What Do We Really Need? A Systematic Literature Review of the Requirements for Blockchain-based E-government Services

Julia Amend
Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Bayreuth, Bayreuth

Julian Kaiser
Universität Bayreuth

Lucas Uhlig
Universität Bayreuth

Nils Urbach
FIM Research Center, Frankfurt University of Applied Sciences, Frankfurt, Germany, Project Group Business & Information Systems Engineering of the Fraunhofer FIT

Fabiane Völter
Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Bayreuth, Bayreuth

What Do We Really Need?
A Systematic Literature Review of the Requirements for Blockchain-based E-government Services

Julia Amend[1], Julian Kaiser[2], Lucas Uhlig[2], Nils Urbach[3] and Fabiane Völter[1]

[1] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Bayreuth, Bayreuth
{julia.amend, fabiane.völter}@fit.fraunhofer.de
[2] University of Bayreuth, Bayreuth, Germany
{julian.kaiser, lucas.uhlig}@uni-bayreuth.de
[3] FIM Research Center, Frankfurt University of Applied Sciences, Frankfurt, Germany, Project Group Business & Information Systems Engineering of the Fraunhofer FIT
nils.urbach@fim-rc.de

Abstract. Information Systems research acknowledges the importance of identifying requirements to ensure the artifact's relevance. However, many research articles addressing blockchain technology for e-government capture the requirements that need to be fulfilled only implicitly by defining system objectives or evaluation criteria. Furthermore, focusing on specific use-cases encompasses the risk of overlooking those requirements, which are not as obvious but equally important. This procedure causes uncertainty regarding the requirements a blockchain-based e-government service needs to fulfill. Therefore, we conducted a systematic literature review on blockchain-based government-to-citizen (G2C) e-government services. On this basis, we categorized the requirements as we find that they address either the data of the system, the user, or the system itself. Our categorization provides a structured overview supporting researchers in conducting research on blockchain technology in the public sector and giving practitioners input to develop, test, and evaluate new blockchain-based G2C e-government services.

Keywords: e-government, blockchain, requirements, literature review, public service

1   Introduction

E-government describes the use of information technologies to improve access to governmental information and services to citizens, businesses, or other governmental agencies [1, 2]. By using (digital) technology to make interactions more convenient, e-government aims to improve the relationship between governmental agencies and the public [1, 3]. The relation may be between a government and its citizens (Government-to-Citizen, G2C), other public institutions (Government-to-Government, G2G), or

businesses (Government-to-Business, G2B) [4]. Despite recent advancements in the field of e-government, Norris [4] emphasizes the unsatisfying development of activities in this domain as "e-government has not produced either e-democracy or e-governance, nor is it likely to do so any time in the foreseeable future" (p. 339). However, the advent of new emergent technology may help fulfill this aim, as governments and public sector bodies are increasingly assessing their potential for delivering services [5]. As such, researchers and practitioners consider blockchain technology to enhance the efficiency of government operations by increasing trust in public sector bodies and improving the delivery of public services [6]. They attribute this potential to the technology's characteristics. Blockchain enables peer-to-peer transactions without an advocate in a tamperproof, transparent, and trustless manner.

Researchers and practitioners developed multiple use cases for blockchain technology in e-government, most of those focusing on G2C applications. For example, blockchain technology may facilitate electronically held election processes, in short called e-voting [7], or taxation services [8], and may serve as an underlying technology for creating digital identities [9]. Most research articles propose applying blockchain technology to specific contexts [10]. Thus, they capture requirements for the solution in a very use case-specific context while some articles capture requirements even only implicitly. Accordingly, blockchain-based G2C e-government services are still immature and mostly lack empirical evidence as well as requirements-driven solution approaches [10]. This observation may also be caused by terminological ambiguities and conceptual fuzziness when it comes to blockchain technology [11]. As a result, it remains unclear which requirements blockchain-based G2C e-government services have to fulfill independent from a specific use case. However, the process of defining requirements is specifically important as it records the specifications of the system's stakeholders. Also, practitioners do not only need to understand the application domain, but also the constraints, functionalities, and essential system characteristics [12]. As a result, capturing the requirements ensures that the proposed solution meets the goals and expectations of potential users [12]. Batubara et al. [11] also stress "the need for a proper design solution at the architecture level in accordance with the specific requirements from e-government processes" (p.7). For this reason, our research aims to answer the following research question:

Which requirements do blockchain-based G2C e-government services need to fulfill?

To answer the research question, we conducted a literature review on blockchain-based G2C e-government services. This approach allowed us to provide a structured overview of the use case-independent requirements which a blockchain-based G2C service needs to fulfill. Furthermore, we grouped these requirements around the three core categories "data", "user", and "system", which provides further structure for researchers and practitioners during the development and evaluation of new blockchain-based solutions. Answering this research question does not only imply supporting the design and evaluation of artifacts. We also contribute to the academic discourse by supporting rigorous design science research in the blockchain domain.

The remainder of this paper is structured as follows: Section 2 introduces e-government services and blockchain technology. Section 3 describes the methodology applied. In Section 4, we present the results of our literature review and provide an overview of the resulting requirements. Finally, we reflect on our findings concerning the requirements of blockchain-based G2C e-government services in Section 5 as well as on limitations and future research opportunities in Section 6.

2 E-government & Blockchain Technology

A central motivation for providing e-government services is to increase accountability, enhance transparency, and increase stakeholder participation [13, 14]. The latter depends on achieving higher efficiency, quality, and effectiveness in the management of public state institutions [15, 16]. E-government initiatives not only provide faster services to citizens while being more cost-effective [17], but also reduce the administrative burden and other bureaucratic hurdles for government employees [18]. Furthermore, initiatives have tried to provide public services in a more direct way, tailored to the needs of citizens [19]. However, better cooperation with partners of all kinds will be required [20] to exploit the potential of e-government services fully. In summary, Moon [2] characterizes the provision of e-government services with four aspects: First, service delivery is based on the web, and second, e-commerce is suitable for conducting transactions. Third, digitalization may reinforce democratic structures, as it enhances the transparent accountability of governments. Lastly, fourth, a secure government intranet and central database increase the efficiency and cooperation between different governmental agencies. However, observing the characteristics of blockchain technology, the latter aspect may be challenged, as blockchain allows inter-organizational collaboration in a decentralized manner [5].

In contrast to a centralized database, blockchain technology is a distributed data structure used to store transactions in a tamper-resistant, decentral, and transparent manner in a peer-to-peer network [21]. The transactions are recorded in chronologically ordered blocks, which are linked using cryptographic hashes, ensuring high tamper-proofness of information and thereby creating a chain of blocks. Accordingly, by design, blockchain encompasses specific characteristics. Among those are *transparency* [5, 22–24], *integrity* [5, 22, 24], *redundancy* [23, 24], *immutability* [5, 22] and *privacy* [24, 25]. The consolidated definitions for each of these characteristics can be observed in Table 1. However, no consensus exists regarding the distinction between the characteristics encompassed by design and further properties of the technology, which can be derived from the latter. For example, while some authors mention auditability as a fundamental characteristic [24], one may also argue that auditability is caused by the underlying characteristics *transparency* and *immutability*. Similarly, Wüst and Gervais [24] state that "*transparency* [..] is a requirement for verifiability" (p. 46), while some authors categorize verifiability as a fundamental characteristic of the technology [23]. Due to those reasons, we identified the characteristics of *transparency*, *integrity*, *redundancy*, *immutability,* and *privacy* as the fundamental characteristics of blockchain technology. Since the invention of blockchain technology

in 2008, researchers and practitioners have addressed a considerably high amount of attention to the exploration of the technology. As a result, use cases and application domains of the technology have expanded immensely. Therefore, blockchain-based solutions have gained visibility in the context of supply chains, healthcare, the Internet of Things, data management, and governmental services [26, 27]. Also, public institutions increasingly acknowledge the enormous potential of blockchain technology for governmental services as they address current challenges by strategically identifying promising use cases of the technology [27]. Thereby, use cases are not only evaluated on a conceptual level but also in pilot projects [28]. For example, an advanced use case for digital identities exists in Estonia using the e-Identity ID card on a blockchain [9].

The potential attributed to the technology in the area of e-government is based primarily on its ability to provide an incorruptible system, to make processes more transparent, and to eliminate the need to entrust in specific institutions or individuals [30]. Furthermore, blockchain technology enables inter-organizational cooperation on a neutral platform [5]. For those reasons, various use cases have been proposed and discussed in the academic literature. Among the most popular G2C use cases are blockchain-based electronic voting processes and the creation of digital identities using blockchain technology as the underlying infrastructure. Furthermore, researchers propose blockchain-based handling of taxes to prevent tax fraud and enhance tax payments transparency [8, 31]. Researchers also attribute the potential to blockchain-based land and property management. Accordingly, the transparent and accountable recording of land titles on a blockchain is more reliable and trustworthy than a paper-based process, especially in developing countries [32, 33]. Also, blockchain-based smart city solutions are addressed. Other G2C use cases include the tracking of funds to prevent misusage due to corruption [34]. Concerning the detection and combat of such misbehavior, blockchain technology may create significant value [32, 35]. Besides, blockchain technology can be very beneficial in sharing data for e-government applications, especially for the citizens' privacy and data reliability [36, 37]. Depending on those use cases, blockchain applications' design and governance may differ. Practitioners may choose between a public and private [38] as well as permissionless and permissioned [5] infrastructure. For the public sector, Shahaab [39] identified "private" and "permissioned" configurations as widely-spread design patterns.

3 Method

We conducted a systematic literature review following Kitchenham and Charters [40] to identify the requirements for blockchain-based G2C e-government services. As literature sources, we chose databases complementary to the ones that Batubara et al. [10] selected to extend existing literature reviews. As a result, we included the databases WebofScience, Business Source Premier, ACM Digital Library, and IEEE Explore Digital Library also to consider the academic discourse in the Computer Science domain. We derived our search string from the main keywords of our research question and complemented them with synonyms and similar terms: ("blockchain" OR

"block chain" OR "distributed ledger") AND ("e-government" OR "government" OR "public service" OR "public sector"). We set the search period to the beginning of 2008 since blockchain was firstly proposed in that year [41]. We searched all databases until the 7th of August, 2020, which revealed 1,051 articles in total.

In the next step, we included all articles that met our inclusion criteria (IC). Regarding the publication type, we only included peer-reviewed research articles and conference proceeding papers. Furthermore, only articles published in the English language were considered. After we applied the said inclusion criteria, our article set included 853 articles in total.

For selecting relevant studies, we also defined exclusion criteria (EC) based on our research question. First, we excluded duplicate articles (EC1). Second, we omitted articles from our study that were incomplete, e.g., that had no conclusion (EC2). Third, also the research domain served as an exclusion criterion (EC3). Articles that neither addressed e-government nor blockchain technology were excluded. Furthermore, this criterion also addressed that the paper's use case needs to address the relation of G2C. Applying the exclusion criteria, we reduced the total amount of 853 to 160 articles for full-text reading. In the next step, we reviewed these articles against defined quality criteria to ensure that the study results were relevant for our research. We discarded articles that mainly describe technical details of a construct, do not address the public sector, or only provide a general overview of e-government applications instead of addressing a specific use case. Besides, we excluded articles addressing only the regulatory aspects of e-government. After this quality assessment, the article set ultimately contains 89 articles. Figure 1 depicts the data collection process.
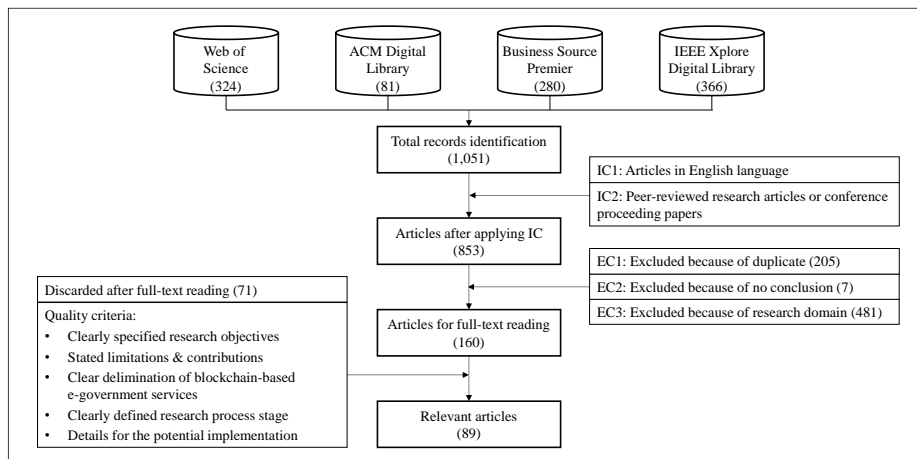

Figure 1. Data collection process

During the data extraction phase, we extracted the following data: use case, research question or objectives, evidence, validity of the study, research challenges, and limitations. In the subsequent data synthesis phase, we analyzed the results of the selected studies considering the publication year and type, use case, research process

stage, and the requirements imposed on a blockchain-based e-government solution. For the classification of the research process stage, we used the categorization of system development research proposed by Nunamaker [42]. Those stages are: (1) conceptualization, (2) system architecture, (3) system design, (4) prototype, and (5) evaluation. Following the data extraction phase, we consolidated the identified requirements by analyzing the definitions of the requirements. Thereby, we found that they are addressing either the data, the system itself, or the user. For this reason, we chose to classify the requirements in the three categories "user", "data", "system". Furthermore, we consolidated overlapping requirements, which addressed the same aspect but used synonyms.

4 Results

4.1 Descriptive Findings of Selected Articles

The number of publications and the variety of use cases show that the academic literature on blockchain-based G2C e-government services develops rapidly. Our article set contained 89 scientific articles that have analyzed or taken up blockchain-based G2C e-government services after we applied our defined inclusion and exclusion criteria. Of these, 75 articles are published in conference proceedings, and 14 articles appeared in scientific journals. A total of 80 articles have been published within the last 2,5 years, which indicates a growing research interest. Furthermore, the research stage has progressed since Batubara et al.'s [10] literature review as the number of publications focusing on evaluating solutions has increased. In particular, the research stages are distributed according to Nunamaker et al. [42] as follows: (1) conceptualization (20 articles), (2) system architecture (19 articles), (3) system design (12 articles), (4) prototype (9 articles), and (5) evaluation (29 articles). The range of discussed use cases is broad. While Batubara et al. [10] found a predominant focus on healthcare, education, and smart cities, we found immense attention on **e-voting** (51 out of 89). Also, articles propose blockchain technology for supporting **land & property management** (12 out of 89) and **smart city** (7 out of 89) solutions. Besides, researchers discuss using blockchain technology as the underlying technology for creating **digital identities** (7 out of 89). However, this use case may address varying aspects [9, 43]. It ranges from government-issued digital identities [9] to using blockchain as a foundation for self-sovereign identities [44]. The idea of using blockchain technology in the domain of **education** (6 out of 89) also becomes more popular. Moreover, researchers discussed blockchain-solutions for **fund tracking** (2 out of 89) and **taxation** (4 out of 89). Most researchers observe the latter use case from the government's perspective [8, 30] rather than from the citizen's perspective.

4.2 Requirements of Blockchain-based G2C E-government Services

As we identified that the extracted requirements address either the user interacting with the blockchain-based solution, the data to be recorded, or the system itself, we used the

three categories "data", "user", and "system" to categorize the identified requirements. Additionally, we consolidated requirements addressing the same aspect but using synonymous terminology. For example, some authors used the term *privacy* [43] while others used anonymity [45] or secrecy [46]. Similarly, authors used the term usability [47] as a synonym for *ease of use* [8], accuracy [48], and correctness [49] for *integrity* [50], credibility [51] and trustworthiness [52] for *reliability* [53]. Also, the definitions of *auditability* [50] with traceability [54] coincide as well as of *instant information* [48] with real-time information [55]. Another overlap exists for *affordability* [56] with low-cost [57] and cost-efficiency [58]. Lastly, *accessibility* [47] represents the same aspect as availability [57].

We found interesting gaps in requirements for some use cases, e.g., all use cases require system-related *interoperability*, except for e-voting applications. In our opinion, this finding is not due to the fact that *interoperability* is not an essential requirement for e-voting applications, as all created services need to be integrated into the existing process and system landscapes. Also, only articles addressing the taxation use cases mention *reversibility*. However, we claim that it is equally important for other use cases, such as land & property management, to correct or delete false transactions. This finding highlights the importance of an integrative observation beyond each use case. Observing a use case in isolation would entail that important but less obvious requirements are potentially missed. Another notable finding impacts the requirement data-related *redundancy*. From our perspective, this requirement should not only focus on "data", as *redundancy* is crucial to reduce the impact of system downtime. Nevertheless, the authors addressed only data-related *redundancy*. However, to create secure and reliable systems, researchers should also assess redundancy from a systems perspective. Table 1 provides an overview of these requirements with their different terminologies, their definitions, and their frequency.

Table 1. List of requirements and their definitions

	Requirement (synonyms)	Definition	Freq.
User	Privacy (anonymity, secrecy, confidentiality)	The data may not be associated with a user.	61
	Verifiability	Anyone may verify the correctness regarding the system state, including its transactions and results.	56
	Trust	The user must trust in the system itself.	59
	Authenticity (identifiability)	Users are who they claim to be.	74
	Integrity (eligibility)	Users fulfill specific prerequisites to use the system.	43

	Ease of use *(user-friendly, usability)*	The system is convenient to use, and users can easily add transactions.	30
Data	Transparency	Process information and data are generally visible for users, but in case of necessity, this visibility can also be limited.	75
	Integrity *(accuracy, correctness)*	The data may not be altered, such that the resulting evaluation of the data (e.g., election result) is accurate.	68
	Reliability *(credibility, trustworthiness)*	The credibility of the data and transactions can be trusted.	53
	Immutability	No data is lost or deleted.	43
	Auditability *(traceability)*	The transaction history may be shared in a traceable and reliable manner.	43
	Confidentiality	The contents of transactions are hidden or unreadable.	27
	Instant Information	Data is exchanged instantly.	21
	No double spending	Every transaction is executed only once.	25
	Reversibility	Conflicting edits or errors can be managed by counter-transactions.	1
	Redundancy	Data is kept redundantly.	3
System	Security	The system is resistant to errors and attacks.	86
	Scalability	The system can handle a growing number of transactions.	30
	Affordability *(low cost, cost-efficient, financial viability)*	The implementation and maintenance of the system should be affordable and, in the best case, also be less expensive than analog alternatives.	37
	Accessibility *(availability)*	Users can remotely access the system to participate regardless of their physical location at any time.	34
	Robustness	The system is not only resistant to attacks but is also scalable and resource-efficient.	32
	Interoperability	The system is integrable with existing systems and processes.	12

Ease of maintenance	Services are separated to guarantee efficient maintenance.	7

Based on the analysis of various definitions, we are able to form a categorization of all requirements and their inter-relation with general blockchain characteristics, which we described in Section 2. Accordingly, analyzing the definitions of the found requirements allowed us to categorize the identified requirements either as a characteristic embedded in blockchain technology or as further feature. However, this differentiation between "characteristics" and "features" is not unambiguous in all cases. For example, researchers on blockchain technology often refer to user-related *trust* as one of the underlying characteristics of blockchain technology [25]. However, we follow the argumentation of Ostern [59] and Marella [60] that users' trust is not inherent to blockchain technology itself. Instead, other underlying characteristics and requirements like integrity and immutability of the data stimulate *trust*. For this reason, we categorize *trust* as a user-related feature rather than as a blockchain characteristic.

Similarly, some authors refer to the data-related *auditability* requirement as an underlying characteristic [5]. However, *auditability* is defined as the ability to examine records. Accordingly, we argue that data-related *transparency, redundancy,* and *immutability* create this ability for the said examination. Thus, we categorized *auditability* as a feature. Resulting, we positioned *transparency*, *integrity*, *immutability, redundancy,* and *privacy* as characteristics, which, however, also serve as requirements for blockchain-based G2C e-government services. Figure 2 provides an overview of the relation between characteristics and features as identified requirements.
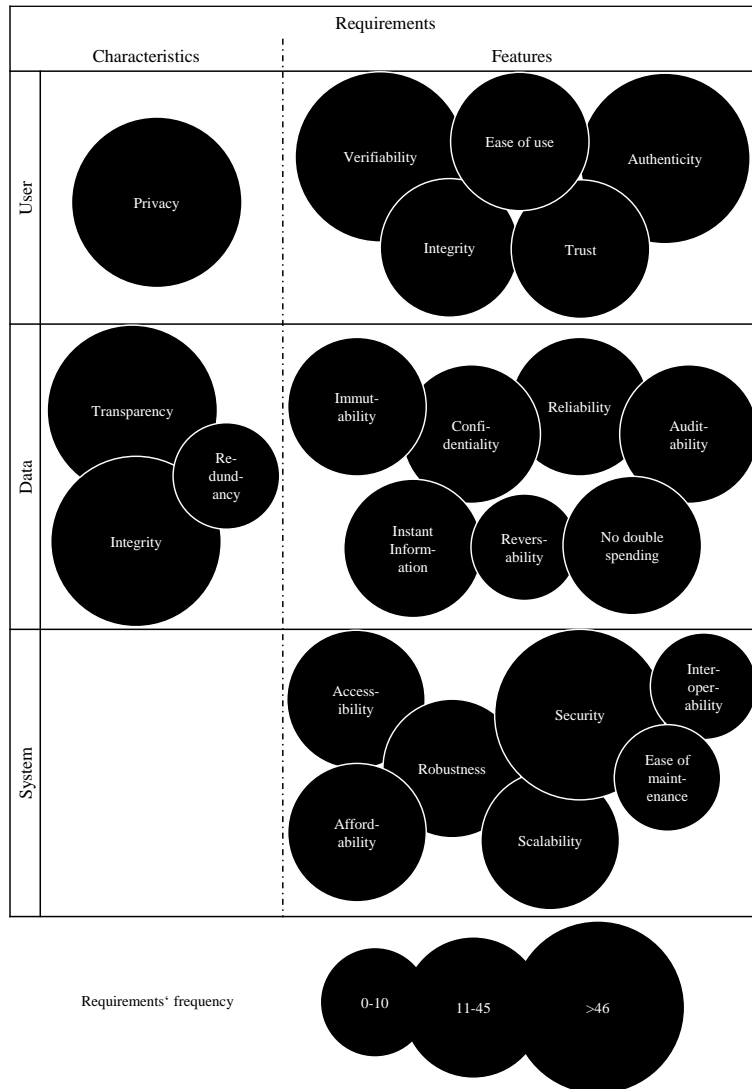
Figure 2. Structured requirements for blockchain-based G2C e-government services

5 Discussion

The current literature on blockchain-based e-government does not provide practitioners and researchers with a precise specification of the requirements that blockchain-based G2C e-government services must fulfill. For this reason, we present a structuring and categorizing overview of requirements as a basis for the development, testing, and evaluation of such services. Our analysis revealed that the requirements user-related *privacy*, data-related *transparency,* and system-related *security* are mentioned

particularly frequent. This finding may indicate an extraordinary importance of those mentioned requirements. Considering that we observe the public sector, this finding is not surprising, as those three requirements are particularly relevant for service delivery in the highly sensitive public sector. Firstly, *privacy* plays an important role in the public sector as it is crucial to prevent discrimination, which most states are committed to eradicating. Secondly, *transparency* is essential for citizens to trace whether the state represents their interests and manages their financial resources to a satisfactory degree. Finally, *security* must be guaranteed within a system, as an attack, for example during an election, would have an immense impact on the country's stability due to the great number of people affected. Against this backdrop, researchers and practitioners should consider the requirements *privacy, transparency,* and *security* when developing, testing, and evaluating blockchain-based G2C e-government services.

However, an alternative explanation for their frequency is that they are rather apparent requirements. Thus, researchers and practitioners should also be aware of the less frequently mentioned requirements, as they might be equally important. For example, *reversibility* was mentioned in total only once as a requirement for the use case taxation. However, we argue that reversibility of the data is not only essential for blockchain-based taxation services, but also for other use cases like land and property management. A mistaken assignment of a property to an individual, which lasts perpetually, would have immense consequences and may even discredit the proposed solution. This finding might even imply that blockchain, which was originally designed to immutably record unchangeable transactions, may not be the ideal solution. However, workarounds for this problem prevail [28]. In any case, the configuration and design of blockchain-based solutions must be considered very carefully and in light of alternative solutions. Furthermore, we found this requirement only once while we consider it equally important for other use cases. This gap highlights the importance of an integrative observation of all use cases to prevent missing out on some less obvious but still vital requirements.

In fact, our analysis shows that compliance with specific requirements is crucial for blockchain-based services in the public sector. Consequently, our results offer a guideline for practitioners and researchers for the development and testing as well as the evaluation of such services. In the following, we demonstrate how this can be accomplished by defining user stories. Using the taxation services use case as an example, we show how the three requirements *privacy*, *transparency, security,* and *reversibility* can be specified further. A user story addressing *privacy* might be that firstly, "as a user, my personal and financial information shall remain anonymous for the public", but secondly, "be accessible for authorized individuals such as authorized public officials". The latter is also addressed under the requirement of *transparency*: "As an authorized person, such as a public official, I may see personal and financial data of a set of specific persons". Furthermore, "as a citizen, I am able to see the aggregated sum of collected taxes transparently". Regarding its *security,* a taxation system needs to be protected against cyberattacks such as a denial-of-service attack. Moreover, practitioners could specify the requirement *reversibility* as "transactions of tax payments, which are mistakenly associated with the wrong individual, are reversible based on a substantial justification". While we exemplarily used the use case taxation

services for the specification of potential user stories, we propose that our requirements can be used as a basis for all use cases targeting the relation of G2C. Furthermore, our requirements can serve as an input for evaluation. In specific, we suggest the definition of key performance indicators based on the requirements and user stories for an evaluation of the developed services.

6 Conclusion

Regarding our theoretical contribution, our comprehensive literature review as well as the organizational and technical requirements identified lay the foundation for a successful application of blockchain-based G2C in the public sector. While we present a snapshot of the current research on blockchain-based G2C e-government services, the identified requirements may also function as a basis for an evaluation encompassing acceptance criteria. Regarding our managerial contribution, we offer a guideline for researchers and practitioners in developing, testing, and evaluating their solutions. By categorizing the identified requirements, we contribute to a harmonized and integrated view on requirements, which a blockchain-based G2C e-government service needs to fulfill. We captured requirements independently from its use case, which has two implications. On the one hand, we showed that many use cases demand similar requirements. As a result, our overarching requirements are valid for all investigated use cases. On the other hand, this approach allowed us to identify those requirements, which are not as obvious, but important, nevertheless. Hence, we support researchers and practitioners in preventing to overlook the latter.

Although having pursued a rigorous research approach, we acknowledge three limitations of our study, which may stimulate further research opportunities. Firstly, we only included peer-reviewed research articles to ensure that our results are based on high-quality research. However, grey literature may deliver even further, recent aspects. Secondly, we also observed conflicts with terminological determinism according to Ostern [11], which represents a significant problem for meaningful empirical research. Thus, the current literature on blockchain technology does not provide a clear overview of the characteristics inherent to the underlying technology and further features. By proposing a delimitation on those characteristics and features, we aim to stimulate the academic discourse on blockchain terminology. Lastly, we exclusively addressed blockchain-based G2C e-government services. In our opinion, the assessment of the relations G2G or G2B would be a promising future research opportunity, as currently no conclusion can be made whether our structured requirements in the context of G2C can also be applied to the relations of G2G and G2B.

In conclusion, our research, despite limitations, provides a structured overview of requirements, which blockchain-based G2C e-government services need to fulfill. As we showed that many requirements are rather obvious, whilst some are at risk of being overlooked, our created overview serves as a important input for the development, testing, and evaluation of such services.

References

1. Layne, K., Lee, J.: Developing fully functional E-government: A four stage model. Government information quarterly 18, 122–136 (2001)
2. Moon, M.J.: The Evolution of E-Government among Municipalities: Rhetoric or Reality? Public administration review 62, 424–433 (2002)
3. Janowski, T.: Digital government evolution: From transformation to contextualization. Government information quarterly 32, 221–236 (2015)
4. Norris, D.F.: e-government… not e-governance… not e-democracy not now! In: Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance, pp. 339–346. ACM (2010)
5. Fridgen, G., Radszuwill, S., Urbach, N., Utz, L.: Cross-organizational workflow management using blockchain technology-towards applicability, auditability, and automation. In: Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS), pp. 3507–3516 (2018)
6. Konashevych, O.: The concept of the blockchain-based governing: Current issues and general vision. In: Proceedings of the European Conference on e-Government, ECEG, pp. 79–85 (2017)
7. Khan, K.M., Arshad, J., Khan, M.M.: Investigating performance constraints for blockchain based secure e-voting system. Future Generation Computer Systems 105, 13–26 (2020)
8. Hyvärinen, H., Risius, M., Friis, G.: A blockchain-based approach towards overcoming financial fraud in public sector services. Business & Information Systems Engineering 59, 441–456 (2017)
9. Kuperberg, M., Kemper, S., Durak, C.: Blockchain Usage for Government-Issued Electronic IDs: A Survey. In: Advanced Information Systems Engineering Workshops. CAiSE 2019 International Workshops, 349, pp. 155–167. Springer, Cham, Switzerland (2019)
10. Batubara, F.R., Ubacht, J., Janssen, M.: Challenges of blockchain technology adoption for e-government. In: Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age, pp. 1–9. ACM Press, New York, New York, USA (2018)
11. Ostern, N.K.: Blockchain in the IS research discipline: a discussion of terminology and concepts. Electronic markets, 1–16 (2019)
12. Sommerville, I.: Integrated requirements engineering: a tutorial. IEEE Software 22, 16–23 (2005)
13. Gaventa, J., McGee, R.: The Impact of Transparency and Accountability Initiatives. Development Policy Review 31, 3-28 (2013)
14. Kosack, S., Fung, A.: Does transparency improve governance? Annual review of political science 17, 65–87 (2014)
15. Mensah, I.K., Vera, P., Mi, J.: Factors determining the use of e-government services: An empirical study on Russian students in China. International Journal of E-Adoption (IJEA) 10, 1–19 (2018)
16. Scholl, H.J., Klischewski, R.: E-government integration and interoperability: framing the research agenda. International Journal of Public Administration 30, 889–920 (2007)

17. Carter, L., Weerakkody, V., Phillips, B., Dwivedi, Y.K.: Citizen adoption of e-government services: Exploring citizen perceptions of online services in the United States and United Kingdom. Information Systems Management 33, 124–140 (2016)

18. Zawaideh, F.: Acceptance of E-Government services among Jordanian citizen. International Journal of Recent Advances in Multidisciplinary Research 4, 2348–2351 (2016)

19. Molnar, A., Janssen, M., Weerakkody, V.: E-Government theories and challenges: findings from a plenary expert panel. In: Proceedings of the 16th Annual International Conference on Digital Government Research, pp. 160–166. ACM Press, New York, New York, USA (2015)

20. Abu-Shanab, E.A.: Reengineering the open government concept: An empirical support for a proposed model. Government information quarterly 32, 453–463 (2015)

21. Glaser, F.: Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017). Hawaii International Conference on System Sciences (2017)

22. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A Taxonomy of Blockchain-Based Systems for Architecture Design. In: IEEE International Conference on Software Architecture (ICSA), pp. 243–252. IEEE (2017)

23. Fridgen, G., Schlatt, V., Urbach, N., Schweizer, A.: Unchaining Social Businesses– Blockchain as the Basic Technology of a Crowdlending Platform. In: Proceedings of the 38th International Conference on Information Systems (ICIS) (2017)

24. Wüst, K., Gervais, A.: Do you Need a Blockchain? In: Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45–54. IEEE (2018)

25. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: IEEE International Congress on Big Data (BigData Congress), pp. 557–564. IEEE (2017)

26. Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics 36, 55–81 (2019)

27. Alketbi, A., Nasir, Q., Talib, M.A.: Blockchain for government services — Use cases, security benefits and challenges. In: 15th Learning and Technology Conference, pp. 112–119. IEEE, Piscataway, NJ (2018)

28. Guggenmos, F., Lockl, J., Rieger, A., Wenninger, A., Fridgen, G.: How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure. In: Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS), pp. 4023–4032 (2020)

29. Lacity, M.C.: Adressing Key Challenges to Making Enterprise Blockchain Applications a Reality. MIS Quarterly Executive, pp. 201–222 (2018)

30. Avital, M., Beck, R., King, J., Rossi, M., Teigland, R.: Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future. In: Thirty Seventh International Conference on Information Systems (2016)

31. Hoffman, M.R.: Can Blockchains and Linked Data Advance Taxation. In: Companion Proceedings of the The Web Conference, pp. 1179–1182. ACM, New York, USA (2018)

32. Natarén, C., Herran, A.: Restoring Trust in Mexican Government. Preliminary Assessment of DLT Implementation. In: Proceedings of the 2019 International Conference on Blockchain Technology, pp. 24–29. ACM, New York, New York (2019)

33. Yapa, I., Heanthenna, S., Bandara, N., Prasad, I., Mallawarachchi, Y.: Decentralized Ledger for Land and Property Transactions in Sri Lanka Acresense. In: 2018 IEEE Region 10 Humanitarian Technology Conference (R10-HTC). IEEE, New York, NY, USA (2018)

34. Sanka, A.I., Cheung, R.C.: Blockchain: Panacea for Corrupt Practices in Developing Countries. In: 2019 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf), pp. 1–7. IEEE (2019)

35. Mohite, A., Acharya, A.: Blockchain for government fund tracking using Hyperledger. In: Proceedings of the 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTMES), pp. 231–234. IEEE, New York, NY, USA (2018)

36. Liu, L., Piao, C., Jiang, X., Zheng, L.: Research on Governmental Data Sharing Based on Local Differential Privacy Approach. In: 2018 IEEE 15th International Conference on E-Business Engineering (ICEBE), pp. 39–45. IEEE, Los Alamitos, CA, USA (2018)

37. Fan, L., Gil-Garcia, J.R., Song, Y., Cronemberger, F., Hua, G., Werthmuller, D., Burke, G.B., Costello, J., Meyers, B.R., Hong, X.: Sharing big data using blockchain technologies in local governments: Some technical, organizational and policy considerations. Information Polity 24, 419–435 (2019)

38. Beck, R., Müller-Bloch, C.: Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization. In: Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS), pp. 5390–5399 (2017)

39. Shahaab, A., Lidgey, B., Hewage, C., Khan, I.: Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review. IEEE Access 7, 43622–43636 (2019)

40. Kitchenham, B., Charters, S.: Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3. Engineering (2007)

41. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)

42. Nunamaker, J.F., Chen, M., Purdin, T.D.: Systems Development in Information Systems Research. Journal of Management Information Systems 7, 89–106 (1990)

43. Fu, M.-H.: Ballot Mechanism Design Based on Blockchain Methodologies. In: Proceedings of the 2nd International Conference on Computing and Big Data, pp. 91–93. ACM, New York, New York (2019)

44. Rotuna, C., Gheorghita, A., Zamifiroiu, A., Smada, D.-M.: Smart City Ecosystem Using Blockchain Technology. Informatica Economica 23, 41–50 (2019)

45. Hossain, S.S., Arani, S.A., Rahman, M.T., Bhuiyan, T., Alam, D., Zaman, M.: E-voting system using Blockchain technology. In: Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, pp. 113–117. ACM, New York, NY, USA (2019)

46. Akbari, E., Wu, Q., Zhao, W., Arabnia, H.R., Yang, M.Q.: From Blockchain to Internet-Based Voting. In: 2017 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 218–221. IEEE (2017)

47. Perez, A.J., Ceesay, E.N.: Improving End-to-End Verifiable Voting Systems with Blockchain Technologies. In: 2018 IEEE International Conference on Internet of Things

(iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1108–1115. IEEE (2018)

48. Singh, A., Chatterjee, K.: SecEVS : Secure Electronic Voting System Using Blockchain Technology. In: 2018 International Conference on Computing, Power and Communication Technologies (GUCON), pp. 863–867. IEEE (2018)

49. Murtaza, M.H., Alizai, Z.A., Iqbal, Z.: Blockchain Based Anonymous Voting System Using zkSNARKs. In: 2019 International Conference on Applied and Engineering Mathematics (ICAEM), pp. 209–214. IEEE (2019)

50. Sheer Hardwick, F., Gioulis, A., Naeem Akram, R., Markantonakis, K.: E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1561–1567. IEEE (2018)

51. Khan, K.M., Arshad, J., Khan, M.M.: Secure Digital Voting System Based on Blockchain Technology. International Journal of Electronic Government Research 14, 53–62 (2018)

52. Wibowo, S., Sandikapura, T.: Improving Data Security, Interoperability, and Veracity using Blockchain for One Data Governance, Case Study of Local Tax Big Data. In: 2019 International Conference on ICT for Smart Society (ICISS), pp. 1–6. IEEE (2019)

53. Cooley, R., Wolf, S., Borowczak, M.: Blockchain-Based Election Infrastructures. In: 2018 IEEE International Smart Cities Conference (ISC2), pp. 1–4. IEEE, Piscataway, NJ (2018)

54. Nguyen, N.-H., Nguyen, B.M., Dao, T.-C., Do, B.-L.: Towards Blockchainizing Land Valuation Certificate Management Procedures in Vietnam. In: 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), pp. 1–6. IEEE (2020)

55. Alam, A., Zia Ur Rashid, S.M., Abdus Salam, M., Islam, A.: Towards Blockchain-Based E-voting System. In: 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET), pp. 351–354. IEEE, Piscataway, NJ (2018)

56. Fatrah, A., El Kafhali, S., Haqiq, A., Salah, K.: Proof of Concept Blockchain-based Voting System. In: Proceedings of the 4th International Conference on Big Data and Internet of Things, pp. 1–5. ACM, New York, NY, USA (2019)

57. K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri, S. Gupta: A Comparitive Analysis on E-Voting System Using Blockchain. In: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pp. 1–4 (2019)

58. E. Zaghloul, T. Li, J. Ren: Anonymous and Coercion-Resistant Distributed Electronic Voting. In: 2020 International Conference on Computing, Networking and Communications (ICNC), pp. 389–393. IEEE (2020)