Blockchain Technologies Towards Data Privacy—Hyperledger Sawtooth as Unit of Analysis

Pascal Moriggl, Petra Maria Asprion, and Bettina Schneider

Abstract For digital business models data is the most crucial asset—this calls for increased awareness of appropriate privacy protection measures. The European Union *General Data Protection Regulation* is a consequence that followed the discussions and now forces organizations to ensure that their information ecosystems comply with the law. There is currently an emerging trend to apply blockchain technologies to business models that rely on data exchange, because the technology promises to make a centralized data authority redundant. We have taken this as the purpose for our efforts to provide insights that will help decision-makers select a suitable blockchain configuration that complies with data privacy regulatory requirements. By applying design science, we created a morphological box along with a grid, serving as a 'data privacy assessment tool' for the blockchain configuration *Hyperledger Sawtooth*. The research results can potentially be generalized to assess any other blockchain configuration.

Keywords Blockchain · Data privacy · Information security · Distributed ledger · Hyperledger Sawtooth · Information ecosystem (IES)

1 Introduction

There is a growing interest in the fields of *blockchain technologies* and *data privacy*, which is reflected in an increasing number of publications. We analyzed relevant databases (Scopus, Web of Science, and IEEE Xplore) with the result that

P. Moriggl (✉) · P. M. Asprion · B. Schneider
School of Business, Institute for Information Systems, FHNW University of Applied Sciences and Arts Northwestern Switzerland, Peter Merian-Strasse 86, 4002 Basel, Switzerland
e-mail: pascal.moriggl@fhnw.ch

P. M. Asprion
e-mail: petra.asprion@fhnw.ch

B. Schneider
e-mail: bettina.schneider@fhnw.ch

R. Dornberger (ed.), *New Trends in Business Information Systems and Technology*,
Studies in Systems, Decision and Control 294,
https://doi.org/10.1007/978-3-030-48332-6_20

in September 2019 Scopus showed 512 hits, Web of Science resulted in 398 hits and in IEEE Xplore 54 hits were returned; in comparison, in 2015 the identical keyword search in Scopus, Web of Science and IEEE Xplore led to only one hit.

Applicable since 2018, the European Union (EU) *General Data Protection Regulation* (GDPR) is a strong driver for researchers and practitioners to evaluate the impact of privacy regulations on an information ecosystem (IES) or on business processes. Over the past decade, blockchain, as an emerging technology with various configurations (e.g., Bitcoin, Ethereum, and Hyperledger) and with high disruptive potential, has enabled new opportunities to design and execute business processes; this is especially relevant for processes that involve a variety of IESs and associated stakeholders. Although there are some research activities that use blockchain configurations to ensure data privacy in IESs [1–3], there is no standardized assessment available that helps evaluate and compare different possible blockchain configurations for their suitability regarding data privacy capabilities.

One explanation for this lack of research interest might be the circumstance that under certain conditions, data privacy issues can be circumvented for blockchain applications. First, the problem of data privacy can be "outsourced" and therefore classified as not relevant because personal data could theoretically be encrypted and pseudonymized outside the blockchain (off-chain); with this approach, personal data processing risks and data privacy requirements can be by-passed for any blockchain-based solution. Another way to avoid data privacy issues is to store only *hashes* or *checksums* of the personal data on-chain. In addition, any personal data could be encrypted in order to hinder other network participants without a valid private key to see the content. However, with regard to encryption in general, it needs to be discussed whether it will withstand future advancements in technologies that potentially could decrypt its content [4].

Despite these avoidance strategies, the storing and processing of private sensitive data in blockchain configurations occurs in practice and we consider data privacy as highly relevant for our society, driving us to advance this unresolved research issue. Therefore, the goal of this study is to design a conceptual assessment—a morphological box along with an assessment grid—that allows the comparison of blockchain configurations based on their data privacy capabilities. The morphological box and particularly the grid provide a starting point for further discussions and refinements that could lead to a standardized framework for assessing data privacy in a blockchain-based IES. Target audiences are both researchers and decision-makers in organizations that analyze or plan to establish blockchain-based solutions.

This study follows a design-based research approach [5]. First, according to [5] the existing knowledge around data privacy and blockchain solutions is analyzed, condensed, and used to scope this research. Second, the design process is outlined, starting with elaborating blockchain- and privacy-related characteristics to include in our morphological box. This leads to the foundational artifact, an assessment grid, evaluated by applying it to a dedicated blockchain configuration. The artifact makes use of the morphological analysis, a general method for non-quantified modeling [6]. The development of the morphological grid follows privacy audit criteria for IESs [7, 8] adapted to be used for blockchain-based solutions dealing with private data.

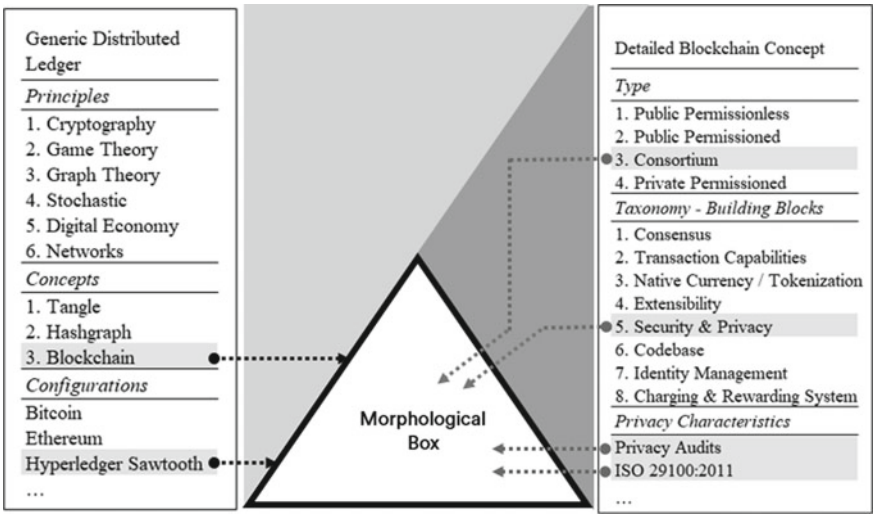

Fig. 1 Research domain resulting in a morphological box

Figure 1 shows (1) our research domain synthesis, a "Generic Distributed Ledger" with its three abstraction layers, related characteristics/attributes (left box) and (2) the elements from one "Detailed Blockchain Concept" (right box). We selected an exemplary *Hyperledger Sawtooth*, and (3) in the center of Fig. 1, the specific elements that are relevant to design our desired artifact—the morphological box (the triad and related arrows). The characters marked in grey in the left box set the artifact boundaries, whereas the ones marked in grey in the right box set its content.

The remainder of this contribution is structured as follows. The foundations of our research—data privacy and blockchain—are elaborated in Sect. 2. In Sect. 3, we discuss the characteristics forming the morphological box; as baseline, we use blockchain and data privacy characteristics to discuss relevant attributes. These include the application of the morphological box to highlight how *Hyperledger Sawtooth* fulfills data privacy requirements at the technical level. The contribution concludes in Sect. 4 with a short summary of the practicability and further research opportunities in the field of technical data privacy characteristics.

2 Foundation

The foundation section covers data privacy and blockchain as central units of analysis. It elaborates firstly the concept of data privacy and highlights its increasing relevance in digitalized IESs. Secondly, relevant essentials of blockchain will be introduced that allow demarcating the boundaries of this research.

2.1 Data Privacy

Historically, in the EU, privacy is regarded as a fundamental individual right and a social value; it can be described as "the right to private life, to be autonomous, in control of information about yourself, to be let alone" [9]. In an increasingly digitalized world, it has become common that plenty of data about individuals are created and processed electronically [10]. Therefore, privacy must be considered and established with particular care. According to a study by the Swiss Federal Office for Statistics, 87% of EU residents living in the most advanced countries in terms of digitization provide personal data of various kinds via the Internet [11, 12]. Serious data breaches—such as the scandal of Cambridge Analytica, a British company, which had harvested data from up to 87 million Facebook users without their explicit consent [13]—have revealed the importance of monitoring the processing of personal data. The EU had anticipated this requirement and responded with GDPR, which became applicable on 25 May 2018. This regulation, aiming towards protecting natural persons and their data (GDPR, Article 1), unfolds extraterritorial effects; it refers to any data processing related to individuals who are in an EU member state—irrespective whether or not the data processing itself takes place in the EU [14]. Consequently, this means every organization, across all industries and locations, except non-EU countries without EU trade relationships, must verify whether it is affected and is required to comply with GDPR [9]. As a very special case, non-EU organizations, such as higher education institutions must also consider GDPR [15]. As the new regulation not only replaces but also updates the preceding EU Data Protection Act (DPA) from 1998, several new elements have been introduced. An example is the mandatory data protection impact assessment, "a process to manage risks related to the processing of personal data by assessing and mitigating such information" [16].

In addition, the GDPR leads to a close link between data protection and information security. GDPR Article 32 explicitly obliges organizations to process personal data securely using "appropriate technical and organizational measures", such as encryption and pseudonymization. The Information Commissioner's Office (ICO), a regulatory body used to protect information rights in the public interest, confirms that concepts originally stemm from the field of information security [17], e.g. from the CIA triad [18]—a widely used model for managing information security policies. The abbreviation CIA comes from the attributes (1) *Confidentiality* as a set of rules that limits access to information, (2) *Integrity* as the assurance that the information is trustworthy and accurate, and (3) *Availability* as a guarantee of reliable access to the information by authorized people [17].

The three attributes of the CIA triad are essential information security characteristics and delineate the boundaries in which our research operates. The attributes of the CIA triad will be referred to when building and testing the research results.

2.2 Blockchain

The term blockchain first appeared in 2008 after *Satoshi Nakamoto*, a pseudonymous person or group, published an essay about a peer-to-peer electronic cash system using the terms *blocks* and *chain* [19]. Nowadays, blockchain is understood as a concept with the umbrella term *distributed ledger*. According to Burkhardt et al. [20], a distributed ledger can be defined by complementary principles, which focus on mathematical and information technology-related aspects, such as *cryptography*, *stochastics*, *graph theory,* and *network* structures. The principles themselves focus on economic aspects: 'crypto-economics' exploiting the *game theory* [21, 22] and strategies to build consensus in untrusted environments and issues of a 'digital economy', e.g. double-spending digital money or dealing with cryptocurrencies [23].

The distributed ledger principles can be assembled in particular ways forming three distinctive distributed ledger services (DLS) [24]: (1) tangle, (2) hashgraph, and (3) blockchain. The three concepts differ in their architecture, where tangle and hashgraph are based on a 'directed acyclic graph', and blockchain is based on its own 'blockchain'-technology [20]. The latter became widely known among the public and in the scientific community when in 2009 the first cryptocurrency whitepaper titled as *Bitcoin* was released [19, 25]. Today, many implementations of the blockchain concept are actively developed by researchers or leading commercial players (e.g., IBM, Intel, Ethereum Foundation).

For this study, Hyperledger is chosen as an analytical unit to test the applicability of the developed assessment instrument, the morphological box. Hyperledger is considered the most appropriate because it is an open-source collaborative effort designed to advance cross-industry blockchain technologies. The underlying design philosophy of Hyperledger fits perfectly with this research as it aims to keep ledgers distributed and make smart contracts safe, in particular for enterprise applications. Its distinctive architecture separates the core system from the application domain, which aims on the one hand to simplify blockchain application development and on the other hand allows developers to choose their preferred programming language [26]. Hyperledger is based on a global collaboration including leaders of different industries. The Linux Foundation, known as a worldwide acting non-profit technology consortium, is hosting it [26]. The selected configuration for this study, *Hyperledger Sawtooth*, in the following abbreviated as *Sawtooth* is a project under the Hyperledger umbrella. It is a modular platform for creating, deploying, and running distributed ledgers [26]. For our desired artifact, an assessment tool in the form of a morphological box, the fundamentals of blockchain set the boundaries. Table 1 consolidates the distributed ledger characteristics, namely the principles, the DLS and the configuration along with respective values (alphabetically ordered). We highlighted the values delineating the scope (italics formatting)—general distributed ledger characteristics, focusing on blockchain such as DLS and Sawtooth as the exemplary unit of analysis.

Table 1 Generic distributed ledger characteristics setting the scope of this study

Characteristics	Values					
Principle	*Cryptography*	*Digital Economy*	*Game theory*	*Graph theory*	*Networks*	*Stochastic*
Service	Tangle		Hashgraph		*Blockchain*	
Configuration	Bitcoin	Ethereum	IOTA	*Hyperledger Sawtooth*	Ripple	…

3 The Morphological Box

In the previous section, we introduced the basics of data privacy, information security, and blockchain to demonstrate research boundaries. This section elaborates the building blocks for the morphological box drawing on existing research work. It starts with the blockchain-related characteristics followed by data privacy characteristics. Currently, there is no conclusive research on blockchain configurations that best correspond to data privacy requirements because of the difficulty of matching technical features with data privacy requirements that do not necessarily dictate configuration choices.

3.1 Blockchain Characteristics

Two relevant characteristics, the "Blockchain Design Elements" and the "Blockchain Type" will be incorporated into the assessment tool. Table 2 shows both characteristics and related values; values that apply to our unit of analysis, Sawtooth, are highlighted (italics formatting).

3.1.1 Blockchain Types

When selecting the blockchain-related characteristics to build the morphological box, we first draw on one of the blockchain principles described in Sect. 2.2,

Table 2 Blockchain-related characteristics of the morphological box

Characteristics	Values			
Blockchain design elements	Charging and rewarding	*Consensus*	*Identity management*	Tokenization
	Codebase	*Extensibility*	*Security/Privacy*	*Transaction capabilities*
Blockchain type	*Consortium*	Private permissioned	Public permissioned	Public permissionless

namely the network structure principle that focuses on different participation modes; this principle is used to classify a distributed ledger based on its centralization degree and participation mode. The network principle differentiates between three degrees: *centralized*, *decentralized*, or *distributed*, and two participation modes: *permissioned*, or *permissionless* [27].

Blockchain as a concept aims to achieve a decentralized consensus on valid ledger entries among untrusted participants. The blockchain concepts are compelling and can be differentiated in two classes of blockchain types that are either "*open* or *closed*", as visualized in Table 3 where example configurations are outlined that are currently used in several applications of the concept of blockchain. When it comes to our unit of analysis, Sawtooth, it is considered an enterprise blockchain platform and allows inherently to deploy different blockchain types, but for this project the base is *consortium.*

According to Burkhardt et al. [20], a blockchain is composed of six building blocks (1) transactions, (2) roles, (3) blocks, (4) verification and validation processes, (5) algorithms, and (6) cryptography. In general, transactions (1) are transparent and visible to each participant, depending on the two complementary blockchain types (Table 3). Participants in a blockchain-based network have an identical copy of the current ledger [20], depending on the permission settings and the blockchain design.

Blockchain participants have roles (2) with associated tasks to interact with each other and find consensus. These roles work together and build a network that provides an unalterable history of data exchange in form of transactions between the participants, whereas all transactions are stored in blocks. Roles, for example, are "smart contracts", "endorsers", "committers", "validators", and "orderers" [29]. Blocks (3) are cryptographically concatenated and always chained to the previous block. All

Table 3 Competing blockchain types [28]

			Read	Write	Commit	Examples
Blockchain type	Open	Public permissionless	Open to everyone	Everyone	Everyone	Ethereum, Ethereum classic
		Public permissioned	Open to everyone	Authorised participants	All or subset of authorized participants	Sovrin
	closed	Consortium	Restricted to an authorised set of participants	Authorised participants	All or subset of authorized participants	Multiple banks operating a shared ledger
		Private permissioned	Fully private or restricted to a limited authorised set of participants	Network operator only	Network operator only	Internal bank ledger shared between parent companies

blocks together form the blockchain (ledger) and depict a single point of truth to all nodes that have access to it. In this context, a node can be either a full node or a light node that participants use to access the network. A full node downloads and stores the whole blockchain and is designed to verify and validate (4) transactions back to the very first block ("genesis block"), whereas light nodes only download the block header of the previous block. Light nodes rely on full nodes for operations requiring the complete blockchain, thus, the data storage is less consuming/expensive for the participant of light nodes [29]. Blockchain participants have an identical copy of the current ledger [20], depending on permission settings and technical design,. The participants agree on the current ledger state by relying on a (consensus) algorithm (5), and today many different algorithms exist [30]. The encryption (6) as the last building block additionally increases the difficulty for attempts that want to alter the ledger state history and thus assures a high degree of immutability [31].

3.1.2 Core Design Elements

Tasca and Tessone [32] developed a taxonomy for blockchain which can be used as a blockchain reference standard. The reference standard covers, among other things, the smallest required technical elements that are part of a blockchain configuration; they allow to differentiate the configurations at a technical level, which reflects the different purposes they target. The taxonomy provides a clear structure to categorize the relationships of the inherent blocks and is a sufficient tool, when applied rigorously, to compare different, heterogeneous configurations [21].

The taxonomy encompasses the identification, description, nomenclature, and hierarchical classification of blockchain components. In addition, it groups them in a hierarchical structure that highlights functional relations and design patterns. The taxonomy focuses on generic blockchain design choices and consists of eight core design elements:

(1) *Consensus*: The consensus describes the validation and verification process that leads to mutual trust among participants in a blockchain network. The consensus directly affects the reliability, authenticity, and accuracy of the stored data within the blockchain [30]. The consensus algorithms are different regarding immutability and failure tolerance, latency, and finality and relate "to the set of rules and mechanics that allows for the maintenance and updating of the ledger and guarantees the trustworthiness of the records in it." [32].
(2) *Transaction Capabilities*: Transaction capabilities determine transaction scalability and transaction usability. In this context, a transaction initiates a ledger state change. Transaction scalability relates to quantitative measures such as transactions per second (TPS) that allow a performance comparison between a blockchain and other solutions (e.g., MasterCard Payment Gateway) that serve similar functionality, while transaction usability relates to the degree, to which the transactions are suitable to be used in IESs [32].

(3) Native Currency/Tokenization: The 'digital economy' (value in Table 1) includes the so-called *cryptonomics* empowered through tokens. The Swiss Financial Market Supervisory Authority (FINMA) classifies tokens as blockchain-based units that can be categorized as either (1) payment tokens, (2) utility tokens, or (3) asset tokens. The first, payment tokens, are native currencies such as Bitcoin—they have no other functions aside from the currency. The second, utility tokens, provide digital access to services or applications; the third, asset tokens, represent ownership of an underlying asset, which can be both physical or digital [33].
(4) Extensibility: Extensibility is the degree to which a blockchain network can be extended to interact with elements outside the network. Extensibility stands for interoperability, intraoperability, governance, and scripting language components as part of a blockchain. As an example, the governance can be performed through an open-source community (e.g. Hyperledger), through a technical solution provider (e.g. Microsoft), or through an alliance (e.g. R3) [32].
(5) Security and Privacy: Security and privacy design differentiate between data encryption and data privacy settings. Data encryption stands for the encryption algorithms that are used in a blockchain to ensure (1) integrity, (2) authenticity and (3) the correct order of events. (1) and (2) can be aligned with two of the attributes from the CIA triad—*integrity* and *confidentiality* [32]. Data privacy can either be an integral part of the blockchain network ('by design') or an add-on relying on external solutions [32].
(6) Codebase: The coding language, code licensing, and software architecture define the codebase. The latter can be described as a collection of source code used to build a system, application, or one of its components. A blockchain supports either single or multiple languages, open-source or closed-source license and either a monolithic or a polythic software architecture design [32].
(7) Identity Management: The blockchain identity management builds on three layers: (1) identity, (2) access, and (3) control. (1) and (2) can be aligned with the attributes *confidentiality* and *integrity* from the CIA triad [32]. The access and control layer refers to the blockchain type (Table 3) [32].
(8) Charging and Rewarding System: A blockchain depends on computing power using hardware and electricity. A cost model that organizes resources and rewards contributors is essential for a blockchain to ensure the ongoing service and the *availability*—the third CIA triad attribute [32]. The incentives that root in the charging and reward system do not apply to all blockchain architectures, because such modalities could also be defined outside the blockchain system. A simple solution would be a consortium with participating members that contribute to the same amount of resources (e.g. a full node).

The eight core design characteristics and their outlined specifics are an excellent theory-based foundation to map and compare complementary blockchain configurations. However, the taxonomy does not provide guidance for comparison and, finally, the selection of a specific blockchain configuration based on dedicated requirements, such as data privacy to comply with a specific law such as GDPR. Consequently,

Table 4 Data privacy-related characteristics of the morphological box

Characteristic	Values		
Data operation	Store	Transfer	Use
Permissions, policies and roles	Least privilege	Logical access	Segregation of duties
Encryption	Data encryption		
Security mechanism	Monitoring and logging	Third-party controls	Transparent changes

we claim that it is necessary to add guiding factors that explicitly target the privacy design attributes. This will lead to a more detailed taxonomy and a prioritization scheme.

3.2 Data Privacy Characteristics

Four technically relevant audit characteristics, "Data Operation", "Permissions, Policies, Roles", "Encryption" and "Security Mechanism" will be incorporated to enrich our morphological box. Similar to the previous section, these characteristics draw on existing contributions and will be explained in more detail in the following paragraphs. Table 4 summarizes the data privacy-related characteristics.

As a specific contribution to closing the derived research gap, we united the data privacy-related characteristics of the morphological box into a novel assessment matrix—we call it 'morphological grid' (Fig. 2). Instead of highlighting values in Table 4, this time the newly developed morphological grid will be applied to our Sawtooth analyses unit. The parameters are based on audit guidelines.

Safeguarding Controls		Data Operations		
		Use	Transfer	Store
Permissioning, Policies, Roles		1	2	3
Logical Access Controls	a	+	+	++
Least Privilege	b	+	++	++
Segregation of Duties	c	+	++	++
Encryption				
Data Encryption	d	+	++	++
Overall Security Mechanism				
Transparent Changes	e	+	++	+
Third-party Controls	f	+	-	-
Monitoring & Logging	g	++	++	++

++ default
+ on demand
- missing

Fig. 2 Morphological grid for assessing blockchain-privacy applied to Sawtooth

An audit is a sufficient procedure to review relevant activities in an organization that affects the IES and thus data privacy [34]. The IES and the related information life cycle ranges from data creation/collection to deletion and can be assessed regarding its data privacy maturity [35]. To conduct a data privacy audit, an audit framework/standard should be used that enables organizations to assess their IES in a structured and recommended way. The results should reflect an organization´s ability to comply with given privacy requirements. Some leading audit-related institutions work on common privacy assessment standards that include specific guidelines to audit IESs [34]. For example, the International Standard Organization (ISO) provides the "ISO 29100:2011 Information technology—Security techniques—Privacy framework" [36], which includes essential elements of a data privacy audit [37]. To apply ISO 29100:2011 for the assessment of blockchain-based IESs, the standard needs to be adopted since it covers business logics, e.g., legal requirements related to the business case and not to the enabling IES, and because it handles data operations that are usually not part of blockchain configurations but of 'classical' (relational) databases. The ISO 29100:2011 provides privacy safeguarding controls, which are techniques or practices that can be aligned with data operations within IESs. The related controls are broadly categorized into (1) permissioning, (2) policies and roles, (3) encryption, and (4) overall security mechanism, and are adopted from an exemplary data privacy controls audit [38].

In order to judge the privacy capabilities of a blockchain configuration, the relevant data privacy characteristics must first be established. When technical data privacy attributes are defined, a blockchain configuration's privacy capabilities can be assessed by analyzing which defined privacy attributes it fulfills. The configuration has these attributes that are built in either by default or as needed, or they do not existent and cannot be implemented with this configuration.

For our study, we build on two existing works: Firstly, the data operations [39] from ISO 29100:2011 and secondly, detailed privacy safeguarding controls for a privacy control audit based on [38]. Other ISO 29100:2011 privacy framework elements were not considered because they are directly relevant for technical features and therefore ignored.

The developed morphological grid to assess blockchain configurations is shown in Fig. 2, with its three data operation-related columns "Use", "Transfer", and "Store"; these three operations match the blockchain data operations, where a state is stored ("store"), its status is transferred ("transfer") or accessed ("use"). In the columns, the attributes "Permissioning, Policies, Roles" refer to the more detailed safeguarding controls that are not described in the ISO framework. The controls are (a) "Logical Access Controls" for each data operation step (b) "Least Privilege" for the principles in place, meaning system components (user, processor, program), which must be able to access only the information and resources that are necessary for its legitimate purpose of either using, transferring, or storing data. Next, (c) "Segregation of Duties" forces the concept of having more than one person or system component to process the task of either using, transferring or storing the data. The second attribute part assesses the (d) "Data Encryption". The last attribute group looks at the "Overall Security Mechanism" with the perspective on (e) "Transparent Changes" that affect

data operations. The attribute (f) "Third-party Controls" refers to controls that allow software from outside a blockchain network to control internal changes. In this context, a blockchain network is a closed system with only limited interaction with the outside world. Therefore, there are no possible specific third party controls over key roles (validators, processors, peers). The only interface that theoretically allows third-party controls is the client itself. The last security mechanism that is part of the morphological grid relates to (g) "Monitoring & Logging" procedures, also applied to the three data operations.

Figure 2, the morphological grid, is—in addition to the characteristics of the morphological box (Fig. 1) our main research contribution, the artifact with its relevant data operations on the x-axis, and seven outlined privacy safeguarding controls on the y-axis. The safeguarding controls correlate with *confidentiality*, one of the three attributes from the CIA triad [18]. Although a blockchain configuration often provides other attributes from the CIA triad (e.g. consensus) or availability (e.g. transaction capabilities), confidentiality is most relevant from a privacy perspective and therefore should be emphasized with a specific focus. The term *confidentiality* stands for a set of rules that limits access to information or according to the ISACA glossary is vital for "preserving authorized restrictions on access and disclosure, including means of protecting privacy and proprietary information" [40]. In the blockchain context, confidentiality is dedicated to authorized restrictions which relate to participants, their identities, permissions, and roles; access and disclosure of information relate to transactions that contain payloads (information), their flow through the system and their encryption.

The following three mutations are the base for setting the horizontal and vertical morphological grid axes. They describe the changes made to the original ISO 29100:2011 framework:

(1) Environmental factors including privacy principles, legal requirements, and the business case defining involved personal identifiable information (PII) are not part of the morphological grid and were removed. They belong to the business logic and define the steps that must be undertaken before deciding to use a blockchain configuration. The "collect" data operation depends on the business logic that specifies what data needs to be collected and how this task can therefore be performed by applications other than a blockchain. The data operation "destroy" is, by default, not foreseen to be implemented on a blockchain. In contrast to a blockchain configuration, "destroy" or "delete" is a standard operation for a regular database.
(2) "Privacy Safeguarding Controls" were specified by listing control elements that are part of privacy audits for IT system controls [38].
(3) Each grid indicates whether the configuration has the privacy capability integrated by default, on-demand, or whether it is missing and cannot be implemented on the configuration in question.

4 Conclusion and Outlook

The goal of this study was to develop a tool that helps organizations make decisions for a blockchain configuration that matches their use case. The developed morphological box and the grid allow to identify Sawtooth's technical capabilities that secure data and support data privacy at different levels. In order to apply the morphological box and the assessment grid, thorough knowledge about the assessed blockchain configuration is required, in terms of the architecture and the different component roles and not least how they work together. For this reason, our theoretical approach is perfect for open-source configurations. It does, however—and this is one limitation of our research—potentially not work for closed-source configurations because of their lack of transparency. Another limitation is that the morphological box and the related grid do not distinguish between diverse encryption methods, and therefore inherently assume that any encryption method relies on a proper encryption algorithm. Nevertheless, the research output can be used (on a high/medium level) to evaluate each blockchain configuration, in particular with regard to its data privacy capabilities.

Future research opportunities could be firstly a more detailed breakdown of the outlined privacy safeguarding controls based on different or complementary security frameworks. Secondly, a thorough guide could be developed for different target groups (more or less experienced with blockchain and data privacy) that explains the application of the developed artifact and related assumptions. Finally, the developed artifact could be enhanced with information on other blockchain configurations (e.g., Stellar, Quorum). Sawtooth is a modular platform that comes—by default—with robust security functionalities and offers various customizing options. The validation on Sawtooth worked well because Sawtooth is designed to be secure and appropriate for enterprise applications that naturally have various data privacy requirements. However, it remains unclear to what extent the artifact is able to reflect the actual data privacy capability of a blockchain configuration because many factors from regular privacy audits are not considered in this study (e.g., hardware controls). Further research on data privacy and blockchain configurations will hopefully path the way for organizations to adopt the technology at a faster rate, and eventually develop feasible applications that protect personal data in a better and auditable way.

References

1. Gur, A.O., Oksuzer, S., Karaarslan, E.: Blockchain based metering and billing system proposal with privacy protection for the electric network, pp. 204–208 (2019)
2. Jiang, Y., Wang, C., Wang, Y., Gao, L.: A privacy-preserving e-commerce system based on the blockchain technology. In: IWBOSE 2019—2019 IEEE 2nd International Workshop Blockchain Oriented Software Engineering, pp. 50–55 (2019). https://doi.org/10.1109/IWBOSE.2019.8666470
3. Marsalek, A., Kollmann, C., Zefferer, T., Teufl, P.: Unleashing the full potential of blockchain technology for security-sensitive business applications. In: 2019 IEEE International Conference

Blockchain Cryptocurrency, pp. 394–402 (2019). https://doi.org/10.1109/bloc.2019.8751444
4. Chang, H.: Blockchain: disrupting data protection? Priv. Laws Bus. Int. Rep. (2017)
5. Hevner, A.R., Chatterjee, S.: Design science research in information systems (2010)
6. Ritchey, T.: Adapted from "Fritz Zwicky, morphologie and policy analysis. In: General Morphological Analysis A general method for Non-quantified Modelling, pp. 2002–2013 (2013)
7. Bakis, Bruce J., J.S.M.: How to conduct a privacy audit. http://www.mitre.org/sites/default/files/pdf/HowToConductPrivacyAudit.pdf
8. Snedaker, S., Russ, R.: IT Security Project Management Handbook. In: Syngress IT Security Project Management, pp. 196–197, Canada (2006)
9. EUFRA: The EU's independent data protection authority. In: Handbook on European Data Protection Law, pp. 1–402. Publications Office of the European Union, Luxembourg (2018)
10. Tankard, C.: What the GDPR means for businesses. Netw. Secur. **2016**, 5–8 (2016). https://doi.org/10.1016/S1353-4858(16)30056-3
11. Federal Statistical Office: Erhebung zur Internetnutzung 2017. Digitale Kompetenzen, Schutz der Privatsphäre und Online-Bildung: die Schweiz im internationalen Vergleich. https://tinyurl.com/bfs-study-2017
12. eurostat: Digital economy and society statistics—households and individuals. https://tinyurl.com/eurostat-survey
13. BBC: Facebook fined GPB 500,000 for Cambridge Analytica scandal (2018). https://www.bbc.com/news/technology-45976300
14. European Union: Regulation (EU) 2016/679 (General Data Protection Regulation—GDPR). Off. J. Eur. Union. EN 1–88 (2016)
15. Habbabeh, A., Schneider, B., Asprion, P.M.: GDPR assessment instrument an exemplary case for higher education institutions. Int. J. Manag. Knowledge, Learn. 311 (2019)
16. Data Protection Working Party: Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP29). Artic. 29 Data Prot. Work. Party. WP 248 rev 22 (2017). https://doi.org/10.2139/ssrn.2972855
17. Information Commissioner's Office: Guide to the general data protection regulation (GDPR). https://tinyurl.com/GDPR-UK
18. Perrin, C.: The CIA triad (2008). https://www.techrepublic.com/blog/it-security/the-cia-triad/
19. Nakamoto, S.: Bitcoin (2008). https://bitcoin.org/bitcoin.pdf
20. Burkhardt, D., Werling, M., Lasi, H.: Distributed ledger. In: 2018 IEEE International Conference on Engineering, Technology and Innovation. ICE/ITMC 2018—Proceedings, pp. 1–9 (2018). https://doi.org/10.1109/ICE.2018.8436299
21. Shapley, L.S.: A value for n-person games. In: Contributions to the Theory of Games II, Annals of Mathematics Studies. Princeton University Press (1953)
22. Kuhn, H.W.: Lecturers on the Theory of Games—Annals of Mathematics Studies. Princeton University Press, Princeton and Oxford (2003)
23. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: SoK: research perspectives and challenges for bitcoin and cryptocurrencies. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 104–121 (2015). https://doi.org/10.1109/SP.2015.14
24. Margolis, E., Laurence, S.: The ontology of concepts—abstract objects or mental representations? Nous. **41**, 561–593 (2007)
25. Hobson, D.: What is bitcoin? XRDS crossroads. ACM Mag. Stud. **20**, 40 (2013). https://doi.org/10.1145/2510124
26. Hyperledger: Hyperledger Sawtooth project page (2019). https://www.hyperledger.org/projects/sawtooth
27. Sawnson, T.: Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems (2015). http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf
28. Tasca, P.: Swiss Blockchain Research Symposium (2019)

29. Palai, A., Vora, M., Shah, A.: Empowering light nodes in blockchains with block summarization. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security NTMS 2018—Proceedings, pp. 1–5 (2018). https://doi.org/10.1109/NTMS.2018.8328735
30. Alsunaidi, S.J., Alhaidari, F.A.: A survey of consensus algorithms for blockchain technology. In: 2019 International Conference on Computer and Information Sciences, ICCIS 2019, pp. 1–6 (2019). https://doi.org/10.1109/ICCISci.2019.8716424
31. Hyperledger: Hyperledger Sawtooth documentation. https://sawtooth.hyperledger.org/docs
32. Tasca, P., Tessone, C.J.: A taxonomy of blockchain technologies: principles of identification and classification. Ledger **4**, 1–39 (2019). https://doi.org/10.5195/ledger.2019.140
33. FINMA: ICO Guidelines, pp. 1–11 (2018). https://doi.org/10.1515/9783598440397.13
34. Cooke, I.: IS audit basics: auditing data privacy. ISACA J. **3** (2018)
35. Riffat, M.: Privacy audit—methodology and related considerations. ISACA J. **1** (2014)
36. International Organization for Standardization: ISO/IEC 29100:2011. https://www.iso.org/standard/45123.html
37. Lachapelle, E., Ajvazi, B., Rama, F.: ISO 29100 how can organizations secure its privacy network? https://tinyurl.com/y2l4on83
38. Photopoulos, C.: Managing Catastrophic Loss of Sensitive Data. Syngress (2011)
39. Andress, J.: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress (2011)
40. ISACA: Glossary (2019). https://tinyurl.com/ISACAGlossary