AI & SOCIETY (2021) 36:725–735
https://doi.org/10.1007/s00146-020-01023-w

ORIGINAL ARTICLE

IIoT and cyber-resilience

Could blockchain have thwarted the Stuxnet attack?

Sebastian Gajek[1] · Michael Lees[2] · Christoph Jansen[1]

Received: 27 February 2019 / Accepted: 13 July 2020 / Published online: 4 August 2020

Abstract
Contemporary business (including those with integrated AI capabilities) often encompasses or aspires towards the automated, networked production of industrial goods across transnational supply chains that have many digitalized interfaces. This allows competitive operations in time, costs, and quality, which have been widely discussed. On the downside, it entails cyber threats with significant risks for society in areas including business, environment, and health. Hence, to adequately manage these risks in the emerging digital world, there is a vital necessity to raise awareness, establish, maintain, and further develop cyber-security measures to ensure an appropriate level of protection along the entire value chain and supply chain. Blockchain capabilities are introduced to improve the technical and organizational basis for secured operations in industrial networks. Its advantages are explained by a simple USB-device use case, that has often been the root cause to subsequent security incidents, especially in the Stuxnet incident.

Keywords Resilience · Cybersecurity · Enterprise · Supply chain · Digitalization · Industry 4.0 · Blockchain · USB · Stuxnet · Digital twin

1 Introduction

Since its inception, industry has been under relentless pressure to increase its efficiency, improve (and validate) product quality and, more recently, to minimize its impact on the environment. Automation and plant information systems have been instrumental in driving the significant advancements in this direction over the last few decades. More recently, the emerging integration of AI has further increased the sophistication and capabilities of digital environments. Such systems typically rely on access to data often across interconnected business entities. The same autonomous high-speed decision-making capability of AI systems that provide higher productivity can also propagate consequences of malware at unprecedented speed.

Cybersecurity has long been an issue in industry since the introduction of computers. The use of computers in automation (particularly the introduction of commodity operating systems into the factory floor) has extended cybersecurity risks deep into manufacturing facilities. The interconnection of automation networks and in particular the convergence and integration of Operational Technology (OT) and IT networks has further increased the cybersecurity risks and the probability of issues. The *Petya* and *WannaCry* ransomware attacks infested a huge number of systems worldwide in 2017. The adoption of Industrial Internet of Things (IIoT) devices results in the networked integration extending much deeper into devices (sensors, actuators, etc.), significantly increasing the degree of vulnerability and impact. Integrated Business-to-Business (B2B) systems both within transnational sections of a company as well as across integrated supply chains provide an unprecedented expansion of attack surface that spans separate companies and countries.

✉ Michael Lees
Michael.Lees@cub.com.au

Sebastian Gajek
Sebastian.Gajek@hs-flensburg.de

Christoph Jansen
Christoph.Jansen@hs-flensburg.de

[1] University of Applied Sciences Flensburg, Flensburg, Germany

[2] Carlton & United Breweries and The Department of Electrical and Electronic Engineering, The University of Melbourne, Melbourne, Australia

The advent of the Fourth Industrial Revolution and the push towards Industry 4.0 is accelerating the adoption of networked technologies. This impacts the entire enterprise control system hierarchy (Jansen and Jeschke 2018), and spans from IIoT-enabled devices through the digitization of company internal and external interfaces enabling interconnected transnational supply chain management.

One specific use case within a supply chain is the utilization of USB-stick devices in manufacturing automation infrastructures. Who assures that USB sticks are only used within a dedicated IT infrastructure, e.g., to update a certain software package on a production machine? Who can assure that this stick has only been used for the intended procedures on specific machines—along the entire life cycle of the device? Enterprise procedures, education of staff, and rules for selecting USB-stick suppliers can only be auxiliary measures as they still rely on human behaviour to identify, authenticate, and track devices in IIoT environments. A prominent illustration of this use case has been the Stuxnet attack that affected an Iranian facility handling nuclear substances. From an operator's viewpoint, a system is required that identifies, authenticates, and subsequently controls the access of the device throughout its entire lifecycle. The physical level of the hardware device has to be connected to an entity in the IT level, which addresses the concept of a digital twin.

Contemporary cybersecurity protection concepts (models, infrastructure, and approaches) have a number of limitations. Lees et al. (2018) state that "The current state of ICS cybersecurity defence (across most industry sectors) is arguably typically inadequate". In addition, the current infrastructure stack has a number of inherent vulnerabilities, some of them deep within established mechanisms. Although implementation of cybersecurity measures can never achieve total protection against cyber threats of any kind, it is of vital importance to understand the necessity of appropriate protection levels, including the ability of the target to recover. In an analogous reference to biological systems, this system feature is called cyber-resilience (Lees et al. 2018).

This paper presents an advanced protection mechanism based on blockchain, which identifies, authenticates, and subsequently controls the access of the device throughout its entire lifecycle, and hence significantly improves the inherent resilience of digitalized industrial business environments.

2 The digital world—the interconnection of architectures, systems, and supply chain organisations

Interconnections within Supply Chain organisations obviously pre-date the digital era. The difference is that in the digital world the interconnections are a lot faster, more efficient, and more plentiful. There are also many new categories of connection that did not exist prior to the digital world. Many of these are in relation to contemporary services such as third-party support and maintenance, software updates, and cloud-based services and data storage.

2.1 Connectivity, the industrial enterprise, and IIoT

Industry's relentless pursuit of growth, efficiency, and profitability has inevitably resulted in a drive for greater data analytics. The Industrial Internet of Things, which is an industry version of IoT, implemented across industrial automation infrastructure, has provided a pathway for sourcing the type and volume of data that is required to fuel the analytics. While industrial automation has long been providing data connectivity and visibility, using any number of fieldbus technologies, the IIoT has enabled a significant step change in data accessibility. The IIoT momentum has flooded the industrial automation market with Ethernet enabled devices that were previously non-networked (or connected via traditional fieldbus only). Among other things, Ethernet provides ease of integration, making data and information available across network boundaries. Recent advances and the convergence of a number of technologies—including IIoT, big data, cloud computing, and data analytics—have led to Industry 4.0 and the era where the concept of the 'smart factory' has become a serious aspiration.

There are a number of emerging themes that are transformative in their impact on the digital ecosystem of the enterprise. Some of the more prominent examples include:

1. Interconnection: Businesses are now undoubtedly more (digitally) interconnected with each other. Some of the dominant examples include: interconnection with each other across the supply chain, with cloud or platform services and with third-party infrastructure. All parties now have a greater dependence on the Internet.
2. Large-scale data: Automated data connectivity from the plant floor to corporate applications has existed for decades via traditional fieldbus technologies. However, the recent drive towards Industry 4.0 and interconnected business has contributed to the exponential increase in IIoT-enabled, vertically integrated devices.
3. Abstraction of platforms: The virtualisation of servers, platforms, and networks is largely an outcome of the quest to minimise capital and operating costs of operations. While it arguably exists independently, the drive for business interconnection and Industry 4.0 has accelerated the proliferation of these technologies (particularly in terms of off-site cloud platforms). The optimisation in footprint has often come at the cost of increasing sophistication (however, transparent to the user it may appear).

4. Mobile devices: The use of mobile terminals, tablets, and platforms of OT-related apps in the plant floor of the manufacturing enterprise have become increasingly common. Hence, networking is no longer solely controlled via physical media.
5. Bring your own device (BYOD): An organisation's opportunistic/parasitic use of equipment that it neither owns nor controls.

These emerging characteristics (among others) have collectively and significantly altered the topology of the digital ecosystem of the enterprise.

2.2 Supply chain

In the context of the contemporary manufacturing-based enterprise, the term Supply Chain typically refers to the collection of people, organisations, resources, and activities that are required to obtain raw materials, transform them into products of value, and distribute them to the customer. The term also (increasingly) encompasses Reverse logistics; the return of spent product components; and materials for reuse or disposal. More specifically, the term is used here in reference to manufacturing industries that rely on automation within networked facilities across transnational environments.

Within transnational companies, there are typically two categories of supply chain:

1. Product stream: Raw materials to customer (often also reverse logistics)
2. Support stream: Support services required for the company /infrastructure to function (e.g., maintenance and support from equipment suppliers and Original Equipment Manufacturers (OEM), external service providers: training, HR, IT, cloud host and third-party data analytic or AI platforms, building services, invoice/billing mechanisms, etc.)

The drive for increased business integration across the supply chain has a number of objectives, typically including:

- Efficiency: coordination of just-in-time production to minimise stock buffers
- Resilience and risk management: ensure that minimal stock buffers are sufficient; feasible contingency plans for supply of materials and services.

The developments in supply chain management result in significant and important alterations and expansions to the digital ecosystem of the enterprise.

Some of the significant implications include the expansion of the company's digital ecosystem. This could be either traversing the intracompany's footprint via the Internet, dependence on cloud infrastructures and providers, and, finally, the integration with the digital environments of other members of the supply chain.

There is an increased reliance on Internet between premises of the same company and between adjacent third-party companies and an increased level of trust in the security of infrastructure and platforms that are managed by others. Typical scenarios include:

- Within the same company (the same company policies and procedures) but subject to laws and regulations and cultures of a different country
- Between different companies (typically no visibility of policies, procedures).

In addition to this, there are a number of compounding factors including:

- Pace of change and adoption of new platforms
- Increasing sophistication (abstraction/virtual platforms and components)
- Lack of transparency of what is hosted (physical locations of data centres, and backup repositories of international cloud providers).

The changes to the digital ecosystem of the contemporary enterprise are substantial and the consequential emerging demands on cybersecurity are significant.

3 Cyber vulnerabilities of the digital interconnected supply chain

3.1 Cyber-resilience

Cybersecurity is a key consideration in the design of contemporary information systems. For many areas of industry, cyber-resilience is a non-optional component of business continuity and risk mitigation processes. The United States National Institute of Standards and Technology (NIST) have developed some concise definitions for cyber-resilience and cyber-resilient systems (Stouffer et al. 2015):

- "Cyber resilient systems have required security safeguards that are "built in" as a foundational part of the system architecture and design and that can withstand an attack and continue to operate "even in a degraded or debilitated state" to carry out essential functions."
- "...cyber resiliency, which is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cybersecurity resources."

In addition to malware immunity, this, of course, includes such considerations as: resilience by design, redundancy, and disaster recovery planning and systems.

Estimates of the annual economic impact of cybercrime vary. However, two things that are apparent are: the estimates are large and that they tend to increase year on year. The IBM sponsored report "2018 Cost of a Data Breach Study" by Ponemon (2018), reported that the "global average cost of a data breach is up 6.4% over the previous year to $3.86 million.".

Today's supply chain is arguably less resilient against cyber-incident induced downtime due to a number of reasons, including:

1. Globalisation/consolidation of production facilities: Globalisation of production facilities and, thus, consolidation within multinational corporations typically provide less alternative options during times of interruption.
2. Lean and progress towards Manufacturing Excellence: Through the systematic elimination of (all) forms of waste within operations, programs of Lean Management and Manufacturing Excellence have a side-effect of effectively reducing the disturbance rejection capabilities of the supply chain. Just-In-Time (JIT) stock management has minimised stock-holding costs at the expense of minimal (if-any) stock buffer. This has also shortened the time to flow-on impact to adjacent companies. A major portion of industry are now participating in some form of Manufacturing Excellence program journey.
3. Joint vulnerability—shared consequences: In a JIT/Lean supply chain, all participants are vulnerable to any interruption to supply chain workflow. The supply chain is only as strong as its weakest link. All members have business interest in the cyber-resilience of other members in the supply chain.

3.2 Cyber-resilience requirements of enterprises

3.2.1 Key cyber-resilience challenges of the emerging digital ecosystem

In manufacturing environments, physical machines (e.g., production machines, or machine tools) are important assets, which are quite often crucial to the whole production process. Failure of operations might affect the output of an entire production line. The addition of contemporary automation infrastructure to these machines brings with it an IT layer that opens up the conceptual space of networked cyber-physical systems (Jansen and Jeschke 2018). Business impact analyses of cyber-incidents often bring out these machines as critical assets.

Internet connection of machines became common largely due to cost saving opportunities for OEMs during maintenance. Hence, advanced protection measures need to be applied that take additional inter-company data transfer requirements into account.

Transnational premises, third-party interaction, and cloud services have resulted in data pathways that can re-enter the Internet multiple times during the journey from source to destination. This results in complex, re-emergent pathways of data through the Internet and private networks.

The attack surface has dramatically expanded, resulting in a new scale of challenges within the emerging digital ecosystem:

1. Depth of vertical integration
2. Volume of IIoT devices
3. Previously non-networked devices
4. Maintaining currency of patches and software/firmware updates.

It is important to note that the boundaries between IIoT and IoT are conceptually overlapping. To give an example: inadvertently used commodity smart light bulbs within IIoT process cells on the shop floor can unintentionally introduce additional vulnerabilities into the process cell's control system.

The emerging digital ecosystem clearly segregates accountability and the ability to effectively control digitalized systems and processes to their full extent. Obvious examples are (1) the usage of third-party platforms and cloud providers, (2) BYOD strategies/ acceptance, and (3) interdependent and shared accountability within the supply chain. Such boundaries can present significant challenges when purging an infection.

Hosting network nodes of distributed ledgers and maintaining the security of digital interfaces require a different category of responsibility and consequences, e.g., for product tracking and tracing. It typically comes along with more sophisticated protocols such as blockchain.

OEMs often require remote access deep into the automation layer of their customer's plant control network to provide the required/contracted maintenance services to the equipment that they have supplied. If these kinds of maintenance services are delegated to a third party, adequate protection becomes more complex. A specific type of supply chain deals with the supply of IT security services, as described in Jansen and Jeschke (2018).

Besides the service level, the supply chain (in terms of material flow) provides additional complexity: The handling of any data in conjunction to the flow of material or goods like specifications or documentation has to be agreed upon and managed, complying to the most advanced protection concept. The supply chains within some industries (such

as automotive) contain players that have sufficient dominance to define the cyber-protection rules and requirements to which the other players must adhere.

3.2.2 Vulnerabilities

Vulnerabilities of digitalized enterprises are weaknesses that can be exploited by attackers to perform unauthorized actions within the IT/OT systems. Dominant categories of vulnerabilities and constraints include technical vulnerabilities, compliance, and resourcing.

Technical vulnerabilities encompass deficiencies within the existing state-of-the-art. They are related to assets like hardware, firmware, software, or networks.

Compliance is addressing the availability and adherence to policies and procedures for any IT/OT processes. It closely connects technical assets and humans by organizational means.

Resourcing aims at achieving and sustaining best-practice compliance. It requires the ability (and capacity) to adequately implement security measures both initially as well as to relentlessly adhere to required update cycles, e.g., patching of software and firmware.

In the context of this categorisation, the attack vector of malicious USB devices is a technical vulnerability. Existing defence measures typically rely on human compliance and administrative processes. It has to be noted that relying on compliance is neither sufficient nor sustainable (Tischer et al. 2016). The impact of a successful attack can be amplified in insufficiently resourced environments where patching and software updates are not up-to-date.

4 Cyber-resilience strategies and tools for managing risks in the emerging digital world

The frequency, scale, and impact of cyber-incidents illustrate that contemporary progress towards cyber-resilience is largely insufficient and is lagging both the traditional and emerging vulnerabilities within the industrial manufacturing landscape.

4.1 Protecting the enterprise's digital ecosystem

A number of standards, guidelines, best practices, and maturity models have been developed to help the enterprise to maximise its cyber-resilience and to protect its digital ecosystem. In this context, there are two dominant categories of vulnerability that still exist in practice:

1. Inadequate implementation and adherence to existing state-of-the-art: While standards, guidelines, and maturity models have existed for some time, they are all too often not followed or implemented correctly (Lees et al. 2018). As would be expected, the financial impact of cyber crime has been found to vary in proportion to cyber-security maturity (McAfee 2019). Excuses for lagging compliance (be they inadequate resourcing or lack of awareness) are of little consolation following a cyber-security incident.
2. Deficiencies within the existing state-of-the-art: There is a specific class of yet to be discovered (and hence currently unpatchable) zero-day vulnerabilities. These vulnerabilities are inherent in existing technologies, protocols, and hardware, and could only be downscaled by well-established components to minimize the attack surface.

4.1.1 Contemporary state-of-the-art

Industrial manufacturing facilities with a contemporary level of automation require adequate protection from cyber threats. Given the different levels of automation, this protection ranges from office level to field level. A range of standards, frameworks, and guidelines exist including:

- ANSI/ISA 62443 (Formerly ISA-99): A standard for the implementation of electronically secure Industrial Automation and Control Systems (IACS) (ISA 2016)
- National Institute of Standards and Technology (NIST): A framework or guideline for securing Industrial Control Systems (Stouffer et al. 2015)
- The MITRE Corporation: A set of cyber-resiliency design principles (Bodeau and Graubart 2017).

4.2 Entry points for malicious code—managing the USB threat vector

The Universal Serial Bus (USB) is a protocol that defines an interface for the interconnection of peripherals and devices. Its performance and ease-of-use have resulted in its ubiquitous deployment across computer systems from servers to plant controllers and IIoT devices.

4.2.1 Risk of USB as an attack vector

While USB has been a known attack vector for some time, in 2018, Honeywell have reported some interesting research findings (Honeywell Process Solutions 2018). In an experiment spanning 50 locations across 4 industries (and 4 continents), USB-based malicious (or malware related) code was detected and blocked at 44% of the locations. One in four of the detections that were blocked "... had the potential to cause a major disruption to an industrial control environment, including loss of view or loss of control, and 16% were

targeted specifically against Industrial Control System (ICS) or Internet of Things (IoT) systems." Interestingly, 9% of the discovered malware was specifically designed to exploit weakness in a USB protocol or interface.

4.2.2 Probability of security breach

If there is a perception that USB devices can be 'controlled' with policy, then what is the likelihood of a security breach? In an experiment with 300 USB flash drives, Tischer et al. (2016) verified the assumption that users will simply and reliably pick up and plug in flash drives that they find. Astonishing 45–98% (depending on how they were labeled) of deliberately 'dropped' USB drives were connected (one of them within just 6 min) (Tischer et al. 2016). In this context, the apparent air gap is not so insurmountable.

4.2.3 Consequences

Quite a number of potent malware variants have been found to propagate across USB including: Stuxnet, Mirai, TRITON, and WannaCry (Honeywell Process Solutions 2018). The consequences of such a breach in an ICS environment can range from physical damage to equipment through to the financial implications of extended periods of production downtime. "USB represents an even greater threat than spreading malware: a USB device can be used to attack systems directly, using the USB interface as a powerful attack vector. Ever since the Stuxnet attack used a USB flash drive to obliterate any semblance of an air gap in an Iranian nuclear facility, the industry has been well aware of the vulnerability that USB devices can introduce to their operations." (Arampatzis 2018)

4.2.4 Solutions

Attempts to improve the vulnerabilities of the USB attack vector have taken a number of directions. Some of the prominent examples include:

- Policy management: Company policies are often set in place to shape human behaviour as well as electronic policies to disable USB ports via active directory
- Commercial products: As an example—Honeywell have developed a Secure Media Exchange (SMX) product "System and method supporting secure data transfer into and out of protected systems using removable media"
- Patents: A number of relevant patents exist including "Using a USB host controller extension for controlling changes in and auditing USB topology" "The invention provides systems and methods for protecting computer systems from attacks that attempt to change USB topology and for ensuring that the system's information regarding USB topology is accurate." (Avraham et al. 2019)

Yet, the ubiquitous USB is still a significant cyber-security vulnerability.

4.3 The case study: Stuxnet

The air-gap defence (or perception of its defence) is often relied upon as a component of a cyber-protection strategy of a critical network. One of the reasons that USBs are a significant cyber-security target is their potential to cross the air gap. One of the most prominent examples of this was the Stuxnet worm.

4.3.1 A brief introduction to Stuxnet

Stuxnet was an advanced worm that was designed to target specific industrial control system technology (Matrosov et al. 2019; Langer 2011). While several variants exist, it made use of four zero-day Microsoft vulnerabilities and contains a PLC root kit. In a suspected operation against critical infrastructure in the Iranian nuclear program, it was applied in a semi-targeted attack that had an impact on the Natanz Fuel Enrichment Plant (infecting Siemens SCADA software and Siemens S7-417 PLCs). It was first discovered in 2010.

Stuxnet was specifically designed to damage centrifuges that are used for Uranium enrichment. While it has not been confirmed, Stuxnet is believed to have been responsible for damage to 1000 centrifuges (Brown 2011), significantly slowing down the Iranian nuclear program. As the first discovered malware that targets industrial control systems, it has irreversibly changed the cybersecurity world.

4.3.2 The role of USB in Stuxnet

USB enabled Stuxnet to traverse the air gap and access the control network in the Natanz Nuclear enrichment plant in Iran. According to Langer (2013) "Whatever the cyber-security posture of contractors may have been, it certainly was not at par with the Natanz Fuel Enrichment facility. Getting the malware on their mobile devices and USB sticks proved good enough as sooner or later they would physically carry those on site and connect them to the FEP's [fuel enrichment plant's] most critical systems, unchallenged by any guards."

4.3.3 Pathways for managing the USB entry point

It is clear that a reliable and effective means of managing access and control of USB device is required. The ability to restrict USB access to a set of company internal devices that are tightly controlled would help to reduce the

USB-associated vulnerability within an attack surface. This is not so easy to do with the existing USB devices as they are clonable making it difficult to police the software content and the hardware component concurrently and to confirm that they have not been separated. To manage and control a USB device, a means of binding the hardware with its digital twin is required. Once this is achieve, a means of authentication to confirm that the binding is correct and valid is also required.

4.3.4 Digital twin

A digital twin is a digital representation of a physical object, process, or system, and it can exist in many forms. Digital Twin in the human context is all the data footprint that we as humans create through our attributes and interactions. Attributes are core data that make up what we are, including name, age, gender, address, ethnicity, education, salary, etc. Interaction refers to all the data and footprint that is created when we interact with the external world. The term Digital Twin, therefore, can be loosely applied to any form of digital representation.

The concept of a digital twin may be applied to physical objects, as well. The vision of the Digital Twin is depicted as "a comprehensive physical and functional description of a component, product or system, which includes more or less all information which could be useful in all—the current and subsequent—lifecycle phases" (Boschert and Rosen 2016). Typically, the digital twin has some cryptographic identity linked to a digital certificate summarizing the attributes and properties of the physical object. The fact that a physical object has a cryptographic identity facilitates the authentication of the physical object, proof of ownership, tracking, and tracing.

5 Blockchain-based solution approach

5.1 A primer: decentralized ≠ distributed

The blockchain is a promising technology that recently received much attention in industry and academia. The reason is that the blockchain technology changes the way that computation occurs and revolutionises the design and implementation of computer networks, most notably the Internet. In a nutshell, the blockchain technology stands for the paradigm shift of moving from a centralized computing network infrastructure to a decentralized one. The canonical example for a centralized infrastructure is cloud computing. While, in general, cloud architectures are distributed over multiple computing nodes, they are owned, managed, and governed by a single authority. Hence, the central authority has full control over the infrastructure. The data and events which the authority receives, processes, and generates are typically relied upon for continued plant operation.

Enterprises need—by assumption—to trust the infrastructure. Trust is a critical factor in cloud computing; in present practice, it depends largely on perception of reputation and self-assessment by providers of cloud services (Huang and Nicol 2013). However, the lack of methods to quantify and verify reputation and self-assessment makes trust a fragile foundation for sustainable and robust IIoT cyber-resilience methodologies. This is a severe problem for many IIoT corporates and service providers, as the lack of trust raises security, privacy, and reliability issues (Jansen 2011). On the other hand, trust becomes a dominant requirement in future emerging IIoT use cases, as the trend is to open up industrial automation networks and services. Future emerging business models require collaboration of potentially competing and distrusting entities. Consider, for example, the emerging use case where industrial robot maintenance data are sold to some third-party AI-empowered data analytics service. For such a use, case trust is an ultimate prerequisite to attain a prolonged and stable business model. Centralized or distributed technologies are incapable of achieving trust beyond the internal security perimeter, as—by design—they are under the control of a single authority.

5.2 The blockchain trustlessness

At the bottom of blockchain technologies stands the idea of trustless decentralization. The approach leverages the democratization of centralized computing networks, applications, and services. Instead of a single authority being responsible for the computation, the blockchain network consists of multiple, independent entities (nodes) computing the same task. What the network relies on is a mechanism to agree on the common truth of the outcome of the task known as consensus (Lamport et al. 1982). Due to network latencies, faults and crashes a node's local state can deviate from the global view of the common state of all other nodes. A key property of the consensus mechanism is to ensure all nodes are in sync and share the same local state. Implicitly, a consensus guarantees the soundness of the computation, as a quorum is required to accept the common truth. As long as the majority of the nodes agree on the outcome, the minority will sync with the view. In other words, the blockchain carries over the principles of democratism to the world of computation.

While the redundant computation of the task by multiple, potentially malicious nodes leads to significant overhead, it also leads to a trustless infrastructure: despite the distrust between the nodes, the susceptibility of nodes to cyberattacks, or the presence of a coalition of nodes aiming to game the outcome, the network achieves the correct

result (in the sense of the quorum). That paradoxical property of trustful agreement in the light of untrusted entities is a fundamentally novel computing paradigm, which has not been achieved with prior consensus mechanisms in that full dimension. To be a bit more precise, one classifies blockchain technologies into two groups according to the underlying consensus mechanism. In a private blockchain, sometimes referred to as Enterprise Blockchain, the number of nodes is known in advance and is typically fixed, while in a public blockchain nodes can go online/offline at any point in time. Example mechanisms belonging to the first category are Lamport (2011) and Kotla et al. (2009), while Proof of Work (Nakamoto 2008) and Proof of Stake (Kiayias et al. 2017) are examples for the second category. Moreover, consensus mechanisms differ in the number of nodes covering the blockchain network, effectiveness to perform the consensus (scalability), costs related to transactions, and universality of the smart contracts. Blockchain technologies also vary in the computational task which they agree upon. Looking at the evolution of blockchain technology, we identify three variants.

5.2.1 Blockchain as a storage

One of the first applications of blockchains are decentralized storage mechanisms. In contrast to distributed databases, no single administrator exists that orchestrates the databases and their replicas. The fact that the data are stored over multiple, independent nodes, each representing a different organization or trust entity, has the advantage of being significantly more cyber-resilient against internal or external cyberattacks. Blockchains have the unique property of immutability. The data cannot be erased, manipulated, or overwritten for the lifetime of the blockchain.[1]

5.2.2 Blockchain as a payment

Probably, the task which has led to the rapid proliferation of blockchain technologies is the application to cryptocurrencies. A bank implements a centralized database and maintains accounts associated with its clients. Loosely speaking transactions are updates in the database of the sender's and receiver's account, which apply digital signatures to approve and validate the transaction. A blockchain can implement the same functionality without the need of a centralized, trusted bank. In fact, each customer may become the bank by hosting its own blockchain node, thus decentralizing the bank and sharing the trust among the network.

5.2.3 Blockchain as a distributed computing platform

Generalizing the above ideas, the nodes execute any program not only limited to a payment transaction and agree upon the outcome. This leads to a trustless, distributed computing platform with the following advantages: No entity owns the platform and controls the outcome of the computation. In comparison to the existing cloud computing platforms, computation becomes not only more fault tolerant, but the correct result is independently verified by the network.

5.3 Blockchained digital twins

Creating a Digital Twin within a Blockchain is not different from the standard approach. The manufacturer of the physical object issues a cryptographic identifier. The corresponding certificate attesting the objects attributes is stored in the blockchain. Here, the immutability property of the blockchain ensures the integrity and verification of the certificate. Once stored in the blockchain, no party has the opportunity to modify the digital identity of the physical object. In an interconnected enterprise, this approach can lead to improvements of various standardized tasks. Sharing information about manufacturing process, assembly, delivery, and maintenance of products with suppliers and vendors becomes transparent. The blockchain serves as a common ground for suppliers and vendors for their Digital Twins. Not only do they benefit from a common view of all twins and the processes which they are involved in, they may also leverage the common view to detect and exclude fraudulent devices harming a sustainable supply chain. As a direct consequence tasks such as assigning or verifying certifications or certain properties of physical products becomes easier. Also origin and ownership claims are clear and subject to a common understanding between supply chain nodes. All supply chain nodes may derive at any point in time the truthful view of the object, track, and trace the purchase orders, change orders, receipts, shipment notifications, or other trade-related documents.

5.4 Thwarting the Stuxnet attack

Regardless of the application, blockchain technologies offer sustainable supply chains versatile advantages. Let us elaborate on the advantages in the Stuxnet case. Suppose that the USB stick has a Digital Twin, represented by a unique, unclonable cryptographic identifier.[2] The certificate mapped

[1] Technically, this is achieved by writing each entry into a block linked to the previous block containing a link to all previously written entries. Hence the name blockchain.

[2] Physical Unclonable Functions (PUFs) empower the realization of a hardware identifier. Due to the unique physical properties of the hardware implementation, PUFs are unclonable. The replication of a PUF would require replication of the hardware material at a level of granularity that is currently considered to be technically infeasible.

to the identifier is stored in the blockchain. This way, virtually, any number of participants, accessing from any number of touchpoints, have access to the information on the blockchain, including a register of legitimately created USB sticks. None of the parties can modify the blockchain entry and, for example, inject a malign Digital Twin without the consent of the network. To increase trust and eliminate the bias in today's opaque supply chains, one could document the journey of the USB stick across the "blockchained" supply chain during its production, trace the transfer of ownership, and the instalment of firmware on the stick. With the information on the blockchain, participants have a common understanding about the content and ownership of the USB stick. Smart contracts can codify rules to eliminate the possibility of storing Digital Twins whose journey is noncompliant with the security policy of suppliers and vendors. An IIoT machine or any other USB-enabled digital device would now require authentication against the Digital Twin's identity on the blockchain (including compliance check with security policy) to interact. Failed authentication would prevent propagation of Malware, as an infected USB device would be denied connection through the interface. No key management and revocation has to be installed at the machine, as it only has to look up the twin's identity in the blockchain. In the negative case, the machine rejects to read from the USB device and avoids installing the software.

5.5 Blockchained (dis-)incentive mechanism: the case of curated registries

Stuxnet serves as a running example for malware attacks. The attack and related cyber attacks share one notion. There is a strong incentive to commit the attack. In the case of Stuxnet, the motivation may have been the delay of a nuclear war (Brown 2011). In general, the attacks are motivated by personal or political enrichments. Analysing the scenarios from a game-theoretic angle, the incentives to put the attack in execution outvote the disincentives. Reasons include the inability to technically trace the origins of the attacks due to the anonymity of the Internet or the lack of criminal proceedings over multiple legislatures. Cyberattacks are economically asymmetrical. The costs to implement, for example, malware and propagate it through the Internet stand in no relation to the costs resulting in their damage (for example, Industroyer shut down Ukraine's power grid in December 2016).

Another useful (less publicised) characteristic of Blockchains is the ability to design protocols and applications based on incentive strategies. Although a token is a sequence of bitstrings along a digital signature, it is widely accepted as an object with value. It can be traded and exchanged for fiat. A strong ecosystem already exists for turning tokens into assets and it has proven to work. In addition, the blockchain network offers the necessary infrastructure to implement the enforcement of (dis-)incentive strategies through smart contracts. It shows that participants follow rational behavior and strive to maximize their utility quantified in tokens. With the blockchain comes a new opportunity to (re-)design protocols, applications, and services for interconnected Enterprises. The high-level idea behind it follows a staking and slashing mechanism. By staking, we mean the mechanism of locking the tokens as collateral to backup a future decision, event, or action. In the previous section, we described how a Digital Twin is created in the blockchain and its journey is trackable and traceable. Suppose now, each party in the supply chain is asked to deposit some token collateral for its tasks, actions, or events it creates. The party is challenged for the proposal to accept the activity in the supply chain by a group of validators who co-stake, each validator with an amount of tokens proportional to the size of the group, and verify the proposal. By a majority decision, the stake of the parties deviating from the quorum is slashed among the majority. This implies that the proposer fortifies her stake in case of a correct proposal. However, she loses her stake in case of a dishonest proposal.

Analyzing the mechanism, we observe that the proposer is incentivized to make an honest proposal from which all supply chain nodes benefit. Otherwise, she loses her stake. Furthermore, she has a natural incentive to volunteer. Validators have the incentive to vote honestly as they risk losing their stake in the event of a decision against the quorum. The fact that they potentially receive a reward is an incentive to engage in the validation process.

6 Discussion

A cardinal question remains. Could the application of blockchain potentially have stopped Stuxnet? To answer the question, one needs to look deeper into the infection vector. The attack exploited vulnerabilities on two fronts. The first is related to lack of human authentication. The networks of many industrial factories (especially top secret nuclear facilities and other critical infrastructures) are not connected to the Internet, making it much harder to introduce malware to the system from the outside. The attacker thus had physical access to a computer in the Intranet of the uranium enrichment facility. From here on, Stuxnet propagated to the other computers with the goal to reach the computer running the industrial control application.

Humans are known to be the weakest link in a security system. The presence of blockchain technologies would not have helped to stop a human from perpetrating the attack.

The second front is related to the lack of device authentication. Present computer systems lack the ability to authenticate an external USB device. Looking at the USB standard,

no cryptographic measures have been implemented to authenticate devices. Hence, any device may access the universal serial bus to connect to the computer. The conclusion is that the implementation of device authentication mechanisms would have already thwarted the Stuxnet attack from propagation and infiltration of other computers, provided that USB devices have a Digital Twin to cryptographically authenticate the device.

A problem remains. How does the computer know it shall grant a particular USB device access, while rejecting other USB sticks. Given the large number of USB manufacturers and owners it is merely infeasible to implement for each computer an access control list locally. A look-up in a database is, however, a technically promising and practical approach. As argued before, a centralized or decentralized database is under the control of a single entity. If corrupted, the entity might manipulate entries in the database, add certificate of malign digital twins, and this way allow the circumvention of any access control mechanism in place. Storing the Digital Twin's certificate in the blockchain and adding track and trace information of the journey from the device manufacturer to the owner give the required level of security.

To conclude, Stuxnet and related attacks in general can be thwarted when a blockchain is in place. A prerequisite is the ability to implement unclonable Digital Twins and ensure that the blockchain mirrors the Digital Twin.

7 Conclusion

The advancement and proliferation of IIoT, at deep automation device level, has increased the attack surface and vulnerability of the contemporary enterprise. The adoption of AI and machine learning technologies means that the associated analysis and decision-making capabilities place an even greater reliance on the resilience and integrity of the IIoT connectivity. Transnational supply chain integration means that the vulnerabilities are no longer as contained as they once were. With integrated B2B networking the supply chain is almost the one entity and its cyber-vulnerability has evolved accordingly. The contemporary just-in-time supply chain is only as strong as its weakest link.

Existing cybersecurity protection methods are arguably inadequate for managing the risks in the emerging digital world. They are often not implemented as designed and hence fail to achieve full benefit. There are also some significant fundamental technical weaknesses in the infrastructure stack such as USB devices.

There is an opportunity to reduce some of the cybersecurity vulnerabilities by redesigning key elements of the stack. This paper presents a method for positively identifying and managing USB sticks using a mechanism based on blockchain. The proposed solution also enables the entire history of a USB stick to be tracked and stored in the blockchain making it available for use during automated access decisions (pre-connection device authentication). This enables the realistic development of a managed segregated USB system that is independent of human (non-)compliance. It provides a significant improvement in reducing the Malware risks that have long been inherent in USB devices. Further research is recommended to demonstrate the technical feasibility of implementation (for USB device management) in a factory environment.

Acknowledgements The first author's work is supported by the EU H2020 project FENTEC (Grant no. 780108). The authors would also like to thank the management of Carlton & United Breweries for permission to publish this work.

References

Arampatzis A (2018) USB threats to cybersecurity of industrial facilities. https://www.tripwire.com/state-of-security/ics-security/usb-threats-cybersecurity-industrial/. Accessed 25 Feb 2019

Avraham I, Ray K, Williams M, Wooten DR (2019) United States Patent No. US7761618 B2, July 20, 2010. http://patentimages.storage.googleapis.com/pdfs/US7761618.pdf. Accessed 10 Feb 2019

Bodeau D, Graubart R (2017) Cyber resiliency design principles. Technical report. The MITRE Corporation. https://www.mitre.org/publications/technical-papers/cyber-resiliency-design-principles. Accessed 27 Jan 2018

Boschert S, Rosen R (2016) Digital twin—the simulation aspect. Springer, Berlin, pp 59–74

Brown G (2011) Why Iran didn't admit Stuxnet was an attack. JFQ (63). SSRN. https://ssrn.com/abstract=2485181. Accessed 19 Feb 2019

Honeywell Process Solutions (2018) Honeywell Industrial USB Threat Report: Universal Serial Bus (USB) threat vector trends and implications for industrial operators. https://honeywellprocess.blob.core.windows.net/public/Support/Customer/Honeywell-USB-Threat-Report.pdf. Accessed 18 Feb 2019

Huang J, Nicol DM (2013) Trust mechanisms for cloud computing. J Cloud Comput. https://doi.org/10.1186/2192-113X-2-9

ISA (2016) The 62443 series standards—industrial automation and control system security. Revised December 2016. https://cdn2.hubspot.net/hubfs/3415072/Resources/The%2062443%20Series%20of%20Standards.pdf

Jansen WA (2011) Cloud hooks: security and privacy issues in cloud computing. In: 44th Hawaii international conference on systems science (HICSS-44). IEEE Computer Society, Koloa, Kauai, HI, USA, pp 1–10. https://doi.org/10.1109/HICSS.2011.103

Jansen C, Jeschke S (2018) Mitigating risks of digitization through managed industrial security services. AI Soc 33(2):163–173. https://doi.org/10.1007/s00146-018-0812-1

Kiayias A, Russell A, David B, Oliynykov R (2017) Ouroboros: a provably secure proof-of-stake blockchain protocol. In: Advances in cryptology—CRYPTO 2017–37th annual international cryptology conference, Santa Barbara, CA, USA, August 20–24, 2017. Proceedings, Part I, pp 357–388. https://doi.org/10.1007/978-3-319-63688-7_12

Kotla R, Alvisi L, Dahlin M, Clement A, Wong EL (2009) Zyzzyva: speculative byzantine fault tolerance. ACM Trans Comput Syst 27(4):7:1–7:39. https://doi.org/10.1145/1658357.1658358

Lamport L (2011) Byzantizing Paxos by refinement. In: Distributed computing—25th international symposium, DISC 2011, Rome, Italy, September 20–22, 2011. Proceedings, pp 211–224. https://doi.org/10.1007/978-3-642-24100-0_22

Lamport L, Shostak R, Pease M (1982) The byzantine generals problem. ACM Trans Program Lang Syst 4(3):382–401

Langer R (2011) Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur Priv 9(3):49–51. https://doi.org/10.1109/MSP.2011.67

Langer R (2013) To kill a centrifuge—a technical analysis of what Stuxnet's creators tried to achieve. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf. Accessed 20 Feb 2019

Lees M, Crawford M, Jansen C (2018) Towards industrial cybersecurity resilience of multinational corporations. IFAC PapersOnLine 51(31):756–761. https://doi.org/10.1016/j.ifacol.2018.11.201 (Proceedings of the IFAC international conference on international stability, technology and culture, Baku, Azerbaijan)

Matrosov A, Rodionov E, Harley D, Malcho J (2019) Stuxnet under the microscope. http://daveschull.com/wp-content/uploads/2015/05/Stuxnet_Under_the_Microscope.pdf. Accessed 18 Feb 2019

McAfee (2019) The economic impact of cybercrime—no slowing down. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf. Accessed 18 Feb 2019

Nakamoto S (2008) A peer-to-peer electronic cash system. White paper

Ponemon (2018) 2018 Cost of a data breach study. https://www.ibm.com/security/data-breach?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US. Accessed 25 Feb 2019

Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A (2015) Guide to industrial control systems (ICS) security. http://dx.doi.org/10.6028/NIST.SP.800-82r2. Accessed 21 May 2018

Tischer M, Durumeric Z, Foster S, Duan S, Mori A, Burstein E, Bailey M (2016) Users really do plug in USB drives they find. In: IEEE symposium on security and privacy (SP). IEEE Computer Society, San Jose, CA, pp 306–319. https://doi.org/10.1109/SP.2016.26