A framework for selecting and integrating blockchain devices into supply chain management

Tan Gürpinar [1], Thuy Tien Nguyen Thi [2], Maximilian Austerjost [2]
[1] Quinnipiac University, Hamden, USA
[2] Fraunhofer IML, Dortmund, Germany

With blockchain technology revolutionizing data exchange and process automation, companies face challenges in securely transferring data, connecting devices, and facilitating ecosystem interactions. We outline a three-phase methodology for selecting and integrating blockchain devices, focusing on their application in supply chain management: (1) initial use case classification, (2) comparison with existing blockchain devices and (3) taxonomy-based fine-tuning. This structured approach combines technology selection procedures with the device taxonomy to provide actionable guidance. Key findings include the selection criteria of blockchain devices, a detailed classification of current devices, and practical recommendations for their application in supply chains. The framework emphasizes blockchain's potential to enhance transparency, security, and efficiency in logistical processes, offering valuable insights for both companies and blockchain enthusiasts.

1. Introduction

Blockchain technology is revolutionizing various industries by offering enhanced security, transparency, and efficiency in data management and process automation. This technological advancement is particularly relevant in supply chain management, where the need for secure and transparent data exchange is critical. However, an empirical study on the adoption of blockchain technology among German companies revealed that only 12% have implemented it in their supply chains so far [1]. Despite its potential, one of the primary challenges is that blockchains, by default, cannot access real-world off-chain data. This limitation significantly constrains the scope of blockchain applications, particularly in supply chains [2]. Therefore, blockchain devices, which facilitate the connection between physical assets and digital records, play a crucial role in leveraging the benefits of blockchain technology in real-world applications.

The importance of researching blockchain devices stems from the fundamental principle that the effectiveness of a blockchain system is heavily dependent on the quality and integrity of the data it processes [3]. Inadequate or erroneous data inputs can lead to unreliable outputs, undermining the system's credibility and effectiveness. Hence, the precise selection and integration of blockchain devices are paramount to ensuring that data remains accurate, consistent, and trustworthy throughout the supply chain [4].

Despite the growing adoption of blockchain technology, there is a notable lack of comprehensive frameworks for selecting and integrating blockchain devices [5]. Current research often focuses on theoretical aspects of blockchain technology or general technology selection methods, which do not adequately address the unique requirements and challenges associated with blockchain devices [6, 7]. This gap in the literature highlights the need for a specialized methodology that addresses both the technical and practical aspects of blockchain device integration.

This paper seeks to address this gap by exploring how companies can systematically select and integrate blockchain devices to enhance their operational efficiency and data integrity. The research question guiding this study is:

How can organizations effectively choose and implement blockchain devices to maximize their operational benefits and ensure reliable data processing?

The paper is structured to first present a definition of the most relevant terms and a detailed methodology for the selection and integration of blockchain devices. It will then analyze the characteristics and capabilities of existing devices, followed by a discussion of practical implementation strategies. Finally, the paper will provide recommendations for future research and development in this area, aiming to support organizations in achieving optimal performance and reliability in their blockchain systems.

2. Theoretical Background

Blockchain devices are pivotal in ensuring the effectiveness and reliability of blockchain systems by serving as the interface between physical assets and digital ledgers. These devices capture and transmit real-world data into the blockchain, making them essential for maintaining the integrity and accuracy of the information recorded on the blockchain. The theoretical background for blockchain devices revolves around several core concepts and challenges:

Data Integrity and Accuracy: Blockchain systems rely on the principle of data immutability, where once data is recorded on the blockchain, it cannot be altered without detection. However, the accuracy of this data is contingent upon the quality of the input provided by blockchain devices. If a device transmits erroneous or

tampered data, it can compromise the integrity of the entire blockchain ledger. Research in this area focuses on developing technologies and methodologies to ensure that data captured by blockchain devices is accurate, reliable, and resistant to tampering.

Device Security: Given that blockchain devices act as the entry point for data into the blockchain, they must adhere to stringent security protocols to prevent unauthorized access and data breaches. This includes implementing robust encryption methods, secure communication channels, and anti-tampering mechanisms. Theoretical frameworks in this domain explore best practices for securing these devices against various types of cyber threats and vulnerabilities.

Integration and Compatibility: Blockchain devices need to seamlessly integrate with existing infrastructure and blockchain networks. This involves addressing challenges related to interoperability, standardization, and compatibility with other systems and devices. Research in technology integration theory examines how blockchain devices can be effectively incorporated into current processes, ensuring that they operate harmoniously within the broader technological ecosystem.

Performance and Scalability: The performance of blockchain devices is crucial for the overall efficiency of blockchain systems. This includes factors such as processing speed, data transmission rates, and the ability to handle large volumes of data. Theoretical research in this area investigates how to optimize device performance to support scalable blockchain applications and prevent bottlenecks in data processing and communication.

Human-Device Interaction: The usability of blockchain devices impacts their effectiveness and adoption. This aspect covers the design of user interfaces, ease of operation, and the ability of devices to provide actionable insights. Research in human-device interaction focuses on improving user experience, which is vital for ensuring that blockchain devices are practical and user-friendly for their intended applications.

By addressing these theoretical aspects, research on blockchain devices can advance our understanding of their role in enhancing the functionality and reliability of blockchain systems. This background provides a basis for developing guidelines and best practices for selecting and integrating blockchain devices, ensuring that they contribute positively to the overall performance and security of blockchain applications.

3. Methodology

The methodology for researching blockchain devices involves a systematic approach to examining their characteristics, performance, and integration into blockchain systems. This approach includes a combination of qualitative and quantitative methods to ensure a comprehensive analysis. The following steps outline the methodology:

Literature Review: We start with a review of existing literature on blockchain devices, focusing on their roles, functionalities, and the challenges associated with their implementation. This step involves analyzing academic papers, industry reports, and case studies to build a foundational understanding of the current state of blockchain device technology and identifying gaps in the research.

Device Classification: We then collect information on the method and the criteria that is used to classify the devices as well as their functions and applications. This classification includes sensors, IoT devices, hardware wallets, and other peripherals that interact with blockchain systems. To classify the devices in a first step (Device Matrix in Chapter 4), we follow the methods developed by [8, 9, 10], which focus on selecting technologies by setting future goals and working backward from there. This approach, known as "retropolation," helps to identify pathways towards achieving these goals. It involves techniques like experience curves, S-curve analyses, and scenario planning.

Among these, the portfolio technique is particularly useful for choosing technologies that need to be implemented within a timeframe of up to 5 years. Therefore, we based our method on the portfolio analysis by [11]. Building on this, this article introduces a portfolio analysis specifically suitable for blockchain devices and uses it for its initial classification process. In a second step, the classification is refined by describing the requirements for the device starting from the information obtained from the matrix of the previous step. For this refinement, the article utilizes a multidimensional taxonomy as described by [12] as this tool has already been successfully utilized to classify blockchain supply chain use cases [13] and hardware [3]. Following the method, in this article a morphological box is used to describe the blockchain device based on predefined dimensions. The taxonomy is used to describe the device required for the use case in a more granular way by selecting appropriate characteristic values for each dimension. The aim is to enable users to draw detailed conclusions and formulate their own requirements for the device.

Case Studies and Interviews: We conduct case studies and interviews with industry experts, developers, and users of blockchain devices to validate theoretical findings and gather practical insights. The former provides practical examples of how devices are used in real-world scenarios, while interviews offer qualitative insights into user experiences, challenges faced, and best practices.

Data Collection and Analysis: We gather quantitative data through surveys, experiments, or testing protocols. This data may include device performance metrics, security assessments, and user feedback. Analyze this data using statistical methods to identify patterns, correlations, and trends. This analysis provides empirical evidence to support the research findings and conclusions.

Comparative Analysis: We perform a comparative analysis of different blockchain devices based on the established criteria. This involves evaluating the strengths and weaknesses of each device category, as well as their suitability for various applications. The comparative analysis helps to identify the most effective and reliable devices for specific use cases.

Integration Strategies: We develop and evaluate strategies for integrating blockchain devices into existing systems. This includes assessing compatibility with different blockchain platforms, identifying integration challenges, and proposing solutions. The aim is to provide practical guidelines for seamless integration and optimal performance.

Recommendations and Best Practices: Based on the findings, we formulate recommendations and best practices for selecting, implementing, and managing blockchain devices. These recommendations are designed to guide stakeholders in making informed decisions and improving the overall effectiveness of blockchain systems.

By following this methodology, the research aims to provide a comprehensive understanding of blockchain devices, their functionalities, and their impact on blockchain systems. The approach combines theoretical insights with practical evidence to offer valuable guidance for researchers, practitioners, and developers in the field.

4. Blockchain Device Matrix

In the following, four blockchain devices are explained as examples and to give a better understanding of how such devices are used in a supply chain scenario:

Temp2Net: This is an IoT device designed for monitoring temperature-sensitive goods along supply chains. It integrates blockchain technology to document and secure data such as location and internal temperature. The device includes a high-resolution e-paper display for real-time information and utilizes a combination of sensors, a light client, and blockchain integration through the Tendermint framework and Cosmos SDK.

DragonDevice: A mobile device developed for handling dangerous goods, DragonDevice focuses on automating and digitizing transport documentation. It supports the carrier by providing electronic transport documents, tracking dangerous goods, and ensuring compliance with regulations. The device features a display, camera, and sensors, and integrates blockchain technology to secure and update transport records. It also supports the "bring your own device" concept to leverage existing mobile hardware.

DragonPuck: This modular IoT device is used for tracking hazardous materials during transportation. It monitors environmental conditions such as temperature, humidity, and acceleration. The DragonPuck operates on energy-efficient batteries, uses Wi-Fi and mobile networks for communication, and integrates with blockchain for transaction recording and data security. The device is designed for long-term operation with minimal maintenance.

Blockchain IoT Gateway: They represent high-performance devices (e.g. a server) that receive data inputs from sensors and send them to a blockchain network. This is necessary as some IoT devices are restricted by their computational performance and memory and therefore cannot participate in blockchain consensus as it is computationally heavy [14].

The following table provides an overview of the two dimensions to create a portfolio analysis of blockchain devices.

Table 1: Features and Examples of Blockchain Devices

Category	Feature	Examples
Mobility	Stationary Device	Server
	Mobile Devices	Tablet, Sensor
Equipment	Low Energy Device	DragonPuck
	Middle Class Device	Temp2Net
	High Performance Devices	DragonDevice

1) Mobility comprises the spatial/local flexibility of the physical blockchain device in the sense of its being (un)bound to a specific location, by describing the transportability or concrete mobility as well as the cable connection. The more pronounced these characteristics are, the higher the mobility of the device can be classified. Two sub-dimensions exist.

Stationary Devices are used in a fixed position (e.g. permanently installed), as no movement is possible or desired on the part of the process (e.g. blockchain gateway server).

Mobile Devices have increasing degrees of freedom for spatial movement, for example because they are moved in the process (e.g. integration on pallets) or there are requirements for the device's own mobility (e.g. tablet, sensors)

2) Equipment characterizes the device in terms of its inherent peripherals and external constitution on the one hand and includes the dimensions of application and communication performance on the other. The higher the identified value of this characteristic, the higher the requirements for the scope of features and performance of the device are assumed. The three-way division into low energy, middle class and high performance devices is based on a classification scheme proposed by the Internet Engineering Taskforce (see Table 2). There, resource-constrained IoT devices are categorized based on their random-access memory (RAM) and flash memory [15].

Table 2: Classification Scheme [based on 15]

Class	Equivalent	RAM	Flash
Class 0	Low Energy	<< 10 kB	<< 100 kB
Class 1	Middle Class	~ 10 kB	~ 100 kB
Class 2	High Performance	~ 50 kB	~ 250 kB

Low Energy Devices allow little or no user interaction and are only used to collect or transmit data. Low-energy devices are also characterized by their low energy consumption, but they generally have limited memory and computing resources (e.g. sensors such as the DragonPuck)

Middle Class Devices are used to support business processes and can be interactively used. They have a number of input, output and operating options. Even though they are more energy-intensive, they have better energy reserves (e.g. rechargeable batteries). Thanks to the memory and computing resources provided, they can perform some tasks themselves in order to control energy requirements, but the device and its functionalities are not used continuously (e.g. Temp2Net).

High Performance Devices have additional peripherals and distinct interaction options, whereby the entire hardware package is more extensive. The high-performance devices are correspondingly energy-intensive, but also offer more comprehensive data processing and data transfer options (e.g. DragonDevice).

After presenting the evaluation criteria for our portfolio analysis, the exemplary devices and other blockchain devices can finally be classified. The (necessary) degree of mobility is shown on the abscissa of the matrix. The ordinate describes the (necessary) performance of the device. Based on these categories, a portfolio diagram is drawn, which can be used to visually classify devices based on the dimensions previously described. There are nine fields within the portfolio matrix, each of which represents a combination of degree of mobility, equipment and performance. According to a simple nearest-neighbor approach, the blockchain devices that are close to the classification of one's own use case in the matrix are suitable as a first approximation (see Figure 1). The smaller the distance between the points, the greater the agreement in the characteristics of the devices.

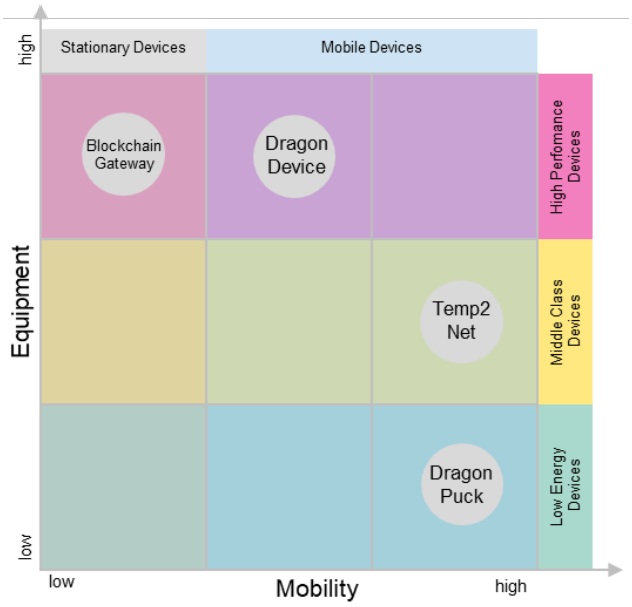

Fig. 1: Blockchain Device Matrix

5. Blockchain Device Taxonomy

In the previous section, we provided a broad classification of blockchain devices, introducing various types and their core functionalities. Here, we delve into a more detailed taxonomy to offer a nuanced understanding of blockchain devices and facilitate further research into their categorization and application.

I. Device Type

a. IoT Devices: These devices are designed for integration into Internet of Things (IoT) ecosystems, enabling real-time data collection and interaction with blockchain networks. They are often equipped with sensors and connectivity features to monitor environmental conditions or track assets. Examples include temperature monitors for supply chains and environmental sensors for hazardous material handling.

b. Mobile Devices: Mobile blockchain devices include smartphones or tablets that have been adapted to handle blockchain transactions or provide specialized blockchain services. These devices often include applications or software for managing digital assets, verifying transactions, or interacting with decentralized applications.

c. Specialized Devices: These are devices tailored for specific use cases or industries, such as compliance documentation for dangerous goods or modular tracking units for logistical operations. They often combine blockchain functionality with industry-specific requirements.

II. Integration Level

a. Full Nodes: Devices operating as full nodes maintain a complete copy of the blockchain and participate in validating and propagating transactions. They typically require significant computational resources and storage capacity.

b. Light Nodes: Light nodes, also known as thin clients, rely on full nodes for blockchain data and focus on reducing computational and storage demands. These devices are often used in environments where resource constraints are a concern, such as mobile or embedded systems.

c. Hybrid Nodes: These devices operate with a mix of full and light node capabilities, balancing between local data processing and reliance on external blockchain networks. They are designed to optimize performance and resource use for specific applications.

III. Application Domain

a. Supply Chain Management: Devices in this category focus on tracking goods through various stages of the supply chain. They may include temperature sensors, GPS trackers, and compliance monitoring tools, all integrated with blockchain for data security and traceability.

b. Environmental Monitoring: These devices are used to measure and report environmental conditions such as temperature, humidity, or air quality. They are crucial in applications where data integrity and real-time monitoring are essential, often used in conjunction with blockchain to ensure data accuracy and reliability.

c. Compliance and Documentation: Devices designed for regulatory compliance and documentation tasks fall into this domain. They often provide functionalities for digital record-keeping, transaction verification, and adherence to legal requirements, leveraging blockchain to secure and verify documents.

IV. Taxonomy

This taxonomy provides a structured framework for classifying blockchain devices based on their type, integration level, and application domain. It serves as a foundation for further research and development, enabling a deeper understanding of how these devices operate and interact within the blockchain ecosystem.

Device Differentiation: The first dimension shows how devices differ according to their performance, ability to interact with the external environment and communication capabilities. The main distinction between low-end, middle-end and high-end was explained in Chapter 4. Within the first dimension, the equipped systems can range from sensors that measure data from the environment or actuator, control and regulation systems that perform actions to maintain a desired state.

The used communication technologies represent a further distinguishing feature. The devices are equipped with at least one of the following communication technologies. Local Area Network (LAN) (e.g. Ethernet or bus systems) represents a wired communication technology. Personal Area Networks (WPAN) have a range of approx. 100 m and typical examples are Bluetooth, ZigBee or Z-Wave equipment. The IP-based network protocol 6LowPAN with its open IP standards and web sockets is also part of the WPAN. Wireless Local Area Networks (WLANs) with the most widespread Wi-Fi standard offer a range of up to 1 km. IoT devices can switch off Wi-Fi connections with the Target Wake Time function most of the time and only connect briefly and on schedule. Low-Power Wide Area Networks (LPWAN) is an emerging communication technology with extremely long battery life and a maximum communication range of over 20 km. The three most important competing standards are LoRa, Sigfox and NB-IoT. Wireless Neighborhood Area Networks (WNANs) lie between WLAN and long-range technologies such as mobile communications in terms of communication range. Typical representatives of this technology include mesh networks such as Wi-SUN or JupiterMesh. Mobile networks such as GSM, 3G, 4G and 5G are used for the long-range operation of IoT devices.

Network Integration: In a second dimension a distinction is made between the network and the gateway. The platform architecture of the IoT devices differs in terms of the use of a central node (e.g. with cloud architectures) or a decentralized IoT platform without a central node. Star, point-to-point and mesh are the three typical network topologies. In a star network, all devices are connected to a central hub. In point-to-point, a direct connection is established between the nodes. In the mesh network topology, all nodes can be connected to each other.

The next step is to take a closer look at blockchain. Blockchain governance is organized either via an independent blockchain network, a participating blockchain network as a connection to an existing blockchain network or as an integrated blockchain network. The distinction between light(weight) nodes and full nodes is particularly relevant for determining communication with the blockchain. The main difference is that, unlike a full node, a light(weight) node does not store the entire blockchain and can only send and process information.

IoT devices that are not clearly identifiable for the blockchain fall into the category of no node (e.g. via communication via an IoT cloud server). A cloud server, an enterprise server (with RPC function, for example), a light(weight) node or a full node can be used as a gateway to the blockchain. With the cloud server and company server, signing only takes place when the data is received by the central server. The full node must be located in the same local network as other IoT devices and is then responsible for signing, transmission and mapping (matching IoT device ID and private key). IoT devices with sensors and an integrated light(weight) node are also able to sign themselves and transfer the collected data to the blockchain, but light(weight) nodes cannot communicate with each other, i.e. with other light(weight) nodes.

Identification and Security: The third dimension comprises identification and security. The identification systems Self-Sovereign Identity (SSI), Bring Your Own Identity (BYOI), Public Key Infrastructure (PKI) and

Decentralized Public Key Infrastructure (DPKI) are used to give objects in cyber-physical systems a digital identity. With SSI, the user receives identity features and authorizations in the form of cryptographically secured digital proofs, which are called verifiable credentials, and can manage and verify these independently using a digital wallet without direct contact with the issuer. In this context, BYOI refers to the idea and goal of being able to use this personal identity in any environment, be it private or business, for online shopping or in an official context. PKI uses digital signatures as an identity. A private key, which is only in the possession of the user, enables content and documents to be signed. The public key allows anyone to verify the signature. The security of the infrastructure depends on the trustworthiness of the third party; DPKI addresses this weakness and uses a blockchain instead of key servers (third parties).

The guiding principle is the hierarchy-free web of trust, in which users confirm the credibility and accuracy of each other's data. Nodes participating in the blockchain are able to secure the origin and security of their collected data with their signature. This also works without publishing their own identity and with the help of various security mechanisms. For security and privacy in blockchain-based systems, the security mechanisms Anonymous Digital Signatures, Mixing, Homomorphic Encryption Algorithms, Secure Multiparty Computation Protocols or Non-interactive Zero-Knowledge Proof System can be integrated.

MD	Dimensions	Characteristics							MEX
Device Differentiation	Performance	Low-end Device		Middle-end Device		High-end Device			Y
	Equipped Systems	Sensor System		Actuator System		Control System	Regulation System	Visual Indication	N
	Communication Technologies	Wired				Wireless			N
		Local Area Network	Sigfox	Software Defined Networks		Personal Area Network	Wireless Area Network	Mobile / Neul	N
Network Integration	IT Architecture	Centralized				Decentralized			Y
	Network Topology	Star		Point-To-Point		Mesh			Y
	Blockchain Governance	Independent Blockchain-Network		Participating (Connection to existing Blockchain-Network)		Integrated (BaaS, Cloud-based)			Y
	Blockchain Types	Public Permissionless		Consortium		Private Permissioned			Y
	Blockchain Identifiability	No Node		Light(weight)-Node		Full-Node			Y
	Gateway	Cloud Server		Enterprise Server		Other Device	No Gateway		Y
Identification and Security	Identity Management	Self-Sovereign Identity		Bring Your Own Identity		Public Key Infrastructure	Decentralized Public Key Infrastructure		Y
	Security Mechanism	Anonymus digital signatures	Non-interactive zero-knowledge proofs	Homomorphic Encryption Algorithm		Secure multiparty calculation protocol	Attribute-based encryption algorithm	Mixing Procedures	N

Fig. 2: Blockchain Devices Taxonomy

6. Conclusion

In this paper, we have explored the landscape of blockchain devices, emphasizing their classification and the taxonomy that underpins their diverse applications. Through a detailed examination, we have identified and categorized these devices based on their type, integration level, and application domain, providing a comprehensive framework for understanding their roles and functionalities within the blockchain ecosystem.

Our analysis highlights the importance of distinguishing between various blockchain devices, including IoT devices, mobile devices, and specialized hardware, each serving distinct purposes and industries. The integration level—ranging from full nodes to light and hybrid nodes—plays a crucial role in defining their operational capabilities and resource requirements. Additionally, the application domains, such as supply chain management, environmental monitoring, compliance documentation, underscore the versatility and significance of these devices in real-world scenarios.

The proposed taxonomy not only aids in organizing existing blockchain devices but also paves the way for future research and development. By providing a structured approach to device classification, it enables researchers and practitioners to better understand the nuances of blockchain technology and its practical implementations. As blockchain continues to evolve, the insights derived from this taxonomy will be instrumental in advancing device design, enhancing functionality, and addressing emerging challenges in the field. In summary, this paper contributes to the body of knowledge on blockchain devices by offering a detailed classification and taxonomy, thus facilitating a deeper understanding and encouraging further exploration of this rapidly advancing technology.

References

[1] Hanseatic Blockchain Institute, Stand der Blockchain Adoption in der deutschen Wirtschaft, W3NOW.DE (2024).

[2] B. Teoh, Solving the blockchain oracle problem to enable supply chain mass adoption, AIP Conference Proceedings 2582 (2023).

[3] J. Maaßen, T. Gürpinar, M. Austerjost, J. Kamphues, Entwicklungsrahmen von Blockchain Devices, Scientific Report, Blockchain Navigator (2021).

[4] T. Gürpinar, M. Austerjost, J. Kamphues, M. Henke, Blockchain technology as the backbone of the internet of things – A taxonomy of blockchain devices, Conference on Production Systems and Logistics – CPSL (2022).

[5] A. Grünewald, T. Gürpinar, C. Culotta, Archetypes of blockchain-based business models in enterprise networks, Information Systems and e-Business Management (2024).

[6] A. Alphonse, M. Starvin, Blockchain and Internet of Things – An Overview (2020).

[7] T. Gürpinar, R. Ashraf, M. Henke, Integrating blockchain technology in supply chain management - a process model with evidence from current implementation projects, Hawaii International Conference on System Sciences (2024).

[8] E. Lichtenthaler, Methoden der Technologie-Früherkennung und Kriterien zu ihrer Auswahl, in: M. G. Möhrle, R. Isenmann (Eds.): Technologie-Roadmapping, 3rd ed, Berlin (2008), p. 59-84.

[9] D. Specht, S. Behrens, Integration der Technologieplanung in die strategische Geschäftsfeldplanung mit Hilfe von Roadmaps, in: M. G. Möhrle, R. Isenmann (Eds.): Technologie-Roadmapping, 3rd ed, Berlin (2008), p. 387-396.

[10] S. Lempert, IoT-Software-Plattformen: Methode zur Bewertung und Auswahl der am besten geeigneten Plattform, Springer Gabler Wiesbaden (2021).

[11] J. Gausemeier, C. Plass, Zukunftsorientierte Unternehmensgestaltung: Strategien, Geschäftsprozesse und IT-Systeme für die Produktion von morgen, 2nd ed, Hanser (2014).

[12] R.C. Nickerson, U. Varshney, J. Muntermann, A method for taxonomy development and its application in information systems, European Journal of Information Systems (2013).

[13] A. Vaghani, T. Gürpinar, N. Große, A Taxonomy Characterizing Blockchain-Empowered Services for the Metaverse, Blockchain and Cryptocurrency Conference (2022).

[14] M. Debe, K. Salah, R. Jayaraman, I. Yaqoob, J. Arshad, Trustworthy Blockchain Gateways for Resource-Constrained Clients and IoT Devices, IEEE Access (2021).

[15] C. Bormann, M. Ersue, A. Keranen, Terminology for Constrained-Node Networks, Internet Engineering Task Force (2014).