systems

MDPI

Concept Paper

Realizing the Role of Permissioned Blockchains in a Systems Engineering Lifecycle

Demetrios Joannou [1,*], Roy Kalawsky [1], Miguel Martínez-García [1], Chris Fowler [2] and Kevin Fowler [2]

[1] Advanced VR Research Centre, Loughborough University, Loughborough LE11 3TU, UK; r.s.kalawsky@lboro.ac.uk (R.K.); M.Martinez-Garcia@lboro.ac.uk (M.M.-G.)

[2] Airbus, Pegasus House, Aerospace Ave, Filton, Bristol BS34 7PA, UK; chris.fowler@airbus.com (C.F.); kevin.fowler@airbus.com (K.F.)

* Correspondence: d.joannou@lboro.ac.uk

Received: 28 September 2020; Accepted: 29 October 2020; Published: 3 November 2020

Abstract: A key requirement for an integrated digital tool chain is secure access and control of data assets. Not all stakeholders will have the same access to or control over the flow of information, some will be able to input or change data whilst others will only be able to read the data. Simply providing secure access protocols is not sufficient because copied data can quickly become disassociated and modified from its original instantiation, leading to its reuse elsewhere or later in the lifecycle but in an inappropriate way. Therefore, data management mechanisms are required that capture information about the data along with any decisions or modifications it has undergone during the course of its life, thus providing complete traceability for later validation purposes. This undertaking is essential across the systems engineering lifecycle. This pursuit involves controlling who can access and modify data within the lifecycle. This paper describes a solution to this by the introduction of blockchain technology, a relatively new technology that allows digital information to be distributed but not copied, making it an immutable set of time-stamped data managed by a network of connected systems and services. Though blockchain technology is not commonly referred to when discussing Industry 4.0, the technology's capabilities should add value when applied in a context of data management and security within the lifecycle of a product or services and in conjunction with digital twins, big data, and IoT. This paper describes how permissioned blockchains can be implemented within a systems engineering lifecycle, providing example architecture patterns showing how data provenance can be maintained throughout.

Keywords: blockchain; digitalization; Industry 4.0; permissioned blockchain; systems architecture; systems engineering

1. Introduction

Over recent years there has been a strong drive towards increasing interconnectivity between products, systems, and services, to provide enhanced or new capability that does not exist in any one individual element. A class of systems engineering known as systems-of-systems (SoS) engineering (SoSE) [1] emerged to deal with the subtleties of creating systems that behave as a collective where constituent systems (CSs) exhibit operational/managerial independency and/or several of the other defining characteristics of an SoS [2]. This interconnectivity can be tightly or loosely coupled depending on the manner in which the CSs interact to achieve the overall SoS mission. Establishing SoS increases the overall complexity of the interactions and information sharing between the CSs, where there are likely to be many different stakeholder interests that have to be considered and these may have different requirements at different stages of the SoS lifecycle. A consequence of this is the need to manage the flow and control of digital information between individual stakeholders and systems. This leads to a significant increase in information, data types, disciplines, and organizational boundaries, which will need to be dealt with by engineers. From a systems engineering (SE) perspective, these challenges would typically be addressed by a systems architect [3], whose role would be to oversee and direct the development of systems, products, and services throughout the lifecycle. In the context of an SoS, the inherent complexities make the challenge of managing and securely controlling information and data throughout a products lifecycle of upmost importance. The development process must provide trusted traceability of key data so that its history is preserved, and all changes are recorded in an immutable form. For complex systems, there may be stakeholders who need to simply access data, although some may wish to submit data or modify existing data. Therefore, there is a requirement for a data management system to allow for the following user types; publishers, subscribers, or both publisher and subscriber. Additionally, there is an obvious requirement for managing access to ensure right of access is carefully controlled and illegal access is prevented. This involves management of data and information across the entire lifecycle; ensuring the correct data is available for those who need it, at the right time and in the appropriate format, for a specific task.

Developing a systems architecture [4,5] is common practice [1] in the development process of an engineered product and forms the basis of a relatively new paradigm known as model-based systems engineering (MBSE). The systems engineer architects the system using models and to test iterative developments of a system prior to implementation; verifying requirements and validating the intended evolutions. Recent advancements in MBSE are regarded as a solution to managing complexity and guiding the development of systems throughout their lifecycles [6]. It has been reported [6,7] that MBSE has the potential to cope with the vast amounts of data associated with the development of products, systems and services, and testing of alternative design options. This involves:

(i) data access and control;
(ii) managing vast volumes of information and data, and;
(iii) using information and data effectively in an SE development process.

Whilst there are many well-known mechanisms for controlling data access, it is the need for maintaining an immutable record of data access/changes that is particularly challenging. This paper proposes a solution to this, which is the introduction of blockchain technology, a relatively new technology that allows digital information to be distributed but not copied, making it an immutable set of time-stamped data managed by a network of computers. The technology has advanced since its creation by Satoshi Nakamoto [8] over a decade ago, where it was proposed as a solution to structuring transactions and avoiding double spending. Lessons can be learnt from current work on implementing blockchain and other distributed ledger technologies (DTL) [9,10], particularly in developing specific architectures for cloud-based manufacturing and to recognize the importance of identifying all the end users of the system for security purposes. It has been reported that more simulation efforts are required to provide a realistic evaluation of proposed blockchain architectures in manufacturing applications.

The core notion of a blockchain is the ability to store data (essentially a database/ledger) across a distributed set of computers linked together (Figure 1), that does not depend on a centralized server to store data. The distinct advantage of a distributed ledger is that it provides a higher degree of data security, transparency, accuracy, transactional freedom, and raises the level of trust. Whereas traditional database networks (client-server networks) depend on a central authority to manage/maintain data, defining administration rights and permissions, the blockchain architecture imposes that all participants within the network approve and update new entries via a consensus algorithm [11]. The data cannot be altered without the consensus of the whole network, ensuring all records are valid after being verified by the network. This paper shows how a specific form of blockchain technology known as permissioned blockchains can overcome the data challenges within complex SE processes. Examples of such challenges come from commonly used centralized database systems that struggle with data security, availability and flexibility.

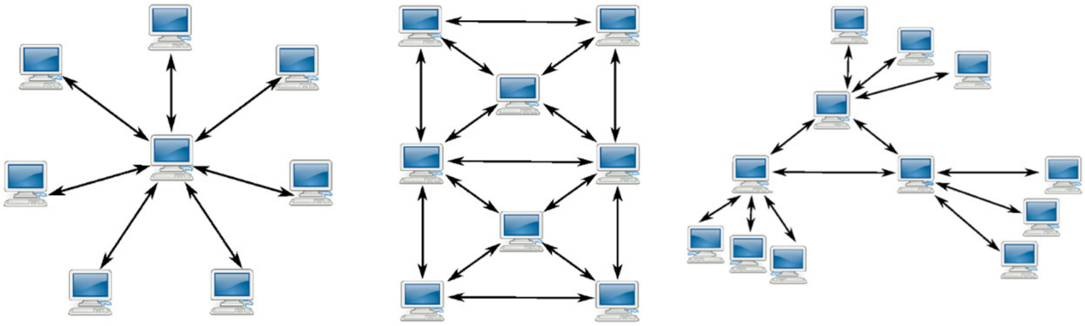

Figure 1. Distributed architecture of blockchain (right image) (left, centralized; centre decentralized).

This paper provides an initial introduction to blockchain and an overview of current uses of blockchain in different domains in Section 2. Section 3 goes on to describe the specific technical aspects of blockchains and more specifically permissioned blockchains, comparing the blockchain types and providing the rationale for their use within a SE context. Section 4 of and Section 5 of the paper focus on the role and implementation of permissioned blockchains within a SE lifecycle, respectively, providing example architecture patterns showing how data provenance can be maintained throughout the lifecycle. Finally, Section 6 provides a discussion on the value of permissioned blockchain technology, the underpinning science, along with the current state of maturity as applied to a full SE lifecycle.

2. Current Uses of Blockchain Technology

The topic of data management and information control is currently a highly active research area, primarily due to the emergence of Industry 4.0 and its encompassing digital technologies [12,13]. Industry 4.0 is synonymous with the movement of manufacturing to more digitized processes to create products using smart and autonomous systems driven by data and machine learning [14]. Although blockchain is not directly linked with Industry 4.0 in the literature, the value that it brings from a data and information perspective brings value to the SE lifecycle process. Some of the key features of blockchain, which will be discussed at length, are features such as: traceability of transactions and information changes; higher levels of data encryption; and no reliance on third parties to mediate transactions and decisions. As a result, there has been a clear increase in the adoption of blockchain since an earlier blockchain survey [15] in 2016, where the application domains were identified as; finance, IoT, public service, reputation systems, and security. A recent systematic literature review of blockchain-based applications by F. Casino et al. [16] highlight the main application areas, some of which are revisited here to demonstrate their recognition. An obvious place to start is its financial application, as this is where the growth of blockchain adoption stems from.

2.1. *Financial Applications*

Bitcoin [17–19], the first of the cryptocurrencies, popularized the interest and attracted great attentions in blockchain technology from academia and industry. It is by far the most successful cryptocurrency with the capital market exceeding $65 billion dollars in 2019 [20]. The key characteristics blockchains offer is the reason why the finance sector is expected to adopt a substantial role for the technology to ensure sustainability in the future global economy [21,22]. The most obvious advantage of blockchain and cryptocurrencies is the potential it has of transforming capital markets and enhancing operations such as digital payments [23,24], securities [25], general banking services [25,26], loan management schemes [27], and auditing [28] amongst other operations. Blockchain acts as a ledger on a global scale, recording financial (but not limited to) transactions on a "trustless network" [27], where there is no middleman to authorize transactions. The beauty of this ledger is that it is immutable [19] and cannot be altered once a transaction has been recorded within the blockchain. This is as a result of proof-of-work, where mathematical puzzles are set to be solved by the different nodes in the network as a means of creating a protection mechanism against hackers [29,30].

2.2. Data Management

Data management is one of the most prominent and undisputable properties of blockchain [4,10,31,32]. Some claim that blockchain has enhanced data management and have created auditability by default as a result of all actions being verifiable [32]. The blockchain also enhances data storage according to Wang et al. [33]; however, the integrity of this secured data depends on the architecture of the blockchain and the privacy keys, which are allocated by the blockchain developer. As a means of navigating through stored data, [34] propose a solution using cryptographic primitives. Building on this idea, Jiang et al. [35] proposed a blockchain-based key word search system.

2.3. Internet of Things (IoT)

One of the main emerging internet technologies, IoT, has been closely associated with blockchain in having a potentially synergetic relationship [9,16,36–40]. There is a substantial amount of literature that emphasizes the potential of blockchain architectures to enhance the potential of IoT and to minimize its deficiencies and drawbacks [41–43]. The prospects of IoT and blockchain can be mapped onto many contexts, for example, capturing information monitored by heterogeneous devices and stored as transactions into the blockchain or even in the form of smart contracts [27,44,45]. Potential applications of this kind are commonly associated with supply chains, inventory management, and transportation services [16]. The benefit of blockchain solutions and the decentralization network architecture could increase the privacy and security of wireless sensor networks that make up the IoT [46].

2.4. Governance

One of the roles of governments at both the state or local level is to manage official records of residents and enterprises. It has been declared that governments globally are trialing blockchain and creating pilot studies using the technology [47]. The Dutch government, for example, has run pilot projects online [48], which cover passports, digital identity, judicial outcomes, money tracing, e-voting, marital status, business licenses, and so on. Many of these services and others, such as taxes and attestation, are covered by Swan [49] in her book Blockchain: Blueprint for a New Economy.

2.5. Integrity Verification

Integrity verification [50–54] is one of the most emerging blockchain-related fields. A set of applications storing information and transactions related to the "creation and lifetime of products and services" [16]. The possible applications have been identified as: (i) provenance and counterfeit, (ii) insurance, and (iii) intellectual property management [16]. IP protection is high on the research agenda, where blockchain applications are attempting to provide such protection to online content for both storage and simultaneous online validation of (digital) assets [55,56].

2.6. Supply Chain Management

The transparency and accountability features of blockchain have made them of interest to supply chain management researchers [57–61]. IBM solutions claim that blockchain has the potential to enhance supply chain management in terms of optimization, visibility, and demand [62]. The claimed key benefit here is the ability for parties to transact with one another without the need of an intermediary, whilst achieving increased and safeguarded security [63] and ensuring robust contract management mechanisms between parties [64]. These prospects have been recognized to be far reaching in terms of application areas within supply chain and include; better information management across supply chains [65]; IP protection [66]; improved inventory management [67]; and finally, offer decentralized manufacturing architectures [16,68].

Many new applications are being built on the blockchain framework; however, the success of these applications is dependent on the type of blockchain classification being implemented. Understanding the subtleties amongst different blockchain types will enable identification of the potential areas of value with regard to SE and the engineering lifecycle of products. The type of blockchain technology will also determine where it will play a role within the engineering lifecycle plan developed for specific product.

3. Blockchain Technology and Permissioned Blockchains

Understanding the various categories of blockchain enables understanding of their potential application. A specific blockchain technology known as permissioned blockchain can be accessed by everyone or by a restricted consortium of participants. Such blockchains are classified depending on their access status; permissioned [69,70] or permissionless [16,71]; and also, on their level of centralization; public [28,72], where there is no centralized management, private [73–75], where there is a single entity who manages the network, or consortium [65,76], where multiple organizations or participants manage the network. In addition to these criterium for classification, different distributed ledger technologies have different models/architectures, which are used to classify the blockchain type, including; participants, privacy levels, computation energy consumption, speed of validation, consensus mechanisms, fees, and so forth. Some of these characteristics have been provided for the different classes of blockchain in Table 1.

Table 1. Blockchain classification and characteristics.

Access	Permissioned	Permissionless	Permissioned	Permissionless	Permissioned
Centralized Management	Public		Consortium		Private
Access Permissions	Open read/permissioned validation of transactions	Open read/open validation of transactions	Permissioned OR open read/permissioned validation of transactions	Open read/open validation of transactions	Permissioned read/validation of transactions
Participants	Unknown	Unknown	Known	Known (usually)	Known
Privacy	None	None	Tailored to requirements of platform	Tailored to requirements of platform	Tailored to requirements of platform
Validation Based on Consensus	Open to every participant in the network, subject to certain conditions	Open to every participant in the network	By preapproved entities	Depending on the consensus protocol chosen	By preapproved entities (within the single entity)
Validation Speed	Quick	Slow	Quick	Quick	Quick
Computing Energy Consumption	High (depending on consensus mechanism)	Very high	Low	Low	Low

The architecture of a blockchain will determine whether it can be classed as public/consortium, permissioned or permissionless, etc. Blockchain structure and its components can be decomposed into their most basic form as [77] follows; these help understand the process of how a transaction within a blockchain occurs as in Figure 2:

- **Node**—user or computer within the blockchain (each has an independent copy of the entire blockchain ledger stored on personal computer).
- **Transaction**—these are the building blocks of the blockchain and are data records, information, etc.).
- **Block**—a data structure used for keeping a set of transactions, which is distributed to all nodes in the network.
- **Chain**—a sequence of blocks in a specific order according to the time of transaction.
- **Miners**—specific nodes, which perform the block verification process before adding anything to the blockchain structure.
- **Consensus** (consensus protocol)—a set of rules and arrangements to carry out blockchain operations.

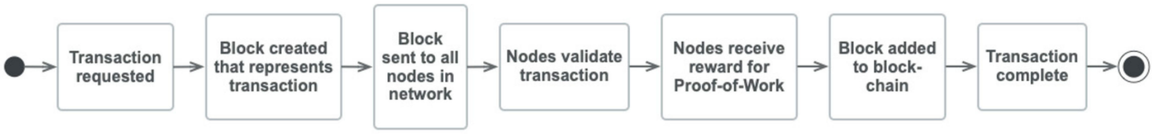
Transaction requested
Block created that represents transaction
Block sent to all nodes in network
Nodes validate transaction
Nodes receive reward for Proof-of-Work
Block added to block-chain
Transaction complete

Figure 2. Blockchain operation process.

Although many people are speculative about blockchain's potential impact in domains other than financial, blockchain's true value in application will be achieved by understanding and exploring its implementation for how it works and the different types of blockchain mechanisms. A blockchain architecture has the potential to provide value to enterprises and organizations in the form of; cost reduction, by eliminating the money spent on central databases; data validity and security, as it becomes extremely difficult to corrupt data, although the processing time increases since all participants need to validate changes; and traceability, where data and historic transactions can be traced back to when they occurred. Where blockchain becomes interesting is when there are more nodes within a consortium and more time is required to complete a transaction, as one node may take longer to validate and thus slow the transaction down.

The role of permissioned blockchain in the end-to-end SE lifecycle of an engineered product or service is anticipated to add the most value from an SE perspective because permissioned blockchains, in both private and the subtype consortium or federated blockchain [15,78], will allow stakeholders to utilize the technology in an advantageous way for information management. A truly public, decentralized blockchain has no specified authority to control the transactions occurring on the platform, thus a completely trustless system exists where users remain anonymous. A platform with more management and control will mean participants and stakeholders will have defined roles and transactions will occur between known entities, thus transactions are monitored and validated amongst a known set of entities. To this end, a permissioned, private, or consortium blockchain is more suitable for SE lifecycle management activities. Thus, future work will examine the implementation of blockchain within a SE setting focusing on popular and established blockchains (e.g., Ethereum, Multichain, and Fabric [79]). To summarize the strengths and weaknesses of this type of blockchain, refer to Table 2. A number of strengths are seen to provide value within the engineering lifecycle, for example, traceability of transactions alone will ensure transparency and allow for legitimate contracts to be executed. Further to this, changes in data within the blockchain can be monitored, and the potential to trace back over time and gather the rationale as to why certain decisions were made will prove invaluable to some stakeholders further down the lifecycle. There is the opportunity to speed up the transaction process, resulting in more efficient networks. Permissioned blockchain being a relatively immature technology, will take some time to be fully adopted due to ownership concerns, the huge amount of storage capacity to keep the blockchain network active, and the large investment cost to be incurred by participating organizations.

Table 2. SWOT analysis of permissioned blockchains.

Strengths	Weaknesses
• High level of encryption • Lower risks • More secure • Traceable trail of transactions • No reliance on third party • Open source • Digital transfers of resources and assets	• Technology not 100% mature • Ownership challenges • Low capacity and processing speed • Security threats from cyber criminals • Large storage capacity requirements—especially long term
Opportunities	**Threats**
• Speed up transaction processes • Programmable access and control mechanisms • Smart contracts and insurances • Improved customer experience	• Regulations • Moderately young technology, more research required • High investment costs • Uncertainty

4. The Role of Permissioned Blockchains in the Systems Engineering Lifecycle

The SE lifecycle covers concept creation, through to development, manufacture (if a product), in service, and retirement. Evaluating where blockchain can add value across the SE lifecycle and how it should be integrated amongst existing technologies, the data structures currently in place need to be assessed and understood. The data flow across the lifecycle of a product or service is often referred to as the digital thread [80]. The concept being presented in this paper is how systems engineers and architects will utilize blockchain with a host of other technologies to set up a digital thread within an organization or interconnected stakeholders and organizations.

Permissioned blockchains are prevalent at industry level and business as the concerns for attributes such as security, role assignment, and participant permissions are high. The example commonly associated with industry is the role of blockchain in supply chain management [61,81], where the participants include suppliers, logistics stakeholders, financial services, and so on. The key feature in this scenario is not all participants should, or have need, to access to all information within the blockchain. Therefore, the blockchain configuration should only grant specific permissions to certain participants. This highlights the importance of the role of blockchain development (Figure 3), where access permissions and privacy features, highlighted in Table 1, are assigned and defined. Data are currently stored within databases (on site or cloud services) within organizations; therefore, the blockchain developer needs to understand how to migrate from existing architectures to a blockchain architecture. Prior to initiating a blockchain, the blockchain developer, who may be within the organization or contracted, needs to establish which stakeholders will be included within the consortium and to assign certificates of permission and access rights. This implies that the blockchain developer has the responsibility of incorporating blockchain within a SE lifecycle, alongside the systems architect and their team.

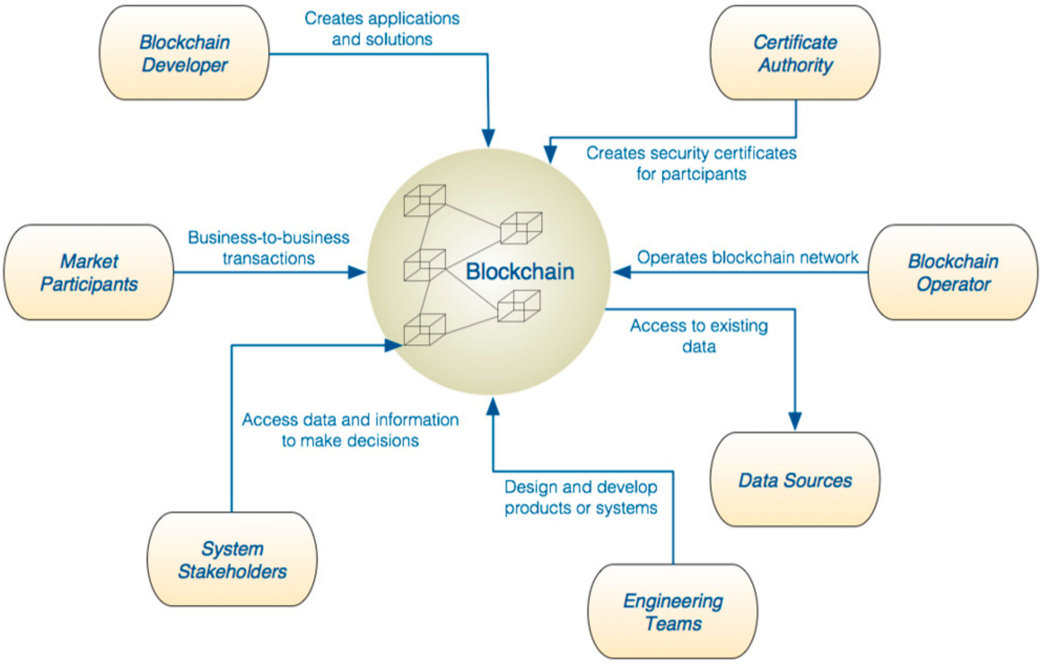
Blockchain Developer
Creates applications and solutions
Certificate Authority
Creates security certificates for partcipants
Market Participants
Business-to-business transactions
Blockchain
Operates blockchain network
Blockchain Operator
Access to existing data
Data Sources
Access data and information to make decisions
Design and develop products or systems
System Stakeholders
Engineering Teams

Figure 3. Stakeholders in blockchain development for systems engineering.

The type of consensus mechanism built into the blockchain is critical to the success of application, and careful thought must be given to this by the blockchain developer. If the ledger is purely for sharing information, then record integrity is arguably a high-level requirement since the tampering with data is undesirable, thus a consensus protocol must be issued to maintain consistency. However, there are several consensus algorithms, and the mechanics behind each different type is not the focus of this paper. Some consensus algorithms include; Proof-of-work (PoW), Practical Byzantine Fault

Tolerance (PBFT), Proof-of-Stake (PoS), or Proof-of-Authority (PoA) [82,83]. Cryptocurrencies typically run PoW and PoS algorithms.

An important question would be, why would an organization want to consider something like blockchain to be a key technology within their engineering lifecycle? The first and most important aspect would be security and privacy, as confidentiality is imperative in any sector and is critical to keeping a competitive edge over competitors, especially in a market that is dominated by only a handful of organizations. Security is a driving force pushing the blockchain concept forward, with its high resilience compared to traditional database architectures, utilizing a decentralized and distributed pattern vs. a centralized one. Cryptography enhances the security of a distributed ledger, making it highly difficult to corrupt the data and information, although total immunity to traditional security issues is not possible yet [84]. Transactional data in the exchange of goods or services are usually extremely confidential, and where multiple stakeholders, suppliers, customers etc. are likely to be participants in a mutual, permissioned, consortium blockchain, there will need to be privacy protocols in place to protect certain data from certain participants. Assigning permissions is a key value of blockchain, in ecosystems where stakeholders may to some extent be rivals, it is not uncommon for certain organizations to keep pricing strategies, etc., hidden from other organizations, to protect their business interests and to remain competitive.

The inclusive nature of SoS and their associated stakeholders require data to be exchanged during the early stages of development, where requirements for a product to be developed are being defined. Requirements specifications could theoretically be specified using blockchain, allowing multiple stakeholders to add their requirements to a blockchain, and which could be validated by the consortium. This raises the issue of conflicting requirements, as different organizations have varying goals and objectives. An important part of the lifecycle is supply chain management [67,85], necessitating information and data are shared amongst stakeholders during all phases of the SE lifecycle, and permissioned blockchain technology could play a significant role here. A lack of transparency in traditional supply chains, partly due to the globalization of manufacturing, often results in unethical and often illegal practices and transactions. Blockchain potentially removes any suspicion as the ledger records all transactions within an economic ecosystem. For example, the food industry [86] is leading the way by applying blockchain to trace food. Walmart uses the technology to track its pork products sourced from China, recording where the meat comes from and how it is processed and stored [87]. This is being achieved using IBM's blockchain solution for supply chains [88].

In the case of commercial aircraft manufacture, a vast supply chain exists to provide parts and services that contribute to the physical outcome of an aircraft. This is a complex ecosystem in its own right, spanning many geographical locations, involving a multitude of contracts, transactions, and invoices, and extending over a period of many years or decades. Currently, document-based systems are utilized to trace the transactions between collaborating organizations, where for example, parts are "signed off" when they have been delivered and received. Importantly, blockchain has the property of enabling the tracing of these interactions, recording movement of goods and information, so that a history of transactions can be tracked back if necessary, by the aircraft manufacturer or other regulatory organizations with an interest. The value of this is huge, not only for the lower tiers in the supply chain, because their processes could become more efficient and organizations become more accountable for their role within the bigger picture. The prime contractor or aircraft original equipment manufacturer should have a much tighter control over manufacturing and assembly.

5. Architecture Patterns for Permissioned Blockchain Integration

When considering the implementation of blockchain technology within SE, the composition of the SoS or system must be understood from the perspective of the organization wishing to implement the technology by the blockchain developer. Systems architecture patterns are a proven way to define interconnectivity of systems using different modeling languages and different styles [89]. Architecture patterns are diagrammatically represented using object-based modeling languages such as the unified modeling language (UML) [90], commonly used for software based application developments, or the Systems Modeling Language (SysML) [91], an evolution of UML to include systems-based development models. For high-level depiction of a blockchain system to be implemented within an organization for sharing of data and information amongst a heterogenous set of stakeholders and organizations, a block definition diagram (BDD) [92] has been devised (refer to Figure 4). The BDD model denotes a blockchain system higher-level construct, which is made up of a blockchain developer, a prime contractor, a set of subcontractors, and a verifier. The prime contractor would typically be an organization wishing to implement a blockchain architecture, and thus would either develop the distributed ledger in-house or delegate this responsibility to an outside agency who specialize in blockchain development and integration. The developer then designs a blockchain system that integrates a selected set of parties and organizations (in the case of a consortium or private blockchain where all members are known) and assigns the connection credentials and their roles and rights with operating within the blockchain. The BDD also shows a verifier, which implies some sort of consensus algorithm be designed within to verify the transactions and data exchanges amongst the nodes.

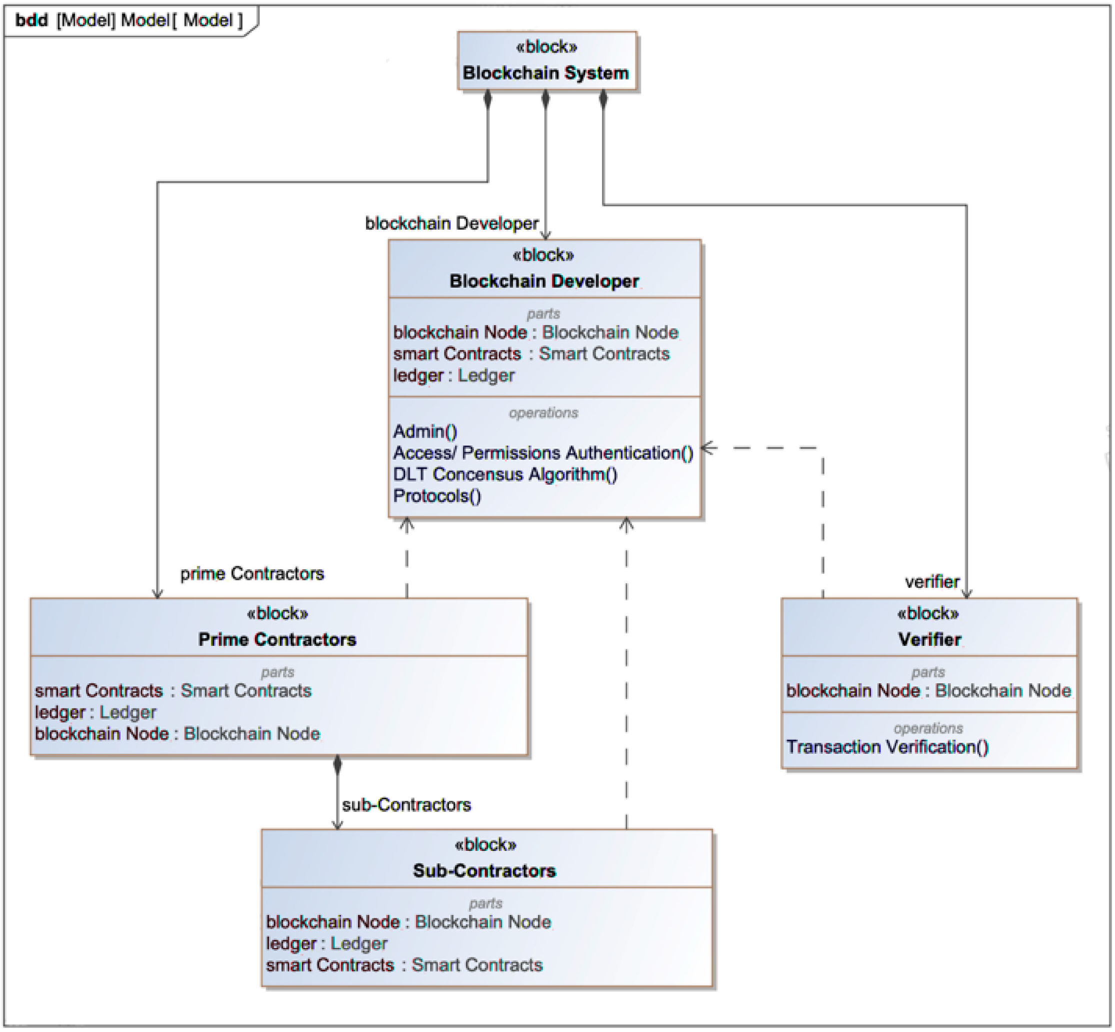
bdd [Model] Model[Model]
«block»
Blockchain System
blockchain Developer
«block»
Blockchain Developer
parts
blockchain Node : Blockchain Node
smart Contracts : Smart Contracts
ledger : Ledger
operations
Admin()
Access/ Permissions Authentication()
DLT Concensus Algorithm()
Protocols()
prime Contractors
verifier
«block»
Prime Contractors
parts
smart Contracts : Smart Contracts
ledger : Ledger
blockchain Node : Blockchain Node
«block»
Verifier
parts
blockchain Node : Blockchain Node
operations
Transaction Verification()
sub-Contractors
«block»
Sub-Contractors
parts
blockchain Node : Blockchain Node
ledger : Ledger
smart Contracts : Smart Contracts

Figure 4. Block definition diagram (BDD) for blockchain implementation.

The blockchain developer, being the entity with the most authority in the network, must be highly trustable by the other entities because it has oversight and determines the permissions for all existing and new users. According to the rules of the blockchain, verification of transactions is conducted by a small collection of nodes, which means these are fast and efficient (compared to public blockchains) [70]. As mentioned earlier, this requires much less computing power for the successful functioning of the blockchain. With regard to new nodes entering the consortium blockchain, or even gaining access to some of the data within the blockchain, access is governed by appropriate levels of authentication, which could be a single leadership or a group of nodes that are preselected. Consider Figure 5, where a third party is requesting access to a set of resources. The blockchain security layer questions whether this is a known participant through requesting login credentials, and if this is cleared by the minimum set of data authorities, i.e., a vote to say yes or no, then access is allowed to the third party. This type of arrangement is common in healthcare applications where healthcare professionals may need access to patient's data and records and do not wish to modify the information (read-only rights).

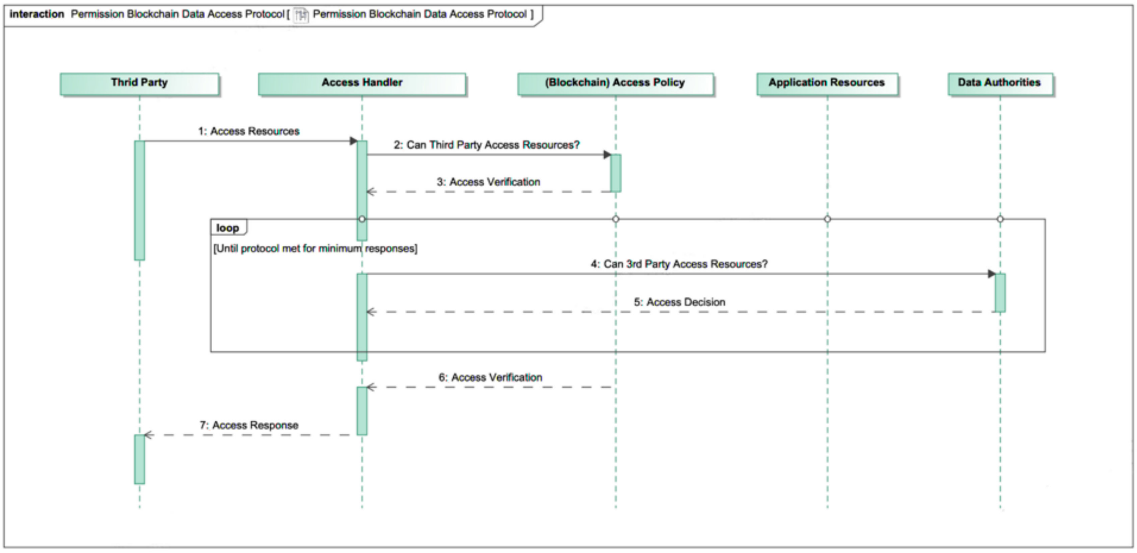
interaction Permission Blockchain Data Access Protocol [Permission Blockchain Data Access Protocol]
Thrid Party
Access Handler
(Blockchain) Access Policy
Application Resources
Data Authorities
1: Access Resources
2: Can Third Party Access Resources?
3: Access Verification
loop
[Until protocol met for minimum responses]
4: Can 3rd Party Access Resources?
5: Access Decision
6: Access Verification
7: Access Response

Figure 5. Permissioned blockchain data access protocol.

Studying the permissioned blockchain in greater detail, it can be noted that the relationship between the nodes is key to the success of the blockchain's application, as consensus is paramount for any transaction or modification of data to occur. Taking a case study of a Systems Applications and Products (SAP) system in data processing for an OEM in the airline manufacturing industry, it is possible to infer the required steps from an SE perspective, to implement a blockchain structure to add the benefits described earlier. SAP systems are centralized with the control and management of the database being undertaken within the organization, shared amongst different departments (finance, sales, production etc.). SAP systems, like most centralized data systems, are effective in eliminating duplication and redundancy in data, providing information across multiple departments. However, it is not so good from an SoS context, where multiple organizations must collaborate and share data in real-time to achieve certain tasks. Therefore, integrating blockchain technology must move away from a centralized architecture and allow for collaboration in a decentralized and distributed manner. As the architecture in Figure 6 shows, the SAP system is connected with a hyperledger (blockchain) that is made up of a known set of nodes (participants), via a server mechanism, which allows the blockchain to access data from the existing database. Consequently, the aircraft OEM can, via an application, access the database, which is also connected to the server, which connects them with the hyperledger (Figure 7). Similarly, those outside of the consortium blockchain who wish to interact with the ledger (whether the ledger is retrieving or submitted information) can do so via a server. It is crucial that the blockchain developer has permissions in place to specifically define who can retrieve and submit information.

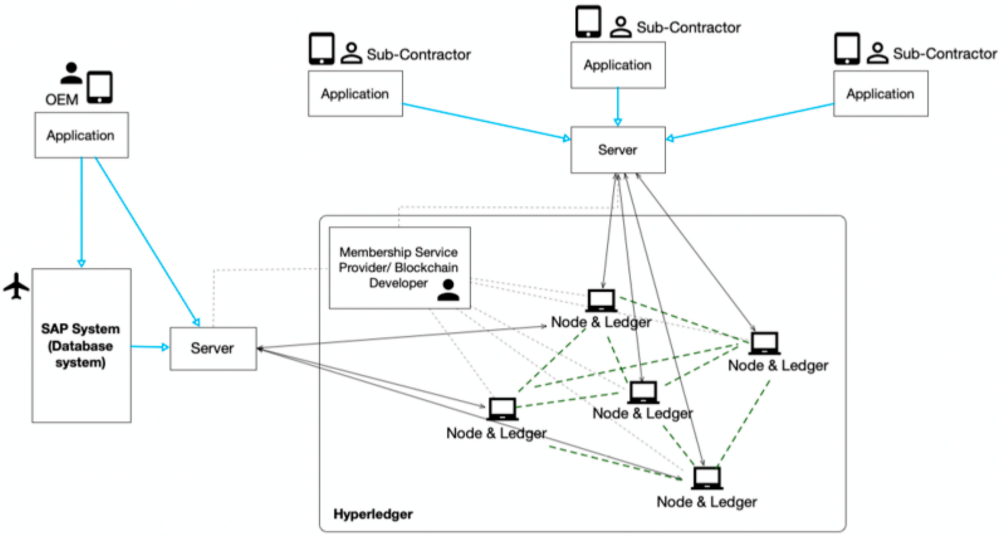

Figure 6. Systems Applications and Products (SAP) system and blockchain integration.

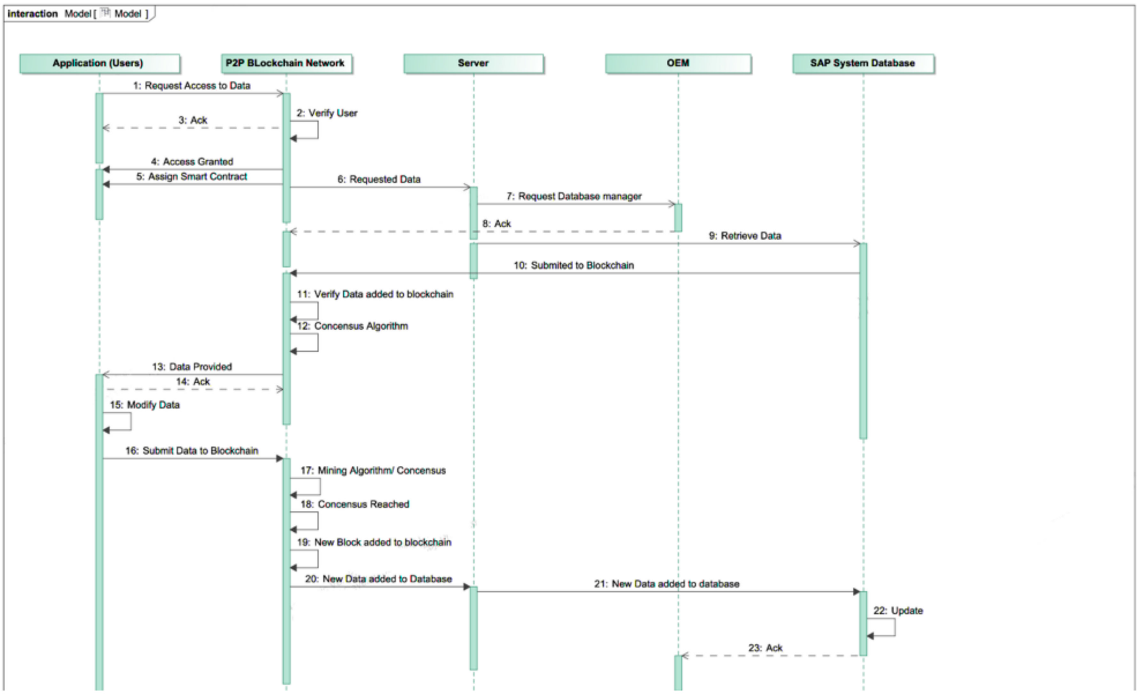
Interaction Model [Model]
Application (Users)
P2P BLockchain Network
Server
OEM
SAP System Database
1: Request Access to Data
2: Verify User
3: Ack
4: Access Granted
5: Assign Smart Contract
6: Requested Data
7: Request Database manager
8: Ack
9: Retrieve Data
10: Submited to Blockchain
11: Verify Data added to blockchain
12: Concensus Algorithm
13: Data Provided
14: Ack
15: Modify Data
16: Submit Data to Blockchain
17: Mining Algorithm/ Concensus
18: Concensus Reached
19: New Block added to blockchain
20: New Data added to Database
21: New Data added to database
22: Update
23: Ack

Figure 7. Sequence diagram showing relationships between traditional database system and a permissioned blockchain ledger.

Example Architecture: Blockchain Forking

As blockchain originated within the cryptocurrency framework, newer blockchain applications may borrow from the experience and efforts within the cryptocurrency domain. One event—ubiquitous in the cryptocurrency industry—is that of forking, where a blockchain ledger is mutated into another one [93]. There are essentially two types of blockchain forks: hard-forks and soft-forks. Hard-forks consist of producing an alternative ledger from a particular block onwards, which is incompatible with the original ledger (Figure 8). A soft-fork is typically a mutation of the original ledger, expanding the functionality of the first while sustaining full compatibility (Figure 9). An example of a hard-fork is that of Bitcoin cash, a new cryptocurrency that spanned out from Bitcoin in 2017. For example, Bitcoin has also undergone soft-forks, to improve the protocol of signature validation.

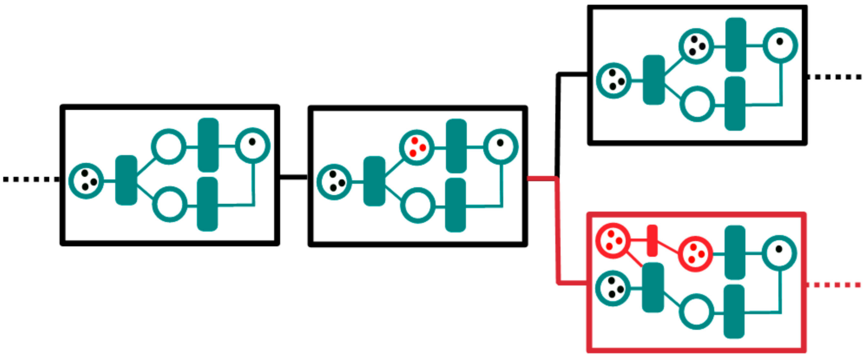

Figure 8. A hard-fork scheme in which a model (a Petri net in the figure) gradually evolves with relatively small changes. Eventually a major change results in a parallel research or production branch, which is incompatible to the first and may be managed by different stakeholders.

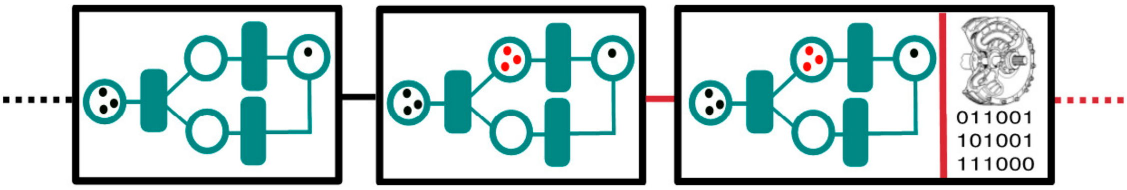

Figure 9. A soft-fork scheme can be employed to update the protocol of the ledger. In the example, the block size is increased with an additional sub-block, which may contain a different type of data encrypted for any subset within the stakeholders.

There are a number of ways in which forking can be employed to address the accountability to a single source of truth in industrial applications and development. In Figure 8, the case of a hard-fork is conceptually explored. In the figure, a model of an industrial design (a Petri net [94] in this example) first evolves within the same fork with slight modifications, perhaps representing a parameter optimization procedure that improves the accuracy of the model. At some point in the development, one of the stakeholders may decide to branch the project to investigate a new disruptive technology, represented in the image as a mutation in the Petri net model in red. The new fork may succeed or may be abandoned, but any design or strategic decision can always be traced back within the branches of the ledger. Figure 9 illustrates the applicability of soft-forking towards scalable blockchain usage. In the figure, a soft-fork expands the capabilities of the blocks, which now—besides including a Petri net model—can also include design schematics and additional digital information such as legal documents. The new sub-block may be only accessible to some of the stakeholders through a permissioned mechanism.

This concept is extremely interesting in the SE lifecycle process, where models (in this case it was Petri net) are to be submitted and shared amongst stakeholders. For instance, in the design phases of a product development plan, alternative design models can be submitted to the consortium, to vote against which one fits the majority of the stakeholder's requirements or expectations. This may be a novel way of collaborative design; however, blockchain poses some thought-provoking concepts of information exchange in the form of models and systems engineering processes; requirements capture and management, design, and verification and validation.

Future work will explore the concept of forking within one of the existing blockchain technologies introduced previously. Multichain [79,95] would be an interesting place to start as it enables users to set several parameters. Within the SE setting, this is crucial as it permits setting the privacy of the chain and controls who can access certain parts of the network. In an SoS, the concept of forking is important as the spectrum of stakeholders involved requires certain types of digital data to be stored and shared amongst set groups. For example, a hard-fork (Figure 8) may mirror evolutions within the SoS as new constituent elements are introduced or removed, depending on the ever-changing requirements.

Similarly, the soft-fork method may be suitable if a selection of stakeholders are required to share data, in which the remainder of the network does not have permission to access.

Multichain is an evolving hyperledger technology and as with any of the blockchain technologies, would need to be tailored to the requirements of a specific SE application. Presently, this private chain application would seem to be a suitable place to begin applying architecture patterns to recognize its implementation, as it can manage the nodes within the permissioned network. However, an in-depth review of the nuances between the technologies would be required to make an informed and evidence-based decision for each specific SE scenario.

6. Discussion on Implementation Challenges of Permissioned Blockchains in SE Lifecycle

Evidence suggests several sectors anticipate blockchain to be a disruptive force, with 62% of executives from the automotive industry say this will be within the next three years. Where this paper suggests its role will be within the end-to-end system engineering lifecycle process, at various phases, the precise role of the technology in digital transformation is still widely uncertain. Data scientists are still skeptical about using blockchain for applications other than its trust-free capability however, from a data and information management standpoint. Many sceptics believe the technology has been overhyped, claiming many are merely "jumping on the blockchain bandwagon" [96]. This paper has made the case for it with regard to storing, sharing, and altering information in a permissioned and consortium structure. Table 3 presents and summarises the challenges posed by permissioned blockchains within the SE lifecycle and from a SE perspective.

Practically, the technology is relatively immature and unestablished in comparison to other database-type products such as Oracle and MySQL, which are mature and proven products. Where the blockchain provides great promise is in its distributed nature that necessitates the validation of transactions by a consortium of known participants (in the permissioned setup, no least). As summarized in Table 3, this can be seen as both a positive and a negative, as this requires all nodes to store a local copy of the complete ledger, locally, demanding high storage capacity, but also requires huge computing power to implement "mining" and proof-of-work and algorithms to validate transactions. This distributed arrangement is desirable for distributing information and for creating an immutable ledger of information; however, it is yet to be seen if these systems are truly trust free. Nakamoto spoke of the "51% Attack" in his seminal paper [8] as a major security issue that if over half the nodes in a network conspire to edit, remove, or change data that already exist on the blockchain, then it can be overwritten and done. Though unlikely in the public blockchain arrangement where the participants are unknown, within a permissioned arrangement this could be done.

Encryption is a key consideration when operating within a permissioned blockchain. Encryption and access to information data are controlled by the blockchain developer, where read/write and access rights are assigned for all participating users and nodes. The realization that new nodes may join the blockchain network later in the SE lifecycle is important to note, and it may be the case that some stored information within the blockchain should be restricted for their access. Confidentiality within multi-stakeholder organizations and supply chains, for example, is paramount, and some parts of the ledger may need to have restricted access. How to manage this access has been touched upon with an authentication pattern in this paper, refer to Figure 5. This raises the possibility to integrate disparate blockchains at certain points, thus, to certificate access to the correct data and information for particular users. Currently, there are no inter-blockchain communication standards, something that would need to be deeply researched and investigated if blockchains were to play a significant role in SE. This is largely due to the fact that the development of complex systems and SoS involved the multi-disciplinary approach and sharing of data amongst a large array of stakeholder groups. Blockchain depends on transactions being verified by a consortium of participants, whereas in the traditional SE arena, only stakeholders who are directly involved within a decision would need to accept the exchange of information or data. This adds to the requirement for integrating blockchains, where only the involved participants within an SE activity would be required to all validate a transaction for a decision to be implemented.

Table 3. Challenges for implementing blockchain within the systems engineering lifecycle process.

Challenge	Blockchain Limitations	SE Considerations	Solutions
Requirement for Large Data Storage Capacity	• Large computational overhead/cost • Large processing power required for "mining" • Execution of complex computational tasks	• Processing speeds important for seamless transactions and efficient development schedules	• Cloud storage • Edge computing
Access Control	• Large P2P networks need a range of access permission levels • Smart contracts • Scalability issues	• Sharing information and data may not be OK between some participants within blockchain network • Supply chain integration	• Disparate blockchains • Integrated blockchains
Trust Management	• Tracing compromised nodes • Homomorphic encryption • Key management needed	• Encrypted data must be decrypted for specific users • Legitimacy of participants	• Trust-based routing protocols • Privacy preserving systems
Connecting heterogeneous databases	• Blockchain acts as a ledger and complete version held by each node • Homomorphic encryption	• Data set types, size, and formats • Supply chain integration • Scheduling processes to ensure effective development of products	• Cloud computing • Edge computing
Conflicting Consensus	• For transaction to be valid, all participants must agree • Verification of results is needed • Mostly based upon theoretical approaches • Tracing conflicting results within network • Smart contracts	• Stakeholders have conflicting goals and objectives • Competition within network itself	• Blockchain P2P with participants with same goals • New consensus algorithms
Integrated blockchains	• No inter-blockchain communication standards	• Complex systems infer multiple stakeholder groups, each with confidential datasets that cannot be shared with all stakeholders	• New blockchain communication standards

Problematically, is the vocabulary and jargon used by the blockchain community are not properly understood by nonexperts and most people, and it is therefore difficult to build that trust in such systems without a trustworthy party involved. It may be seen that blockchain is being developed by blockchain enthusiasts for other blockchain enthusiasts who understand the processes and algorithms required. Following on from this line of thought, the potential for human error is likely to pollute a blockchain if false information is entered. If the blockchain is used as a decentralized database, there is a risk that the quality of data entered at some stage will damage the integrity of the information stored within a ledger. However, the mechanisms in which blockchain is built around should theoretically make the ledger extremely close to immutable; therefore, transactions and information would essentially be stored and referencing to historical data will be undisputable, therefore making the blockchain extremely attractive to many domains, no least to systems engineering itself.

7. Conclusions

This paper has shown there is potential value for implementing blockchain, more specifically permissioned blockchains, within a SE lifecycle to help to cope with the complexities of complex SoS and the huge data management challenges they bring. Blockchain has many qualities that should bring value to an SE process in the form of global traceability, increased transparency, increased trust, and a single location for information and the decisions taken at multiple stages of the development process. In essence, the blockchain becomes a single source of truth where stakeholders can track information and show proof of origin in the case of requirements and system designs (for example), proof of delivery, and proof of receipt and payment etc., in the case of supply chains, all of which can be performed globally.

Numerous blockchain technologies are evolving at the time of writing—some of which have been introduced within this concept paper (Ethereum, Multichain, Fabric)—that could have a significant role in the end-to-end SE lifecycle of an engineered product, service, or, as introduced, an entire SoS. From an SE perspective, this could solve some of the challenges in data management and provide the mechanisms to trace information and data throughout a lifecycle—to further assist in the validation of products and services.

The paper examined a variety of blockchain forms (public, private, consortium, permissionless, and permissioned) and shows that permissioned blockchains within a consortium arrangement, where all participants are approved, would be most suitable within an SE context, as the stakeholders within an SE development process would be all known and will have definitive roles in the development of a product or service. To demonstrate the process of implementing a blockchain architecture, a series of architecture patterns were exhibited to show the considerations to be taken by the systems architect when incorporating the technology into pre-existing legacy systems. The role of different stakeholders within the blockchain integration process were highlighted; however, more work is required to fully understand how a blockchain can truly be realized within an existing SoS framework. To this end, a series of challenges were defined and the limitations of blockchain that need to be addressed by the research community in order to make blockchain a viable solution to data management within a SE lifecycle were outlined.

The recent explosion of the big data era has come with its challenges of trust and security. This is true in all walks of life and in all domains, particularly those who require transmitting data and information in day-to-day operations. Certainly, security is crucial in financial applications (as covered in Section 2), where traditional centralized databases are ineffective when it comes to missing transactional records or defenses against hacking. Blockchain is known for its capabilities in platform security because of its distributed and decentralized architecture. Many lessons can be learnt from other application areas, including finance and supply chains. For instance, blockchain shows great promise in SE lifecycle processes, specifically permissioned blockchains. PBC are trusted data and information storage and sharing platforms that are immutable. For SE, this is fantastic in tracing back where key decisions were made in the development of products or systems but also for tracing transactional data in the case of supply chains when considering the manufacture and production of systems. Permissioned blockchains show great promise if further research is conducted to realize the role of this technology in the systems engineering lifecycle.

Author Contributions: Conceptualization, D.J. and R.K.; methodology, D.J., R.K. and M.M.-G.; software, D.J.; validation, C.F. and K.F.; formal analysis, D.J. and R.K.; investigation, D.J. and M.M.-G.; data curation, D.J.; writing—original draft preparation, D.J., R.K., and M.M.-G.; visualization, D.J. and M.M.-G.; supervision R.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by the Royal Academy of Engineering and Airbus under Grants RCSRF1819\7\14 and REA1819\2\18.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Raz, A.K.; Kenley, C.R.; DeLaurentis, D.A. System architecting and design space characterization. *Syst. Eng.* **2018**, *21*, 227–242. [CrossRef]
2. Maier, M.W. Architecting Principles for Systems-of-Systems. *Syst. Eng.* **1998**, *1*, 267–284. [CrossRef]
3. Dahmann, J.; Rebovich, G.; Lane, J.; Lowry, R.; Baldwin, K. An implementers' view of systems engineering for systems of systems. In Proceedings of the 2011 IEEE International Systems Conference, Montreal, QC, Canada, 4–7 April 2011; IEEE: Washington, DC, USA, 2011; pp. 212–217. [CrossRef]
4. Jin, T.; Zhang, X.; Liu, Y.; Lei, K. BlockNDN: A bitcoin blockchain decentralized system over named data networking. In Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 4–7 July 2017; IEEE: Washington, DC, USA, 2017; pp. 75–80. [CrossRef]
5. Hause, M. The Unified Profile for DoDAF/MODAF (UPDM) enabling systems of systems on many levels. In Proceedings of the 2010 IEEE International Systems Conference, San Diego, CA, USA, 5–8 April 2010; Institute of Electrical and Electronics Engineers (IEEE): Washington, DC, USA, 2010; pp. 426–431.
6. Madni, A.M.; Purohit, S. Economic Analysis of Model-Based Systems Engineering. *Systems* **2019**, *7*, 12. [CrossRef]
7. Holt, J.; Perry, S.; Payne, R.; Bryans, J.; Hallerstede, S.; Hansen, F.O. A Model-Based Approach for Requirements Engineering for Systems of Systems. *IEEE Syst. J.* **2015**, *9*, 252–262. [CrossRef]
8. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 29 February 2019).
9. Li, Z.; Barenji, A.V.; Huang, G.Q. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robot. Comput. Manuf.* **2018**, *54*, 133–144. [CrossRef]
10. Muzammal, M.; Qu, Q.; Nasrulin, B. Renovating blockchain with distributed databases: An open source system. *Future Gener. Comput. Syst.* **2019**, *90*, 105–117. [CrossRef]
11. Wang, Y.; Cai, S.; Lin, C.; Chen, Z. Study of Blockchains's Consensus Mechanism Based on Credit. *IEEE Access* **2019**, *7*, 10224–10231. [CrossRef]
12. Baena, F.; Guarin, A.; Mora, J.; Sauza, J.; Retat, S. Learning Factory: The Path to Industry 4.0. *Procedia Manuf.* **2017**, *9*, 73–80. [CrossRef]
13. Qin, J.; Liu, Y.; Grosvenor, R. A Categorical Framework of Manufacturing for Industry 4.0 and Beyond. *Procedia CIRP* **2016**, *52*, 173–178. [CrossRef]
14. Ahuett-Garza, H.; Kurfess, T. A brief discussion on the trends of habilitating technologies for Industry 4.0 and Smart manufacturing. *Manuf. Lett.* **2018**, *15*, 60–63. [CrossRef]
15. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain Challenges and Opportunities: A Survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
16. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
17. Lewis, A. *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them*; Mango Media: London, UK, 2018; pp. 1–27.
18. Crosby, M.; Nachiappan; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain Technology: Beyond Bitcoin. *Appl. Innov. Rev.* **2016**, *20*, 16.
19. Zhao, J.L.; Fan, S.; Yan, J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financ. Innov.* **2016**, *2*, 28. [CrossRef]
20. CoinMarketCap. 2019. Available online: https://coinmarketcap.com/ (accessed on 21 February 2019).
21. Nguyen, Q.K. Blockchain—A Financial Technology for Future Sustainable Development. In Proceedings of the 3rd International Conference on Green Technology and Sustainable Development (GTSD), Kaohsiung, Taiwan, 24–25 November 2016; pp. 51–54. [CrossRef]
22. Fanning, K.; Centers, D.P. Blockchain and Its Coming Impact on Financial Services. *J. Corp. Account. Financ.* **2016**, *27*, 53–57. [CrossRef]
23. Yamada, Y.; Nakajima, T.; Sakamoto, M. Blockchain-LI: A Study on Implementing Activity-Based Micro-Pricing using Cryptocurrency Technologies. In Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media, Singapore, 28–30 November 2017; pp. 203–207.

24. Beck, R.; Czepluch, J.S.; Lollike, N.; Malone, S. Blockchain—The Gateway to Trust-Free Cryptographic Transactions. In Proceedings of the 24th European Conference on Information Systems (ECIS), Istanbul, Turkey, 12–15 June 2016.
25. Wu, T.; Liang, X. Exploration and practice of inter-bank application based on blockchain. In Proceedings of the 12th International Conference on Computer Science and Education (ICCSE), Houston, TX, USA, 22–25 August 2017; pp. 219–224. [CrossRef]
26. Cocco, L.; Pinna, A.; Marchesi, M. Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology. *Future Internet* **2017**, *9*, 25. [CrossRef]
27. Gazali, H.M.; Hassan, R.; Nor, R.M.; Rahman, H.M. Re-inventing PTPTN study loan with blockchain and smart contracts. In Proceedings of the 8th International Conference on Information Technology (ICIT), Lintong Qu, China, 25–27 December 2017; pp. 751–754. [CrossRef]
28. Hwang, G.-H.; Chen, P.-H.; Lu, C.-H.; Chiu, C.; Lin, H.-C.; Jheng, A.-J. *InfiniteChain: A Multi-Chain Architecture with Distributed Auditing of Sidechains for Public Blockchains*; Springer Science and Business Media LLC: Cham, Switzerland, 2018; pp. 47–60.
29. Ma, Z.; Huang, W.; Bi, W.; Gao, H.; Wang, Z. A master-slave blockchain paradigm and application in digital rights management. *China Commun.* **2018**, *15*, 174–188. [CrossRef]
30. Wang, B.; Chen, S.; Yao, L.; Liu, B.; Xu, X.; Zhu, L. A Simulation Approach for Studying Behavior and Quality of Blockchain Networks. *Lect. Notes Comput. Sci.* **2018**, *10974 LNCS*, 18–31.
31. Zhu, L.; Wu, Y.; Gai, K.; Choo, K.-K.R. Controllable and trustworthy blockchain-based cloud data management. *Future Gener. Comput. Syst.* **2019**, *91*, 527–535. [CrossRef]
32. Neisse, R.; Steri, G.; Nai-Fovino, I. A Blockchain-based Approach for Data Accountability and Provenance Tracking. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017.
33. Wang, J.; Li, M.; He, Y.; Li, H.; Xiao, K.; Wang, C. A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. *IEEE Access* **2018**, *6*, 17545–17556. [CrossRef]
34. Do, H.G.; Ng, W.K. Blockchain-Based System for Secure Data Storage with Private Keyword Search. In Proceedings of the 2017 IEEE 13th World Congress on Services (SERVICES), Honolulu, HI, USA, 25–30 June 2017; pp. 90–93.
35. Jiang, P.; Guo, F.; Liang, K.; Lai, J.; Wen, Q. Searchain: Blockchain-based private keyword search in decentralized storage. *Future Gener. Comput. Syst.* **2020**, *107*, 781–792. [CrossRef]
36. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
37. Jo, B.W.; Khan, R.M.A.; Lee, Y.-S. Hybrid Blockchain and Internet-of-Things Network for Underground Structure Health Monitoring. *Sensors* **2018**, *18*, 4268. [CrossRef]
38. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
39. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
40. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2018**, *125*, 251–279. [CrossRef]
41. Kshetri, N. Can Blockchain Strengthen the IoT? *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
42. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef] [PubMed]
43. Fabiano, N. The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard. In Proceedings of 2017 International Conference on Internet of Things for the Global Community (IoTGC), Funchal, Portugal, 10–13 July 2017; IEEE: Washington, DC, USA, 2017; Volume 2060, pp. 1–7.
44. Patel, D.; Shah, K.; Shanbhag, S.; Mistry, V. Towards Legally Enforceable Smart Contracts. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2018; Volume 10974, pp. 153–165.
45. Gatteschi, V.; Lamberti, F.; DeMartini, C.; Pranteda, C.; Santamaria, V. To Blockchain or Not to Blockchain: That Is the Question. *IT Prof.* **2018**, *20*, 62–74. [CrossRef]
46. Boudguiga, A.; Bouzerna, N.; Granboulan, L.; Olivereau, A.; Quesnel, F.; Roger, A.; Sirdey, R. *Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain*; IEEE: Paris, France, 2017.

47. Ølnes, S.; Ubacht, J.; Janssen, M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Gov. Inf. Q.* **2017**, *34*, 355–364. [CrossRef]
48. Dutch Government Blockchain Pilot Projects. Available online: https://www.blockchainpilots.nl/results. (accessed on 27 February 2019).
49. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
50. Dupont, Q. Blockchain Identities: Notational Technologies for Control and Management of Abstracted Entities. *Metaphilosophy* **2017**, *48*, 634–653. [CrossRef]
51. Jamthagen, C.; Hell, M. Blockchain-Based Publishing Layer for the Keyless Signing Infrastructure. In Proceedings of the 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, 18–21 July 2016; IEEE: Washington, DC, USA, 2016; pp. 374–381.
52. Xu, R.; Zhang, L.; Zhao, H.; Peng, Y. Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology. In Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, Thailand, 22–24 March 2017; IEEE: Washington, DC, USA, 2017; pp. 128–133.
53. Zikratov, I.; Kuzmin, A.; Akimenko, V.; Niculichev, V.; Yalansky, L. Ensuring data integrity using blockchain technology. In Proceedings of the 20th Conference of Open Innovations Association (FRUCT), St. Petersburg, Russia, 3–7 April 2017.
54. Bhowmik, D.; Feng, T. The multimedia blockchain: A distributed and tamper-proof media transaction framework. *Int. Conf. Digit. Signal Process. DSP* **2017**, 1–5. [CrossRef]
55. Fujimura, S.; Watanabe, H.; Nakadaira, A.; Yamada, T.; Akutsu, A.; Kishigami, J.J. BRIGHT: A concept for a decentralized rights management system based on blockchain. In Proceedings of the 2015 IEEE 5th International Conference on Consumer Electronics—Berlin (ICCE-Berlin), Berlin, Germany, 6–9 September 2015; IEEE: Washington, DC, USA, 2015; pp. 345–346.
56. Kishigami, J.; Fujimura, S.; Watanabe, H.; Nakadaira, A.; Akutsu, A. The Blockchain-Based Digital Content Distribution System. In Proceedings of the 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, Dalian, China, 26–28 August 2015; IEEE: Washington, DC, USA, 2015; pp. 187–190.
57. Kshetri, N. 1 Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [CrossRef]
58. Min, H. Blockchain technology for enhancing supply chain resilience. *Bus. Horiz.* **2019**, *62*, 35–45. [CrossRef]
59. Ahram, T.; Sargolzaei, A.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
60. Casado-Vara, R.; Prieto, J.; De La Prieta, F.; Corchado, J.M. How blockchain improves the supply chain: Case study alimentary supply chain. *Procedia Comput. Sci.* **2018**, *134*, 393–398. [CrossRef]
61. Leng, K.; Bi, Y.; Jing, L.; Fu, H.-C.; Van Nieuwenhuyse, I. Research on agricultural supply chain system with double chain architecture based on blockchain technology. *Futur. Gener. Comput. Syst.* **2018**, *86*, 641–649. [CrossRef]
62. IBM. IBM-Zero to Blockchain. Available online: http://www.redbooks.ibm.com/abstracts/crse0401.html?Open&mhq=blockchain&mhsrc=ibmsearch_a (accessed on 1 March 2019).
63. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an Optimized BlockChain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA, 18–21 April 2017; Association for Computing Machinery (ACM): New York, NY, USA, 2017; pp. 173–178.
64. Polim, R.; Hu, Q.; Kumara, S. Blockchain in megacity logistics. In Proceedings of the 67th Annual Conference and Expo of the Institute of Industrial Engineers 2017, Pittsburgh, PA, USA, 20–23 May 2017; pp. 1589–1594.
65. O'Leary, D.E.M. Configuring Blockchain Architectures for Transaction Information in Blockchain Consortiums: The Case of Accounting and Supply Chain Systems. *Intell. Syst. Account. Financ. Manag.* **2017**, *24*, 138–147. [CrossRef]
66. Tsai, W.-T.; Feng, L.; Zhang, H.; You, Y.; Wang, L.; Zhong, Y. Intellectual-Property Blockchain-Based Protection Model for Microfilms. In Proceedings of the 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), San Francisco, CA, USA, 6–9 April 2017; IEEE: Washington, DC, USA, 2017; pp. 174–178.

67. Madhwal, Y.; Panfilov, P.B.; Katalinic, B. Blockchain And Supply Chain Management: Aircrafts' Parts' Business Case. In Proceedings of the 29th International DAAAM Symposium 2017, Vienna, Austria, 11 November 2017; DAAAM International: Vienna, Austria, 2017; pp. 1051–1056.
68. Decentralized Manufacturing. *CIRP Encyclopedia of Production Engineering*; Springer: Berlin/Heidelberg, Germany, 2014; 363p.
69. Vukolić, M. Rethinking Permissioned Blockchains. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts—BCC '17, Abu Dhabi, UAE, 2 April 2017; Association for Computing Machinery (ACM): New York, NY, USA, 2017; pp. 3–7.
70. Hardjono, T.; Pentland, A.S. Verifiable Anonymous Identities and Access Control in Permissioned Blockchains. *arXiv* **2016**, arXiv:1903.04584.
71. Wüst, K.; Gervais, A. Do you need a Blockchain? *IACR Cryptol.* **2017**, 1–7. [CrossRef]
72. Tang, H.; Shi, Y.; Dong, P. Public blockchain evaluation using entropy and TOPSIS. *Expert Syst. Appl.* **2019**, *117*, 204–210. [CrossRef]
73. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in internet of things: Challenges and Solutions. *arXiv* **2016**, arXiv:1608.05187.
74. Duan, J.; Patel, M. Blockchain in Global Trade. *Lect. Notes Comp. Sci.* **2018**, *10974 LNCS*, 293–296.
75. Hawlitschek, F.; Notheisen, B.; Teubner, T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electron. Commer. Res. Appl.* **2018**, *29*, 50–63. [CrossRef]
76. Ross, M.; Hastings, D.E. The tradespace exploration paradigm. *INCOSE Int. Symp.* **2005**, *2005*, 13.
77. Ganne, E. *Can Blockchain Revolutionize International Trade?* World Trade Organization (WTO): Geneva, Switzerland, 2018.
78. BlockchainHub. Blockchains & Distributed Ledger Technologies. 2015. Available online: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/ (accessed on 22 February 2019).
79. Polge, J.; Robert, J.; Le Traon, Y. Permissioned blockchain frameworks in the industry: A comparison. *ICT Express* **2020**. [CrossRef]
80. Singh, V.; Willcox, K.E. Engineering Design with Digital Thread. *AIAA J.* **2018**, *56*, 4515–4528. [CrossRef]
81. Elmessiry, M.; Elmessiry, A. Blockchain Framework for Textile Supply Chain Management. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2018; Volume 10974, pp. 213–227.
82. Nguyen, G.-T.; Kim, K. A Survey about Consensus Algorithms Used in Blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128. [CrossRef]
83. Bach, L.M.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; IEEE: Washington, DC, USA, 2018; pp. 1545–1550.
84. Isaja, M.; Soldatos, J. Distributed ledger technology for decentralization of manufacturing processes. In Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 15–18 May 2018; IEEE: Washington, DC, USA, 2018; pp. 696–701.
85. Wang, Y.; Han, J.H.; Beynon-Davies, P. Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Manag. Int. J.* **2019**, *24*, 62–84. [CrossRef]
86. Bumblauskas, D.; Mann, A.; Dugan, B.; Rittmer, J. A blockchain use case in food distribution: Do you know where your food has been? *Int. J. Inf. Manag.* **2020**, *52*, 102008. [CrossRef]
87. Kamath, R. Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. *J. Br. Blockchain Assoc.* **2018**, *1*, 3712. [CrossRef]
88. IBM. Now Arriving: IBM Blockchain for Supply Chain. Available online: https://www.ibm.com/blockchain/industries/supply-chain (accessed on 5 August 2019).
89. Kalawsky, R.S.; Joannou, D.; Tian, Y.; Fayoumi, A. Using Architecture Patterns to Architect and Analyze Systems of Systems. *Procedia Comput. Sci.* **2013**, *16*, 283–292. [CrossRef]
90. Unified Modeling LanguageTM (UML®) Resource Page. 2015. Available online: http://www.uml.org/ (accessed on 1 November 2020).
91. Friedenthal, S.; Moore, A.; Steiner, R. *OMG SysML TM Specification Specification Status*; Object Management Group: Needham, MA, USA, 2008.
92. Lane, J.A.; Bohn, T. Using SysML modeling to understand and evolve systems of systems. *Syst. Eng.* **2012**, *16*, 87–98. [CrossRef]

93. Vujicic, D.; Jagodic, D.; Randic, S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In Proceedings of the 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), Sarajevo, Bosnia-Herzegovina, 21–23 March 2018; IEEE: Washington, DC, USA, 2018; Volume 2018, pp. 1–6.
94. Barad, M.; Sipper, D. Flexibility in manufacturing systems: Definitions and Petri net modelling. *Int. J. Prod. Res.* **1988**, *26*, 237–248. [CrossRef]
95. Howard, J.P.; Vachino, M.E. Blockchain Compliance with Federal Cryptographic Information-Processing Standards. *IEEE Secur. Priv. Mag.* **2020**, *18*, 65–70. [CrossRef]
96. Greenspan, G. Avoiding the Pointless Blockchain Project. 2015. Available online: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/ (accessed on 5 March 2019).

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.