3rd Conference on Production Systems and Logistics

Blockchain technology as the backbone of the internet of things – A taxonomy of blockchain devices

Tan Gürpinar[1], Max Austerjost[2], Josef Kamphues[2],
Jonas Maaßen[1], Furkan Yildirim[1], Michael Henke[1]
[1]*Chair of Enterprise Logistics, TU Dortmund University, Dortmund, Germany*
[2]*Fraunhofer Institute for Material Flow and Logistics, Dortmund, Germany*

Abstract

While the number of blockchain ecosystems is growing, enterprises are confronted with the decision on how data can be securely and reliably transferred to blockchains. Even though current blockchain solutions proof to be a secure way for cross-enterprise data exchange, the data entries and respective devices might still be tampered and therefore build the focal point of this paper. To give an introduction to blockchain devices, current definitions and relevant device configurations, network connections and communication opportunities are gathered through a systematic literature research. The findings are then clustered and discussed with blockchain experts in a semi-structured interview series. Finally, the paper presents a characterization scheme for blockchain devices in form of a multi-dimensional taxonomy and concludes with further research needs. The outcome of the paper also contributes to practice as the taxonomy may also be used as a basis for management decisions.

Keywords

Blockchain Technology; Internet of Things; Industry 4.0; Hardware Devices; Supply Chain Management

1. Introduction

Progressive digitization and globalization lead to various challenges in today's supply chains. Transparency, security and trust are fundamental factors that play a particularly important role in cross-company business processes between both cooperating and competing companies [1]. Traditional approaches for data exchange often fail to manage relevant information in a way that is both transparent for business partners and at the same time safe and trustworthy [2]. Current approaches also pose risks in terms of system failures, integrity, authenticity, and performance bottlenecks [3]. As a result, companies are striving to adapt to these changing conditions and pilot blockchain solutions in various industries [4,5]. Blockchain technology pursues a decentralized approach for data storage and management creating enormous potential for numerous use cases [6]. Logistics and supply chain management in particular pose a suitable application area, as information can be securely exchanged across the entire value chain [7,8]. Still, for this purpose the help of additional technologies, such as devices to access data from the Internet of Things (IoT) is necessary [9]. Many studies on the possibility of using blockchain technology in real world use cases neglect this necessary interplay of technologies. Nevertheless, only by having the right and correct data stored on the blockchain, it makes sense to benefit from its technical functionalities such as immutability and tamper-proof storage [10].

Until today, numerous blockchain projects remained in a Proof-of-Concept (PoC) status as they did not manage to organize a sufficient interplay of technologies and integrate proper devices in their blockchain networks [11,12]. To address this issue, the Ministry of Economic Affairs, Innovation, Digitalization and

Energy of North Rhine-Westphalia is funding the Blockchain Europe Project and supports this research paper that answers the following research questions:

1. What is a blockchain device and by the use of which dimensions can it be characterized?

2. Which ways exist to integrate devices in a blockchain system and which identity and security mechanisms need to be considered?

To answer these research questions, in the next chapter necessary background information on IoT and blockchain devices is explained. After that the systematic literature procedure, taxonomy development and expert interview approach are explained as used methodologies. Finally, a characterization scheme is presented in form of a taxonomy and discussed in detail. The paper concludes with a summary and further research needs.

2. Background and state of the art

From IoT devices to blockchain devices

An Internet of Things (IoT) device is a physical object that has mechanical or electrical components [13]. It is also "smart" because it is equipped with sensors and microprocessors, enabling the IoT device to perceive and process its environment [14,15]. A further essential characteristic of an IoT device is its digital networking with other devices via standard internet technologies, enabling IoT devices to communicate and perform their tasks automatically [13]. Via equipment systems, such as a monitor, it is possible for humans to interact with the IoT device. Logistics and supply chain management are one of the main application domains for linking blockchain with the Internet of Things and respective devices. Due to the interconnection of resources and goods, both within and across companies, which exchange their states or negotiate interactions, secure storage locations are necessary to keep track of the value-adding activities. Here, the blockchain enables communication between IoT devices as well as the verifiable transmission of information. When used in conjunction with smart contracts, industrial equipment can autonomously provide paid services, report maintenance needs, issue invoices, and make debits. An example of the data that can be exchanged within supply chains is vehicle maintenance data and wear data measured in real time and transmitted directly, conditions such as fill level indicators, derivative indications, or temperature indications for goods subject to a refrigerated container warranty [16]. All of this information triggers follow-up actions, such as intervening when a temperature is exceeded based on tolerance limits or when a vehicle maintenance due date has been exceeded [17].

Blockchain devices - a status quo

Blockchain devices can be represented by different IoT devices, e.g. smartphones, tablets, temperature sensors, or hardware wallets (storage of tokens) that communicate with a blockchain. The first approaches to blockchain devices can be found in the literature: Griggs et al. (2018) designed a blockchain system based on a private Ethereum framework. In this system, sensors communicate with IoT devices that invoke smart contracts and write records of all events on-chain. The IoT device in this system builds a link between sensors and blockchain nodes. The device comes into play as a smartphone that makes patient data visible via appropriate software [18]. Caro et al. (2018) developed a blockchain-based food tracking solution on Ethereum and Hyperledger Sawtooth. In this solution, IoT devices are integrated to process GPS data. By collecting and processing the data directly, IoT devices have direct access to the data and store it as a full node on the blockchain system, ensuring transparent and verifiable traceability. On a truck installed devices scan the batch packaging via an RFID tag and thereby identifiy current goods. When the truck starts moving, the device starts monitoring the temperature and GPS position. [19]. Laszka et al. (2017) describe a privacy preserving energy transactions (PETra) solution for transactive microgrids that allows consumers to trade energy without sacrificing their privacy. PETra is built on distributed ledgers and provides anonymity for

communication, bidding, and trading. In this solution, the development of an IoT infrastructure is described, but it is not defined exactly which device communicates with the blockchain and how. The device mentioned is a smart meter, which must be deployed and authorized at each prosumer (producer and consumer) to measure the prosumers' energy production and consumption in a tamper-proof manner [20]. Grecuccio et al. (2020) report a development of a software framework that enables IoT devices to interact directly with an Ethereum-based blockchain. This solution provides an alternative way to integrate a broad category of IoT devices without relying on a centralized intermediary and third-party service. Each IoT device has its own gateway and can sign transactions locally and offline. Moreover, each IoT device is identified by its address within the blockchain and can thus be a target for potential smart contract events [10].

3. Methodology

Structured literature review

Methodically, a systematic literature review according to 21 was conducted for the scientific base of this paper it is highly suitable for opening up emerging topics. We applied numerous search strings in different combinations. "Blockchain Technology" and "Distributed Ledger Technology" in combination with "Devices", "Internet of Things", "Smart Devices", "IoT Devices", "CPS", "CPPS", were used as keywords. In order to narrow down the field of observation in some places, "Supply Chain Management", "Logistics", or "Enterprise Networks" were additionally added to exclude paper without real world application. Finally, we collected 38 relevant papers that we extended by 12 papers through forward and backward research.

Taxonomy development

Following up on the literature review, we developed a taxonomy based on the approach of 22. The method with its roots in Information Systems (IS) research consists of seven steps (see **Figure 1**). First, one must establish a meta-feature that defines the purpose of the taxonomy. Second, end conditions must be established, and an approach must be chosen. The choices are the conceptual-empirical approach or the empirical-conceptual approach. Each approach is divided into three steps. In the conceptual-empirical approach, the focus is on conceptualizing features and dimensions before examining the objects and then creating a taxonomy, while in the empirical-conceptual approach, the focus is on extracting features and dimensions from the objects before grouping them into a taxonomy. In all iterations, we followed the empirical-conceptual approach. These two approaches need to be run repeatedly until the final conditions are met. Nickerson et al. (2013) defined 13 end conditions, divided into eight objective and five subjective (concise, robust, comprehensive, extensible, and explanatory) conditions. We describe the development of our taxonomy and meta-feature, as well as the dimensions with their features, in the next section.

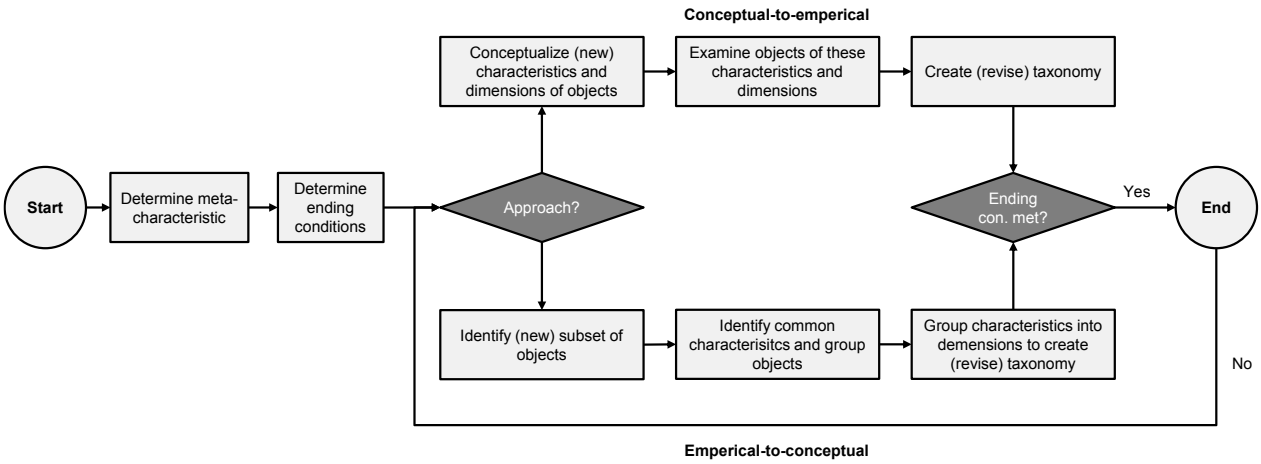


Figure 1: Taxonomy development according to Nickerson et al. (2013)

Expert interviews

The main goal of our taxonomy is to characterize blockchain devices in order to differentiate the large number of devices in the blockchain ecosystem. Therefore, we defined "core features and their feature manifestations of IoT Devices connected to a Blockchain network" as a meta-characteristic for our taxonomy. This meta-characteristic was the basis for identifying additional dimensions and characteristics and did not change during the iterations. The development of the taxonomy required six iterations until we met all 13 final conditions and thus reached the final state. In all iterations, we followed the "Empirical-Conceptual" approach. For additional discussion of the taxonomy with practitioners and to elicit new as well as elaborate on already identified requirements for blockchain devices, semi-structured guided expert interviews were conducted and transcribed according to the clean verbatim transcription approach [23]. The analysis was conducted along the methodology of qualitative content analysis according to 24. The experts listed in Table 1 were approached for interviews.

According to the guidelines, the interviews were scheduled for 45 minutes each. Due to additional explanations, some interviews took a longer time. The backgrounds of the experts cover the fields of business, computer science, logistics, supply chain management and mechanical engineering. The organizations represent application-oriented research institutes and consultancies, as well as a small and large company that both already implemented blockchain applications. All experts have been working on the blockchain topic for at least one year. During each iteration, the derived dimensions for the taxonomy and respective features were discussed, added or deleted.

Table 1: Overview expert interviews

Title	Company	Industry	Date	Duration
Blockchain Developer	Consulting company for enterprise blockchain solutions	Consulting	May 2021	00:45 h
Blockchain Researcher	University chair researching in decentralised markets	Research	May 2021	00:51 h
Consultant	Logistics Service Provider	Logistics	June 2021	01:23 h
CEO	Blockchain Start-up	Logistics and Technology	June 2021	01:16 h
Blockchain Expert	Consulting company for enterprise blockchain solutions	Consulting	June 2021	00:55 h
Researcher in the field of CPPS	University chair researching in CPPS and connection to blockchain systems	Research	June 2021	00:45 h

In the first iteration, we analysed the first 38 papers for the basis of our taxonomy and met seven final conditions set by Nickerson. In this state, we identified 19 dimensions with multiple characteristics each. After discussions in the author team, we realized that some dimensions were not meaningful and in addition duplications occurred, so we decided to reduce five dimensions. In the second and third iteration, we examined the additional 12 papers. After the iterations, we discussed 14 dimensions and met ten final conditions. In the fourth iteration, we decided against categorizing industry use cases and added new dimensions, such as system characteristics, which were used to categorize hardware together with two experts from the interviews conducted in May. Due to ambiguity about whether the system features were low-end or high-end, we decided against it in the fifth iteration after discussions with two further experts from the interviews series in June. We also removed dimensions that related too strongly to IoT. Instead, we added three major layers, which evolved into the final Device Layer, Integration Layer, and Blockchain Layer as we went along. In the last iteration, the taxonomy was finally discussed together in the last two experts from the June interview series and some features were replaced, for example, concrete consensus algorithms emerged instead of categories of consensus algorithms as before, which again was difficult to

prove. This resulted in a concise, robust, comprehensive, extensible, and explanatory taxonomy that does not include repetitive dimensions or features to classify all objects identified in the literature review.

4. Findings and discussion

The taxonomy serves as an answer to the research questions of this paper, as it characterizes types of blockchain devices and requirements for a blockchain device to securely and reliably put data on the blockchain. As shown in Table 2, the taxonomy consists of eleven dimensions with 44 characteristics. To increase the transparency and understanding of the taxonomy, we grouped the identified dimensions into the three layers: Device differentiation, blockchain integration, as well as identity and security mechanisms. In addition, an asterisk (*) at the end of a feature indicates whether it is also possible to select multiple characteristics. We visualise the taxonomy as a morphological box, since this is a common way of visualising a taxonomy and it generally illustrates the set of relations contained in a problem complex in an intuitive way [25,26].

Device differentiation

Performance: IoT devices can basically be divided into low-end and high-end on the criteria of their hardware equipment (computing power, storage capacity, battery capacity, communication capability, etc.). The main difference is the executability of software based on traditional operating systems (such as Linux). While a low-end device cannot execute software based on traditional operating systems, the high-end device is able to execute such software [27–29]. In addition, limited memory capacity, communication capability (broadband), and computational power are not particularly suitable to support resource-intensive distributed ledgers, but sufficient to be able to use the services of a distributed ledger network (e.g., by using an API) [29].

Equipped systems: The interaction with the environment functions via measurement, control and regulation technology. Only sensors that perceive the environment are used for measurement technology. For example, temperature sensors perceive the outside temperature or pressure sensors perceive certain forces [15]. In contrast, control technology exclusively uses actuators. Actuators are the signal converter counterpart to sensors and form the actuators in a control loop, i.e. they convert signals (e.g. commands from the control computer) into mechanical movement or other physical variables (e.g. pressure or temperature). In control technology both, sensors and actuators, are used. The sensor system displays current measured values, while the actuator system triggers a specific action when a measured value is exceeded [18,27,30].

Communication Technologies: One of the main features of blockchain devices is their communication with each other or with other systems via internet. Communication technologies include wired technologies such as the Local Area Network (Ethernet, PLC, bus systems) and wireless ones, such as Wireless Personal Area Networks that represent the most widely used communication technology among IoT devices and have a range of approximately 100m. Examples of WPAN are devices with Bluetooth, ZigBee or Z-Wave equipment [32,29,31]. WLAN, as another wireless communication technology and enables ranges of up to 1 km. In this category, Wi-Fi is the most widely used standard [29]. LPWAN is a communication technology that is predicted to grow rapidly. Key factors are the extremely long battery life and a maximum communication range of over 20 km [29]. Mobile networks, such as GSM, 3G, 4G and 5G, are used for the long-range operation of IoT devices. 2G, 3G and 4G technologies have long been the only option for device connectivity. Now that LPWAN and also 5G are gaining prominence, these legacy mobile standards are expected to give up their share to the new technologies [29,31].

Table 2: Taxonomy for Blockchain Devices

MD	Dimensions	Characteristics							MEX
Device Differentiation	Performance	Low-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	Anonym Digital Signatures	Non-interactive Zero-Kowledge Proofs	Homomorphic Encryption Algorithm	Secure Multiparty Calculation Protocol	Attribute-based Encryption Algorithm		Mixing Procedures	N

MD = Meta-Dimensions; MEX = Exclusivity

Network integration

IT architecture: IT architectures especially in the area of IoT can be divided into centralized and a decentralized types. In centralized architectures, a central hub is used to provide backend services for smart devices. Some of the most important centralized capabilities are event processing, events notification and real-time analytics. In addition to the mentioned capabilities there are also scenarios where decentralized communication between IoT devices is required without the need of a central hub. There are many examples of decentralized IoT applications like peer-to-peer messaging or decentralized auditing and file sharing. [4,31]

Network topologies: The network topologies which are used in IoT can be split into three categories: star, point-to-point and mesh. The point-to-point topology is based on a direct connection between the nodes. In star networks every device is connected to a central hub. In a mesh network topology every node can be connected with each other. There are six networking attributes: latency, throughput, fault resiliency, scalability, the number of hops and range. These attributes can help developers of IoT Applications in knowing the capabilities of the different network topologies to choosing the best topology for their own Application [31].

Blockchain-Governance: Blockchain governance determines the organisational structure, jurisdictions in and requirements for the usage of blockchain-based applications as well as the consortium agreement process. Three governance structures can be distinguished. On the one hand, an independent blockchain network can be established and managed for the individual use case of a company. On the other hand, it is possible to join and participate in already existing blockchain networks and accustom to the already existing governance. Finally, it is also possible to make use of external service providers who make a blockchain network available. These include blockchain-as-a-service- or cloud-based solutions. [33,34]

Blockchain types: public blockchain represents an ecosystem, publicly visible to everyone. This type of blockchain has become known through the crypto networks Bitcoin and Ethereum. [35] Private blockchains (e.g. Multichain) offer governance rules that have to be developed individually during network construction.

With this type, data is shared in a restrictive manner and participants can only view defined transactions. A consortium blockchain is a special form of private blockchain because the consensus process participation is distributed among several organisations in the P2P network. The transaction activity is isolated from the public [35]. Hyperledger Framework of the Linux Foundation can be mentioned as an exemplary framework. A hybrid blockchain offers public access to the network for everyone and at the same time a trust-based governance structure. [36]

Blockchain identifiability: IoT Devices without a direct connection to the blockchain network cannot be identified via the blockchain, as they communicate indirectly (e.g. via a cloud server) with the blockchain network. [10] However, there are also devices that can identify themselves in a blockchain network. On the on hand, there are light clients which are nodes with a computing capacity and network bandwidth that is too low to download and check the entire blockchain [37]. Ethereum has a client application named Mist Browser, a user-friendly wallet also known as a Light Node. This Light Node connects to a blockchain to perform only basic functions of a full node, such as sending and receiving cryptocurrencies which only requires a wallet application on the IoT device [38,39]. A light node is thus able to sign and broadcast transactions on its own. On the other hand, there are devices that hold a full copy of the blockchain and have sufficient processing and storage capacity to act as a Full Node. IoT home gateways, for example a Raspberry PI, can already participate in the blockchain as a full node and thus potentially support blockchains [29].

Gateway: One possible solution for connecting devices consists of a communication between a central cloud server and the devices, also called IoT cloud server. The server is responsible for collecting data from the IoT devices and for storing this data in the blockchain. One of the weak points of this solution is the central server as a single point of failure. Another crucial vulnerability is the lack of digital signatures of the IoT devices. The data that is sent to the blockchain is not signed on the spot by the device, but only when the data is received by the central server. This means that the authenticity and integrity cannot be guaranteed from the source [10]. Based on the remote procedure call (RPC) developed by Birrell and Nelson in 1984 [40], there is the possibility of triggering the execution of a procedure on a remote enterprise server through embedded gateways. The enterprise server provides the gateways with an API, which enables interaction with the blockchain. The gateways should be uniquely identifiable, sign transactions locally and offline with their private keys before communicating with the RPC server. Using its own addresses within the blockchain, each IoT device can be identified and thus be a target for possible smart contract events [10]. Apart from that, other devices can act as gateways to enable a communication from smaller low-end-devices to the blockchain [37].

Identity and security management

Identity management: A relatively new approach to identity management is the Self-Sovereign Identity (SSI) paradigm based on decentralized infrastructures. Typical for SSI is the focus on the user of the digital identity, who is in possession of his personal data himself and decides on third-party access [41]. The user receives identity features and corrections in the form of cryptographically secured digital proofs - the verifiable credentials - and can manage them independently by means of a digital wallet [42]. Bring Your Own Identity (BYOI) in this context refers to the idea and goal of being able to use this own identity on demand in any environment, be it private or business [41]. Public Key Infrastructures (PKI) are one of the mechanisms for managing keys in public key cryptographic systems. A private key owned only by the user allows the signing of different contents and documents. The public key then allows anyone to verify the respective signature [43]. Efforts to adapt PKI systems to emerging challenges, result in the development of Decentralized PKI (DPKI). One guiding and already practiced idea is the hierarchy-free web-of-trust, in which users mutually confirm credibility and correctness of associated data and trust in an assigned public key while network partners authenticating it [41].

Security mechanisms: The idea of anonymous digital signatures is that users or objects within the blockchain network can use pseudonyms to hide their true identity and thus secure their privacy [14,44]. Mixing procedures involve mixing users' or objects' values with each other, which leads to confusion within the network. The identities can be disguised with this mechanism. To protect digital assets from attackers, Mixcoin, for example, obfuscates users by mixing currencies simultaneously and also uses an accountability mechanism to detect asset thefts [14,44]. The homomorphic encryption algorithm is a technique that enables computations to be performed on the cipher text itself. Hence, it is not necessary to convert data into plaintext in order to perform an operation on it. Homomorphic cryptography can be easily applied to the data on-chain without changing the blockchain properties, which ensures privacy and allows data to be verified and managed only in encrypted form. Secure Multiparty Computation Protocols (SMCP) are a class of algorithms that allow a group of mutually untrusting actors to evaluate functions without having to reveal their private inputs [14,44]. Attribute Based Encryption (ABE) is a cryptographic algorithm that uses the attributes as regulatory factors for the cipher text encrypted with the user's private key. The text data can only be decrypted if the attributes of the decoders match the encrypted data [14,44].

5. Conclusion

Previous research has provided good reasons to believe that blockchain solutions will diffuse in various industries over time. To exploit all functionalities of the technologies, getting the right data in an integer and traceable manner on chain, constitutes an important challenge. Appropriate configured blockchain devices address this challenge and are described in this paper by (1) hardware constitution as well as (2) technical possibilities to connect them to the blockchain systems and (3) operate identity as well as security management measures.

The central outcome of the paper is a taxonomy characterizing relevant dimensions of blockchain devices, scientifically substantiated by literature research and expert interviews. It became clear that current enterprise blockchain projects use different blockchain devices with different and individual characteristics. Thus, a strict determination of a singular blockchain device is not possible. However, our characteristics help to understand the range of different device types and possibilities to integrate them in a blockchain system. Therefore, in a first dimension, the devices are differentiated according to their performance and energy efficiency as well as equipped system and communication technologies. A second dimension addresses the type and topology of IoT platform the device gains access to; the type of governance and framework of the connected blockchain system; as well as the way the device is identified by and connected with the system. A final layer addresses possible identity and security management measures for the device.

This outcome aims to advance previous research on devices that are described in blockchain research and delivers a first-ever possibility to classify blockchain devices. The investigation is of considerable relevance to blockchain scholars as well as practitioners that find themselves in PoC blockchain projects and work on device integrations. In order to further validate the developed taxonomy real world blockchain devices will be described by its means in a future research work by the Blockchain Europe Project. Blockchain scholars are invited to build up on the taxonomy and apply it in further case studies to demonstrate international acceptance and applicability in practice.

Acknowledgments

The work was funded by the Ministry of Economic Affairs, Innovation, Digitalization and Energy of the State of North Rhine-Westphalia.

References

[1] Henke, M., 2003. Strategische Kooperationen im Mittelstand: Potentiale des Coopetition-Konzeptes für kleine und mittlere Unternehmen (KMU). Zugl.: München, Techn. Univ., Diss., 2002 u.d.T.: Henke, Michael: Strategische Kooperationen kleinerer und mittlerer Unternehmen (KMU) unter besonderer Berücksichtigung des Coopetitions-Ansatzes. Verl. Wiss. & Praxis, Sternenfels, 208 pp.

[2] Gelhaar, J., Guerpinar, T., Henke, M., Otto, B., 2021. Towards a Taxonomy of Incentive Mechanisms for Data Sharing in Data Ecosystems. Asia Conference on Information Systems.

[3] Neugebauer, R. (Ed.), 2018. Digitalisierung, 1. Aufl. 2018 ed. Springer Berlin Heidelberg, 416 pp.

[4] Große, N., Leisen, D., Gürpinar, T., Forsthövel, R.S., Henke, M., ten Hompel, 2020. Evaluation of (De-) Centralized IT technologies in the fields of Cyber-Physical Production Systems. CPSL.

[5] Gürpinar, T., Guadiana, G., Ioannidis, P.A., Straub, N., Henke, M., 2021. The Current State of Blockchain Applications in Supply Chain Management, 168–175.

[6] Heines, R., Gürpinar, T., 2021. Towards a Typology of Blockchain-based Applications: a Conceptualization from a Business Perspective. BAS21 Mittweida.

[7] Grosse, N., Guerpinar, T., Henke, M., 2021. Blockchain-Enabled Trust in Intercompany Networks Applying the Agency Theory, in: 2021 3rd Blockchain and Internet of Things Conference. Ho Chi Minh City Vietnam.

[8] Gürpinar, T., Harre, S., Henke, M., Saleh, F., 2020. Blockchain Technology – Integration in Supply Chain Processes. Hamburg International Conference of Logistics.

[9] Dujak, D., Sajter, D., 2019. Blockchain Applications in Supply Chain, in: Kawa, A., Maryniak, A. (Eds.), SMART Supply Network. Springer International Publishing, Cham, pp. 21–46.

[10] Grecuccio, J., Giusto, E., Fiori, F., Rebaudengo, M., 2020. Combining Blockchain and IoT: Food-Chain Traceability and Beyond. Energies 13 (15), 3820.

[11] Mika, B., Goudz, A., 2019. Blockchain-Technologie in der Energiewirtschaft: Blockchain als Treiber der Energiewende, 1. Aufl. 2020 ed. Springer Berlin Heidelberg, Berlin, Heidelberg, 113 pp.

[12] Varriale, S., 2019. Unequal Youth Migrations: Exploring the Synchrony between Social Ageing and Social Mobility among Post-Crisis European Migrants. Sociology 53 (6), 1160–1176.

[13] Hompel, M. ten, Bauernhansl, T., Vogel-Heuser, B., 2020. Handbuch Industrie 4.0. Springer Berlin Heidelberg, Berlin, Heidelberg, 631 pp.

[14] Fridgen, G., Guggenberger, N., Hoeren, T., Prinz, W., Urbach, N., 2019. Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik. https://www.bmvi.de/SharedDocs/DE/Anlage/DG/blockchain-gutachten.pdf?__blob=publicationFile.

[15] Kruse Brandão, T., Wolfram, G. (Eds.), 2018. Digital Connection. Springer Fachmedien Wiesbaden, Wiesbaden.

[16] Pandey, R., 2001. Essentials of Supply Chain Management. OPSEARCH 38 (2), 238–239.

[17] Voß, P.H., 2020. Logistik – die unterschätzte Zukunftsindustrie. Springer Fachmedien Wiesbaden, Wiesbaden.

[18] Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T., 2018. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. Journal of medical systems 42 (7), 130.

[19] Caro, M.P., Ali, M.S., Vecchio, M., Giaffreda, R., 2018. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation, 1–4.

[20] Laszka, A., Dubey, A., Walker, M., Schmidt, D., 2017. Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers, 1–8.

[21] Baumeister, R.F., Leary, M.R., 1997. Writing Narrative Literature Reviews. Review of General Psychology 1 (3), 311–320.

[22] Nickerson, R.C., Varshney, U., Muntermann, J., 2013. A method for taxonomy development and its application in information systems. European Journal of Information Systems 22 (3), 336–359.

[23] McLellan, E., MacQueen, K.M., Neidig, J.L., 2003. Beyond the Qualitative Interview: Data Preparation and Transcription. Field Methods 15 (1), 63–84.

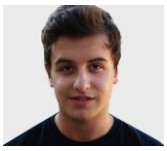
[24]Mayring, P., Fenzl, T., 2019. Qualitative Inhaltsanalyse, in: Baur, N., Blasius, J. (Eds.), Handbuch Methoden der empirischen Sozialforschung. Springer Fachmedien Wiesbaden, Wiesbaden, pp. 633–648.
[25]Ritchey, T., 2006. Problem structuring using computer-aided morphological analysis. Journal of the Operational Research Society 57 (7), 792–801.
[26]Szopinski, D., Schoormann, T., and Kundisch, D., 2020. Visualize Different: Towards Researching the Fit Between Taxonomy Visualizations and Taxonomy Tasks. Proceedings of the Wirtschaftsinformatik.
[27]Hahm, O., Baccelli, E., Petersen, H., Tsiftes, N., 2016. Operating Systems for Low-End Devices in the Internet of Things: A Survey. IEEE Internet Things J. 3 (5), 720–734.
[28]Noura, M., Atiquzzaman, M., Gaedke, M., 2019. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mobile Netw Appl 24 (3), 796–809.
[29]Vermesan, O., 2018. Next Generation Internet of Things. River Publishers, Aalborg, 352 pp.
[30]Hasenjäger, E., 2015. Regelungstechnik für Dummies: Auf einen Blick: Prozesse, Reglertypen, Regelkreise und die mathematischen Gleichungen verstehen, 1. Aufl. ed. Wiley-VCH, Weinheim, 443 pp.
[31]Yaqoob, I., Ahmed, E., Hashem, I.A.T., Ahmed, A.I.A., Gani, A., Imran, M., Guizani, M., 2017. Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Commun. 24 (3), 10–16.
[32]Hinckeldeyn, J., 2019. Blockchain-Technologie in der Supply Chain: Einführung und Anwendungsbeispiele. Springer Fachmedien Wiesbaden; Imprint: Springer Vieweg, Wiesbaden, 56).
[33]van Pelt, R., Jansen, S., Baars, D., Overbeek, S., 2021. Defining Blockchain Governance: A Framework for Analysis and Comparison. Information Systems Management 38 (1), 21–41.
[34]Werner, J., Zarnekow, R., 2020. Governance of Blockchain-Based Platforms, in: Gronau, N., Heine, M., Krasnova, H., Pousttchi, K. (Eds.), Proceedings der 15. Internationalen Tagung Wirtschaftsinformatik 2020. GITO mbH Verlag für Industrielle Informationstechnik und Organisation, Berlin, pp. 128–141.
[35]Hileman, G., Rauchs, M., 2017. 2017 Global Blockchain Benchmarking Study. SSRN Journal.
[36]Tobin, Reed, 2017. The Inevitable Rise of Self Sovereign Identity. Sovrin Foundation. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf. Accessed 27 July 2021.
[37]Al-Bassam, M., Sonnino, A., Buterin, V., 2018. Fraud and Data Availability Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Majorities, 33 pp. http://arxiv.org/pdf/1809.09044v5.
[38]Dannen, C., 2017. Introducing Ethereum and Solidity. Apress, Berkeley, CA.
[39]Gürpinar, T., Ashraf, S.R.B., Broza-Abut, N., Sparer, D., 2022. Blockchain-Based Infrastructure for Product Traceability in the Medical Supply Chain, in: Moumtzoglou, A., Borah, M.D., Zhang, P., Deka, G.C. (Eds.), Prospects of Blockchain Technology for Accelerating Scientific Advancement in Healthcare. IGI Global, pp. 119–134.
[40]Birrell, A.D., Nelson, B.J., 1984. Implementing remote procedure calls. ACM Trans. Comput. Syst. 2 (1), 39–59.
[41]DIN SPEC 3103:2019-06, 2019. Blockchain und Distributed Ledger Technologien in Anwendungsszenarien für Industrie 4.0.
[42]Ehrlich, T., Richter, D., Meisel, M., Anke, J., 2021. Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. HMD 58 (2), 247–270.
[43]Pal, O., Alam, B., Thakur, V., Singh, S., 2021. Key management for blockchain technology. ICT Express 7, 76–80.
[44] Idrees, S.M., Nowostawski, M., Jameel, R., Mourya, A.K., 2021. Security Aspects of Blockchain Technology Intended for Industrial Applications. Electronics 10 (8), 951.

Biography

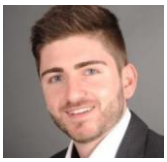
Tan Gürpinar, M.Sc. (*1991) is a researcher and field coordinator for blockchain technology at the Chair of Enterprise Logistics, TU Dortmund University. His work focuses on the effective and profitable integration of new technologies, especially blockchain technologies.

Dr.-Ing. Max Austerjost (*1986) is a researcher at Fraunhofer IML. He leads Blockchain Europe, the project to establish the European Blockchain Institute in NRW. His special research interest is making blockchain technology usable in supply chain management and logistics.

Dipl.-Ing. Josef Kamphues (*1986) is Head of Department Supply Chain Development & Strategy at Fraunhofer IML. His work focuses on the research and application of digital technologies in supply chain management with a focus on blockchain, AI and simulation.



Jonas Maaßen, B.Sc. (*1997) studies Logistics at TU Dortmund University and works as a research assistant for blockchain technology at the Chair of Enterprise Logistics, TU Dortmund University.



Furkan Yildirim, M.Sc. (*1992) is a researcher for blockchain technology at the Chair of Enterprise Logistics, TU Dortmund University. His research focuses on the utilization of tokenomics in supply chain management.

Univ.-Prof. Dr. habil. Michael Henke (*1971) is the chairholder of the Chair of Enterprise Logistics, TU Dortmund University and director of the Fraunhofer Institute of Material Flow and Logistics since 2013.