Trust through Digital Technologies: Blockchain in Online Consultancy Services

Sebastian Gerth
University of Erfurt
Nordhäuser Str. 63
99089 Erfurt, Germany
+49-160-952-666-01
sebastian.gerth@uni-erfurt.de

Lars Heim
Clausthal University of Technology
Julius-Albert-Str. 2
38678 Clausthal-Zellerfeld, Germany
+49-179-742-1866
lars.heim@tu-clausthal.de

ABSTRACT
This paper examines the concept of trust in an increasingly digital society on the one hand and how it can be established with regard to digital documentation of online help services on the other. Trust is particularly important in the sector of digital services sector because requests and offers for help, and thus highly sensitive data, are offered, processed, and used on various online channels. With the advent of blockchain technology, there is a new central opportunity to create trust on digital platforms such as those used for online help services. After clarification of relevant concepts and terms, diverse forms of the blockchain technology are explained on the basis of the individually specific configuration of a blockchain. The main emphasis lies on federated blockchains which provide the central advantages of blockchain technology while avoiding the risk of passing on sensitive data. This results in a possible use of the technology for the area of digital services.

CCS Concepts
• Social and professional topics → Professional topics → Management of computing and information systems → Software management → Software selection and adaptation • Security and privacy → Systems security → Distributed systems security

Keywords
Blockchain; Trust; Digital services; Consulting; Federation

1. INTRODUCTION
The most recent data abuse scandals, such as the Doxing Gate at the end of 2018, where the user "0rbit" or "G0d" made data of celebrities available to the public, or the case of Cambridge Analytica in 2016, where millions of Facebook data were unlawfully evaluated for Donald Trump's election campaign, are probably still well remembered by most readers. The incidents show that we live less in an information age and more in an age of trust. While information on digital news, social media and knowledge platforms is constantly available and growing in content [16, 15, 27], trust is a commodity that the actors either have to strategically develop or laboriously reconquer if they hope for the favour of the users [17, 20, 21]. This article aims to shed light on the contribution of blockchain technology to the creation of trust in digital services and advisory services.

ICBCT'20, March 12–14, 2020, Hilo, HI, USA

ACM ISBN 978-1-4503-7767-6/20/03…$15.00
https://doi.org/10.1145/3390566.3391662

2. DIGITAL SERVICES
2.1 Online Consultancy Services and Trust
The range of digital services is extremely diverse and stretches from the (partial) public provision of information or communication options such as chats, e-mail etc., to online banking, billing and payment systems, e.g. for e-commerce solutions, to e-learning and concrete personal counselling services [7, 24, 39]. A common feature of all digital services is that they are generally provided by centralised institutions which themselves have a high degree of digitization and are represented via digital platforms [27, 31]. As a result, the business models are highly scalable and corresponding organisations can have pronounced market power [22, 41]. In this article, a digital service is defined as a service offered on a digital platform for solving a socially or individually relevant problem: collecting, storing and processing personal data by the providing institution. If individuals need concrete help and request it via a digital platform and receive it online, this is referred to as e-help [12]. As part of this, online counselling is given more attention in this article. We understand it as an exchange of information between at least two persons via digital channels, whereby a counsellor individually takes care of a problem of one or more clients in order to improve their mental state at the content level. In order for an online consultation to take place, the client must trust the digital platform or the consultant and thus intermediaries.

If services are offered on the Internet, the decision to use them is also associated with online trust, which must be given to digital services. Corritore et al. [13] design an online trust model (cf. Fig. 1) with three central factors determining trust (especially in relation to websites): credibility (e.g. expertise or reputation), ease of use (e.g. usability) and the perceived risk. The arrows shown in Figure 1 illustrate the directions of influence of the respective user- or website-centered components and leading external factors, whereby it becomes clear that all model components determine the emergence of trust. Special relevance in this contribution is given to the factor “risk”, because the perception of the same can be minimized by transparent communication via the use of blockchain technology.

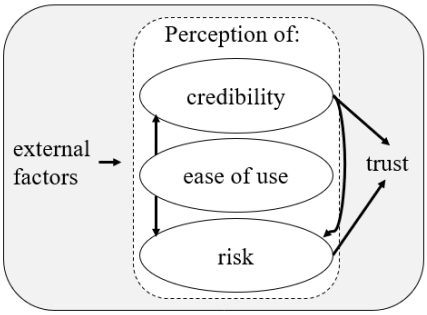

Figure 1. Model of trust for online offers [13, 25]

The prospects for success of a digital service offering thus depend not only on the individual advantage for the customer, but also on short-term and long-term trust in the underlying technology and the company or the actors themselves [2].

2.2 Online Consulting: Trust in the Players?

It is possible to define three different parties involved in online consulting:

(1) those seeking or receiving help,

(2) digital platforms (companies, public institutions or intermediaries) and

(3) providers of assistance in the sense of consultants, who contact the person seeking assistance directly.

In order to take advantage of a help offering, it is essential for (1) to build up trust in (2) and (3) and to maintain this trust after an initial contact or consultation. This trust is not self-evident. Kirchner/Beyer [30] state that the fundamentals of cooperation between customers and providers on the Internet are uncertain. Often the necessary mutual trust is lacking here. With reference to Brinkmann/Seifert [6] and Diekmann/Wyder [18], they also note that overall trust on the Internet is less pronounced [30]. They justify this, among other things, by a lack of cooperation security (market transactions entail risks due to insufficient behaviour between clients and providers). Recent studies also prove the central importance of security. The DIVSI exemplifies that 84 percent of German Internet users think that companies are responsible for the security of their customers – at the same time, two thirds of Internet users have little or no confidence that this will be adequately guaranteed [20]. The Connected Life 2018 study [28] also shows that 56 percent of German respondents are worried about the amount of data collected and its use for business purposes.

The description of trust indirectly refers to the relevant dimensions of trust for reducing the perceived risk of using Internet-based services: discretion on the part of advisors and the security as well as protection of documented or processed data.

Confidentiality can, for example, be guaranteed by a self-imposed pledge of non-disclosure. The existence of confidentiality as well as mandatory compliance with it should be publicly communicated. Ultimately, this is a form of anonymity vis-à-vis third parties. It seems useful if those seeking help always have the same contact person, even though complete digital documentation in the form of a customer administration – for example using a personalized e-file [40, 29] – offers the possibility that colleagues can also offer their help in an emergency. In addition, it is occasionally necessary to consult several times in order to solve a problem, so that a future request for help can be based on the client's record. Availability can be controlled via cloud applications and the assignment of corresponding access rights to the personal e-file, in whatever form it may be. In particular, the protection against manipulation, disclosure and loss of relevant data relates to the underlying IT infrastructure.

Usually, data protection is regulated by specific directives such as the European General Data Protection Regulation (EU-GDPR) and must be implemented by intermediaries or organisations involved in online consultations. In order to archive data digitally in the long term [23], it is principally possible to work with local systems, i.e. software installed on local computers and/or storage on individual data carriers. Modern working environments, on the other hand, use certain cloud systems as de-facto standard. The main advantage of these systems is that the data can be stored on servers that are usually made available externally. These are mostly operated in data centers, which in turn specialize in their operation, administration, security, and access protection as a business model. Hardware acquisition and maintenance are therefore no longer necessary on the company side when external services are used; the services provided can be easily adapted depending on organisational development and, if necessary, several existing or new company locations can be easily integrated. SaaS models, for e.g. specific CRM systems used to document customer contacts, also enable a reliable cost calculation.

This already shows that it is not only clients who must have confidence in the institution in order to use it, but also the management of the organisation itself must have confidence in cloud providers with regard to data security, data sovereignty, access, and processing, as well as storage location, maintenance, failure protection, etc. [1, 8, 43], which provides and secures the technological basis for working with clients. In addition to this trust, dependence on the cloud or SaaS provider also plays an important role, as non-compliance with data protection and security standards ultimately falls back on the institution. The current practice of data processing and the reasons given above motivate us to consider alternatives and/or possible solutions. Blockchain technology offers an opportunity to increase not only data security, but also data protection, as described in the following section.

3. BLOCKCHAIN TECHNOLOGY

3.1 Blockchain: Definition of Terms, Technical Basics, Advantages and Disadvantages

In the scientific literature there is disagreement about a generally applicable definition of blockchain, since different scientific directions, such as economics, computer science and law, collide and simultaneously deal with the common terms used in the practical application of the technology. In a comprehensive, interdisciplinary analysis, Meijer [35] summarizes all relevant elements of definition from both scientific and application-oriented literature. This results in the following description:

"Blockchain technology is a distributed, shared, encrypted, chronological, irreversible and incorruptible database and computing system (public/private) with a consensus mechanism (permissioned/permissionless), that adds value by enabling direct interactions between users" [35].

The Blockchain offers numerous advantages. The technology provides a new level of transparency as all transactions can be monitored. In addition, the blockchain code is often openly

configurable. Decentralization ensures that each participant has equal rights and has a synchronized, validated and up-to-date version of the blockchain at all times. This also means that decisions (e.g. about code updates) are made by the majority. By storing the blocks in the distributed network, verifying the transactions by numerous nodes, cryptographic encryption and complex consensus mechanisms, a high degree of integrity and manipulation security is created in a blockchain [26]. This makes it highly reliable and trustworthy (e.g. for proof to a third party, such as a health insurance company). Decentralized data processing with a large number of replications also leads to a high level of reliability [9]. This redundancy thus provides effective protection against attacks and data loss. The linking of the individual data blocks with the help of transparent hashing in the distributed network also ensures good traceability of the permanently traceable transaction history [14]. The users have more control over their personal data and the transactions themselves and thus over their own privacy [4]. The Blockchain also makes it possible to process transactions faster and more efficiently than previous procedures. This can lead to an increase in quality at lower costs compared to other IT instruments. The technology also provides disintermediation, i.e. the streamlining of value chains, which can prevent dominant market positions [38]. In particular (fee-based) intermediary players are affected as they can be eliminated by the Blockchain [19]. For example, banks would no longer be necessary for a direct transfer or notaries for the confirmation of contracts. In this way, for example, corruption can be prevented, which means that the blockchain is not only technologically and economically but also socially relevant.

3.2 Types and Possibilities of Digital Trust-building in Online Consultancy Services through the Blockchain

A differentiation can be made between the different blockchain types, which offer different application possibilities due to their varying configuration [35]. According to Kudra [33] two essential dimensions can be applied:

1. dimension "access"

user rights with regard to read and write permissions and the execution of transactions (public vs. private),

2. dimension "validation"

user rights in relation to participation in the consensus mechanism (permissionless vs. permissioned).

These two dimensions can be combined to define four blockchain types [3, 11, 32, 33, 35]. These are summarized in the following table 1:

When the possibilities of digital trust-building in online consultancy services through the blockchain-technology are taken into consideration, private blockchains appear to be well suited for use in outwardly separated organizations such as private companies. They seem particularly predestined, even though they do not correspond to the basic idea of the decentralized public with a centralized approach. On a private blockchain, access is approved, for example, by a digital consultation request with subsequent consultation by the operator or consultant and thus ultimately by a specific institution. At the same time, it can be defined within the organizational structure which employee can take care of specific tasks on the basis of the stored data. For example, a consultant needs information on certain matters, while the payment for the service used is essentially of interest to the finance department.

Table 1. Types of blockchain technology

		Validation		
		permissionless	**permissioned**	
			Single Organization *(Single Authority Blockchain)*	**Consortium** *(Federated Blockchain)*
Access	**public**	public-permissionless	public-permissioned	public-permissioned
	private	private-permissionless	private-permissioned	private-permissioned

Source: own presentation

An institution that uses a private blockchain retains complete control over the system because all users and also all operators of the consensus mechanism are known. In comparison to a public-permissionless blockchain, trust in the validators is necessary [10]. External parties – such as health insurance companies, employers or friends and acquaintances of the person looking for help – cannot access the system. This serves to protect the blockchain and the data it contains. Just like the validation of transactions, the further development and updating of the blockchain falls to the limited group of validators [34]. According to Buterin [10], it is much easier to extend or improve the blockchain, since, for example, coordination processes can be streamlined. The revision of transactions is also possible in this environment through a rollback, since the group of validators is clearly defined [34]. Private blockchains are also very well scalable and can be easily extended if necessary. It is therefore well possible to initially test them on a small scale and, if successful, extend them [11]. Legal framework conditions can also be clearly defined, since the blockchain can be clearly assigned to a company or other group of users [5].

These aspects support the use of private blockchains in online consultancy services. However, their centralisation and the associated disadvantages are problematic. In order to avoid the centralization of private blockchains, a so-called Federated Blockchain can be considered as an option. In this case, more than one institution is responsible for maintaining the network or for validation. This results in a mutual control, since the instances make decisions jointly and mostly for the benefit of the network. Such a consortium therefore agrees on a consensus if the majority votes for a certain action (e.g. a change of code, access rights, etc.). Wrong decisions or manipulations by individuals can thus be prevented as far as possible and the advantages of (limited) decentralisation can still be exploited. In the case of online consultations, such a regulatory consortium may consist of companies active in the market, health insurance funds and psychological associations. The blockchain then serves as a digital instrument, which creates trust between all parties involved in the consulting process and at the same time enables the progress of this technology.

4. CONCLUSION

As described above, the topic of digital services has already been established in social and scientific discourse for several years, and blockchain technology is increasingly gaining in-depth, interdisciplinary attention. So far, however, a linking approach to these two technological currents has remained largely unnoticed. This contribution counteracts this lack of awareness by examining relevant terms using the example of online consulting and the possibilities of creating and maintaining trust through the blockchain. We show that online trust is linked to frequently subjectively-perceived factors such as credibility, simplicity, and risk of using digital services (cf. Fig. 1). For the first time in history, the blockchain makes it possible to build trust and maintain it through decentralised technology on an objective level, since trust no longer has to be located centrally [42, 45]. It can be stated that especially Federated Blockchains seem to be suitable for data processing in digital services. They combine most advantages which allow those seeking and receiving help to interact with each other in the best possible way without the risk of data being lost to third parties

Because of all the points discussed, it is plausible that the blockchain will play an essential and important role in the future design of IT processes and will accordingly become of immense importance for a large number of socially relevant areas [36, 37]. A reason for this is that the content of a blockchain does not have to be predetermined. [44].

5. REFERENCES

[1] Backhaus, N. and Thüring, M. 2015. Trust in Cloud Computing: Pro and Contra from the User's Point of View. *I-com* 14, 3, 231-243.

[2] Beldad, A., de Jong, M., and Steehouder, M. 2010. How shall I trust the Faceless and the Intangible? A Literature Review on the Antecedents of Online Trust. *Computers in Human Behavior.* 26, 5, 857-869.

[3] BitFury Group. 2015. Public versus Private Blockchains Part 1: Permissioned Blockchains. (July. 2019). https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf

[4] Bogdan, B. 2018. *MedRevolution*. Springer, Berlin.

[5] Bogensperger, A., Zeiselmair, A., and Hinterstocker, M. 2018. Die Blockchain-Technologie - Chance zur Transformation der Energieversorgung? (July. 2019). https://www.ffe.de/attachments/article/803/Blockchain_Teilbericht_Technologiebeschreibung.pdf

[6] Brinkmann, U. and Seifert, M. 2001. „Face to Interface": Zum Problem der Vertrauenskonstitution im Internet am Beispiel von elektronischen Auktionen. *Zeitschrift für Soziologie.* 30, 1, 23-47.

[7] Bruhn, M. and Hadwich, K. 2017. Dienstleistungen 4.0 – Erscheinungsformen, Transformationsprozesse und Managementimplikationen. In *Dienstleistungen 4.0. Geschäftsmodelle - Wertschöpfung – Transformation,* M. Bruhn, K. Hadwich, Ed. Band 2. Springer Gabler, 1-39.

[8] Buch, M. S., Gebauer, L., and Hoffmann, H. 2014. Vertrauen in Cloud Computing schaffen - aber wie? *Wirtschaftsinformatik & Management*. 6, 3, 67-77.

[9] Burgwinkel, D. 2016. Blockchaintechnologie und deren Funktionsweise verstehen. In *Blockchain Technology: Einführung für Business- und IT Manager,* D. Burgwinkel, Ed. De Gruyter Oldenbourg, Basel, 3-50.

[10] Buterin, V. 2015. On Public and Private Blockchains. (August. 2019). https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[11] Carson, B., Romanelli, G., Zhumaev, A., and Walsh, P. 2018. Blockchain beyond the Hype: What is the Strategic Business Value? McKinsey & Company - Our Insights. (July. 2019). https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

[12] Charman, D., Harms, C., and Myles-Pallister, J. 2010. Help and E-Help: Young People's Perspectives of Mental Healthcare. *Australian Family Physician.* 39, 9, 663-665.

[13] Corritore, C. L., Kracher, B., and Wiedenbeck, S. 2003. On-line Trust: Concepts, Evolving Themes, a Model. *International Journal of Human-Computer Studies.* 58, 737-758.

[14] Consultancy UK. 2017. Blockchain Technology: How it works, Main Advantages and Challenges. (July. 2019).https://www.consultancy.uk/news/13484/blockchain-technology-how-it-works-main-advantages-and-challenges

[15] de Reuver, M., Sørensen, C., and Basole, R. C. 2018. The Digital Platform: A Research Agenda. *Journal of Information Technology.* 33, 2, 124-135.

[16] Demary, V. 2016. *Der Aufstieg der Onlineplattformen: Was nun zu tun ist*. IW-Report, 32. Institut der deutschen Wirtschaft (IW), Köln.

[17] Diekhöner, P. K. 2018. *The Trust Economy. Warum jedes Unternehmen eine Vertrauensstrategie braucht, um im digitalen Zeitalter zu überleben*. Springer Gabler, Berlin.

[18] Diekmann, A. and Wyder, D. 2002. Vertrauen und Reputationseffekte bei Internet-Auktionen. *Kölner Zeitschrift für Soziologie und Sozialpsychologie.* 54, 674-693.

[19] Düring, T. and Fisbeck, H. 2017. Einsatz der Blockchain-Technologie für eine transparente Wertschöpfungskette. In *CSR und Digitalisierung. Der digitale Wandel als Chance und Herausforderung für Wirtschaft und Gesellschaft,* A. Hildebrandt, W. Landhäußer, Ed. Springer Gabler, Berlin, 449-464.

[20] DIVSI, Deutsches Institut für Vertrauen und Sicherheit im Internet. 2017a. Digitalisierung – Deutsche fordern mehr Sicherheit. (May. 2019). https://www.divsi.de/wp-content/uploads/2018/02/DIVSI-Studie_Digitalisierung_Deutsche-fordern-mehr-Sicherheit_2017-08.pdf

[21] DIVSI, Deutsches Institut für Vertrauen und Sicherheit im Internet. 2017b. Vertrauen in Kommunikation im digitalen Zeitalter. (May. 2019). https://www.divsi.de/wp-content/uploads/2017/12/DIVSI-Vertrauen2018.pdf

[22] Gundlach, H. 2009. Marktmacht und Meinungsmacht digitaler Plattformen. In *Fernsehen im Wandel. Mobile TV & IPTV in Deutschland und Österreich,* J. Krone, Ed. Nomos, Baden-Baden, 53-77.

[23] Hackel, S. and Roßnagel, A. 2008. Langfristige Aufbewahrung elektronischer Dokumente. In *Informationelles Vertrauen für die Informationsgesellschaft,*

D. Klumpp, H. Kubicek, A. Roßnagel, W. Schulz, Ed. Springer, Heidelberg, 199-207.

[24] Hanekop, H., Tasch, A., and Wittke, V. 2001. „New Economy" und Dienstleistungsqualität: Verschiebung der Produzenten- und Konsumentenrolle bei digitalen Dienstleistungen. *SOFI-Mitteilungen.* 29, 73-91.

[25] Hauck, J. 2017. *Vertrauen in service-orientierten Online-Communitys*. Nomos, Baden-Baden.

[26] Hooper, M. 2018. *IBM*. (July. 2019). https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/

[27] Jaekel, M. 2017. *Die Macht der digitalen Plattformen. Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz*. Springer Vieweg, Wiesbaden.

[28] Kantar. 2018. Connected Life 2018. (May. 2019). https://www.kantartns.de/wissensforum/studien/connected-life/index.asp

[29] Karg, M. 2013. Datenschutzrechtliche Anforderungen an die E-Akte. *Datenschutz und Datensicherheit – DuD.* 37, 11, 702-708.

[30] Kirchner, S. and Beyer, J. 2016. Die Plattformlogik als digitale Marktordnung. *Zeitschrift für Soziologie.* 45, 5, 324-339.

[31] Kofler, T. 2018. *Das digitale Unternehmen. Systematische Vorgehensweise zur zielgerichteten Digitalisierung.* Springer Vieweg, Berlin.

[32] Kravchenko, P. 2016. Ok, I need a Blockchain, but which one? Medium. (July. 2019). https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-butwhich-one-ca75c1e2100

[33] Kudra, A. 2018. Blockchain trifft Digital Identity. (July. 2019). https://www.informatik-aktuell.de/betrieb/virtualisierung/blockchain-trifft-digital-identity.html

[34] Kudra, A., Baumann, C., Dehning, O., Hühnlein, D., Pirozhkov, S., Raumann, M., and Stommel, S. 2017. TeleTrust- Bundesverband IT-Sicherheit. (July. 2019). https://www.teletrust.de/fileadmin/docs/publikationen/broschueren/Blockchain/2017_TeleTrusT-Positionspapier_Blockchain__.pdf

[35] Meijer, D. 2017. *Consequences of the Implementation of Blockchain Technology*. Delft University of Technology, Delft.

[36] Rieck, S. 2019. Potenzial der Blockchain – Infrastruktureller Paradigmenwechsel. In *Strategie und Transformation im digitalen Zeitalter. Inspirationen für Management und Leadership.* M. Dahm, S. Thode, Ed. Springer Gabler, Wiesbaden, 221-236.

[37] Rosenberger, P. 2018. *Bitcoin und Blockchain. Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik*. Springer Vieweg, Berlin.

[38] Song, W., Shi, S., Xu, V., and Gil, G. 2016. Blockchain Technology. Advantages and Disadvantages of Blockchain Technology. (July. 2019). https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/

[39] Stich, V., Schumann, J. H., Beverungen, D., Gudergan, G., and Jussen, P., Ed. 2019. *Digitale Dienstleistungsinnovationen. Smart Services agil und kundenorientiert entwickeln*. Springer Vieweg, Berlin.

[40] Ströher, A. and Honekamp, W. 2011. ELGA – die elektronische Gesundheitsakte vor dem Hintergrund von Datenschutz und Datensicherheit. *Wiener Medizinische Wochenschrift.* 161, 13-14, 341-346.

[41] Täuscher, K., Hilbig, R., and Abdelkafi, N. 2017. Geschäftsmodellelemente mehrseitiger Plattformen. In *Digitale Transformation von Geschäftsmodellen. Schwerpunkt: Business Model Innovation.* D. Schallmo, J. Reinhart, E. Kuntz, Ed. Springer Gabler, Wiesbaden, 179-211.

[42] Tapscott, D. and Tapscott, A. 2018. *Die Blockchain-Revolution. wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert*. Plassen, Kulmbach.

[43] Walterbusch, M. and Teuteberg, F. 2012. Vertrauen im Cloud Computing. *HMD Praxis der Wirtschaftsinformatik.* 49, 6, 50-59.

[44] Wiefling, S., Lo Iacono, L., and Sandbrink, F. 2017. Anwendung der Blockchain außerhalb von Geldwährungen. *Datenschutz und Datensicherheit.* 41, 8, 482-486.

[45] Wildhaber, B. 2016. Kann man Blockchains vertrauen? In *Blockchain Technology: Einführung für Business- und IT Manager,* D. Burgwinkel, Ed. De Gruyter Oldenbourg, Basel, 149-158.