to do basically whatever the hacker wants, including taking control of webcams, phones and microphones in the room.

HOW SECURE ARE OUR COMPUTERS?
Employees handling sensitive data need to be well informed about information security fundamentals. More emphasis should be directed at projecting the importance of these concerns, even demonstrating how easy it is to collect network packets on an open public network using a cheap WiFi adapter from Amazon and Kali Linux operating system.

Modern intrusion methods enable hackers to perform exploits without the need to sneak into your offices. One of the most vulnerable devices today are printers. An exploit can be delivered to the printer via a resume, which is designed to re-write the firmware to do basically whatever the hacker wants, including taking control of webcams, phones and microphones in the room.

ABOUT THE AUTHOR
With 7+ years experience in the CNC machining industry at Danfoss, Darko recognized Blockchain as a viable alternative to existing ERP systems such as SAP which he used on a daily basis. Studying and writing papers about supply chain applications of blockchain, he crossed over into logistics in 2018 as a Blockchain Business Integration Advisor for CargoX, providing educational and technical support for clients and early adopters of the technology.

ABOUT THE ORGANIZATION
CargoX is an independent supplier of blockchain-based Smart B/L solution that enables extremely fast, safe, reliable and etc. This ‘trustless’ functionality can be thought of as an intrinsic characteristic of Blockchain applications.

BLOCKCHAIN TO THE RESCUE?
A viable solution to cyber threats today is something for which the Blockchain seems to be ideal: a strict separation of the trusted element from the hardware. Crucial information should be kept apart from the computer — think along the lines of cloud computing. However, cloud computing still relies on data centers — critical centralized infrastructure that is demonstrably inferior to Blockchain in terms of data integrity.

Modern encryption techniques and the advent of decentralized computing underlying Blockchain have brought about a torrent of innovation at the foundation of which is digital data integrity that, ideally, we can trust. In the current landscape, we are still faced with many questions which will surely be resolved in the coming years.

One of the qualities of businesses that succeed in challenging times is that they have a rational paranoia of failure. The question of why some companies should take the leap into the wild west of digital frontiers bears with it a reminder that success is a struggle, and fleeting once we attain it. Blockchain may be indistinguishable from inevitable digital progress. Technical adaptation to Blockchain and all related security and management concerns can be perceived as markers of innovative success in the future. We do not want to be absolutely certain of any claim of security today, besides the fact that we have done our due diligence to be contemporaneous with emerging predicaments. Yet this is not to be construed as a lack of trust fatal to Blockchain adaptation, but rather as a rational assessment of the integral parts of future innovation.

ABOUT THE ORGANIZATION
CargoX is an independent supplier of blockchain-based Smart B/L solution that enables extremely fast, safe, reliable and cost-effective global Bill of Lading processing for the logistics industry and supply chains. The company has developed a decentralized platform based on the Ethereum network, and they have a pipeline of future products for the supply chain industry. They have introduced their working solution, live, on stage, in front of 250+ experts and managers, and their respected partners are already testing their solution. CargoX has been founded in 2017 by a group of professionals in logistics and software development industries, and whose aim is to transform the global shipping industry by securing the Bill of Lading documents using blockchain technology.

ENQUIRIES
Web: https://cargox.io