Privacy Concerns and Consumer Acceptance of Blockchain-Enabled Services

Research in Progress

Andreas Strebinger
York University, Toronto
strebing@yorku.ca

Horst Treiblmaier
Modul University Vienna
horst.treiblmaier@modul.ac.at

ABSTRACT

When creating Blockchain-Enabled Services (BCES) for consumers, service providers have to be aware of consumers' privacy concerns. We argue that Blockchains are perceived ambivalently by consumers regarding privacy and that startup BCES companies will be affected differently by privacy concerns than established brands. On the one hand, consumers may perceive the decentralized nature of Blockchains as an inherent privacy risk due to potential data breaches. On the other hand, BCES provide consumers with the opportunity to escape data eco-systems of existing company networks, particularly when BCES are provided by a startup. We develop various hypotheses on the impact of privacy concerns on the acceptance of BCES. Using scenarios with BCES applications for international money transfer and hotel booking, we suggest an experimental design which manipulates the nature of the provider (startup versus established brand) and the amount of services provided.

Keywords

Blockchain, Privacy Concerns, Technology Acceptance, Experiment, Brand, Trust

INTRODUCTION

Blockchain technology is predicted to become a major disruptor for numerous industries, including financial services, tourism, transportation and the public sector (Treiblmaier and Beck, 2019a, 2019b). Designed as a decentralized network controlled by peers, it offers distributed and immutable data as well as a shared and consistent data view for all network participants (Treiblmaier, 2019). Blockchain technology adds a new state layer to the Internet protocol that allows for the recording of product attributes as well as personal information including personal identity, property information and ownership rights (Wolfond, 2017). It also enables secure peer-to-peer transactions which may lead to a full ("true") disintermediation of business-to-business (B2B) and business-to-consumer (B2C) transactions. More likely, though, Blockchain Technology will lead to some form of re-intermediation (Ertemel, 2018), in particular for B2C transactions. For example, numerous startup companies around the world already provide consumers with online platforms and apps to transfer money domestically and internationally on a peer-to-peer basis or to book rooms directly with a hotel (Bouveret and Haksar, 2018; Önder and Treiblmaier, 2018). These platforms and apps work with and without the use of cryptocurrencies. Such BCES may offer consumers lower costs, higher convenience or a lower time to completion of the transaction (Tapscott and Tapscott, 2017).

Similar to the re-intermediation which happened as a consequence of the Internet (Strebinger and Treiblmaier, 2004), trust in online providers will be vital for consumer acceptance of BCES (Chang and Chen, 2008; Morgan-Thomas and Veloutsou, 2013). This may especially affect established companies and well-known brands, even when entering BCES markets as second movers. Also, traditional incumbents such as credit card companies, banks and established booking platforms may be well positioned to provide value-added services to consumers, due to their established supply chains and industry networks.

However, both established brands and startups may also face new challenges due to privacy concerns which consumers could harbor vis-à-vis BCES. In this research-in-progress paper, we investigate the effect of consumers' privacy concerns on the acceptance of BCES. We argue that privacy concerns exert both positive and negative effects on BCES adoption and may affect established brands and startups in a different fashion.

BLOCKCHAIN AND CONSUMER PRIVACY CONCERNS

Privacy concerns may be a major impediment to the acceptance of new technologies and online services (e.g., Lemay, Doleck and Bazelais, 2017; Miltgen, Popovic and Oliveira, 2013; Tan, Li, Kim and Hsu, 2012; Zhou, 2011). Blockchains have profound implications on how data is being recorded and disseminated. Decentralized databases

store exact copies on numerous nodes which makes changes or deletion virtually impossible[1].

Objectively speaking, Blockchain technology may hold advantages and disadvantages for consumer privacy (Rui Zhang et al., 2019; Feng et al., 2019). On the one hand, it allows storing data in an immutable way and may be used, for example, by governments, to create surveillance systems to encourage desired behavior. This evokes visions of intrusive governments overseeing and controlling humans' most private decisions (Sedgwick, 2019). Also, Blockchain technology may be employed by companies to establish a "single customer view" and allows for tracking individual customers across all online platforms (Ghose, 2018) and verifying actual consumer exposure to advertising in order to fight online advertising fraud with invalid traffic (Ghose, 2018; Mamais and Theodorakopoulos, 2017). On the other hand, Blockchain offers the means to give privacy back into the hands of consumers by allowing them to determine which personal information they want to share (Tapscott and Tapscott, 2017; Wolfond, 2017), possibly for a monetary or non-monetary incentive (e.g., https://basicattention-token.org/). In this context, encryption technology can help to conceal the origin of data, enhance privacy and lower the risk of data breaches (Tapscott and Tapscott, 2017; Wolfond, 2017; Feigenbaum, 2019).

Subjectively, consumers may meet BCES with mixed feelings when it comes to their privacy, albeit with a somewhat different reasoning. On the one hand, any form of re-intermediation may offer them a welcome escape from existing "data-hungry" ecosystems built around the current provider of the respective service (e.g., their bank or credit card company, their preferred booking platform) (Subramanian, 2018). Consumers harboring general concerns about "Big Data", namely the amount of data collected and its use and dissemination by companies should hence perceive Blockchain technology to bring about advantages in terms of privacy. This advantage should be more pronounced for BCES offered by startup companies rather than by a BCES provider carrying a well-known brand name.

On the other hand, the complexity of Blockchain technology and its specific implications on privacy may be hard to grasp for average consumers. As of 2019, the general understanding of Blockchain technologies, which are in a permanent state of development, is still rudimentary. This not only is true for the general public but frequently also for C-level management. Currently, mass adoption is being hampered by inefficient user interfaces, a connection to criminal activities as well as scalability issues. Technical, organizational and regulatory issues need to be solved before mass adoption can occur (Hughes et al., 2019), but, given the manifold benefits that are expected, such an adoption on this side of the organizations is reasonable to predict (Clohessy et al., 2019).

Once consumers are rudimentarily familiar with the basic workings of Blockchains, they may intuitively object to the idea of their data being distributed across many nodes, despite promises of powerful encryption and pseudonymity of data, whose limitations have been previously highlighted (Meiklejohn *et al.*, 2016). They may even be afraid that unauthorized access to their data is simpler and data breaches more likely when a service uses Blockchain technology rather than a conventional centralized storage. Previous hacks and breaches associated with Blockchain technologies such as the DAO hack or the recent Binance hack make it hard for consumers without a sufficient technical background to understand the details of the respective hacks and to what extent Blockchain technology was to blame (del Castillo, 2019; Vigna, 2016).

We hence posit that consumers with high privacy concerns view BCES with suspicion. Such consumers should also perceive a higher risk of data breaches when using BCES (Hong and Thong, 2013):

H_1: The perceived risk of data breaches when using BCES is higher for consumers with high rather than low internet privacy concerns regarding the collection of data online.

This, in turn should exert a negative impact on the acceptance of BCES:

H_2: The perceived risk of data breaches when using BCES influences consumer acceptance of BCES in a negative manner.

However, once the perceived risk of data breaches is accounted for, the privacy benefits created by leaving traditional data ecosystems and using BCES should become apparent, particularly among consumers worried by the amount and use of data which companies collect on them:

H_3: When controlling for the effect of perceived risk of data breaches, consumer acceptance of BCES is higher for consumers with high internet privacy concerns regarding data collection.

As we expect the positive residual effect of privacy concerns on attitudes toward BCES to be driven by the wish of leaving "traditional" big data ecosystems, it should be more pronounced when a BCES is offered by a startup rather than by a well-known established company:

H_4: When controlling for the effect of perceived risk of data breaches, the positive effect of privacy concerns

[1] So-called hard-forks can be used to change the history of a Blockchain and "editable" Blockchains have been previously suggested, but it is the immutability of the data which is a core characteristic of Blockchain technology and any deviations from immutability will inevitably lead to other problems and shall not be discussed here any further.

on consumer acceptance of BCES is higher when the BCES is provided by a startup company rather than by a provider carrying a well-known brand name.

Figure 1 shows the conceptual model to be tested in our empirical studies.

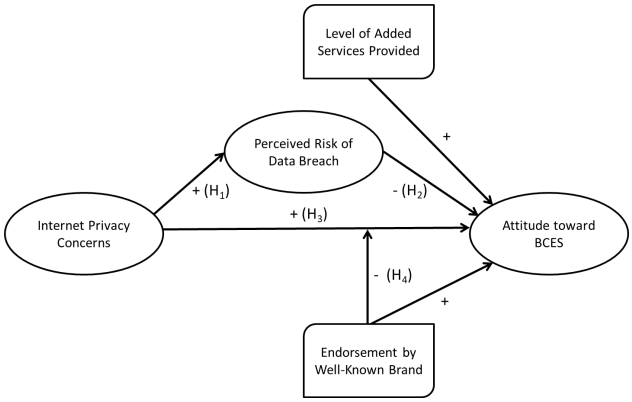

Figure 1: Conceptual Model

METHOD

We test these hypotheses in three studies in which North-American respondents evaluate BCES apps for international money transfer and international hotel bookings. In all three studies, we manipulate, across scenarios and respondents, (1) the nature of the provider of the service (unknown startup company versus endorsement by a well-known brand name); and/or (2) the service level provided by the BCES (transaction only versus added value services provided).

After questions on demographic characteristics, category usage as well as respondents' familiarity with Blockchain technology, subjects are introduced, in everyday English, to the basic concept of Blockchains. They then are presented with two scenarios (one hotel-booking scenario, one money-transfer scenario) randomly rotated across respondents.

For the condition "startup company" for money transfer and travel booking, we use a fictitious app name of generic nature (BLOCKPAY) and pretested for neutral meaning (ITC Hotel Booking), respectively. In the condition "endorsement by a well-known brand", we employ the same app names, but the brand (i.e., name and logo) of a well-known tech company is added in slightly smaller size underneath the fictitious app name (study 1: Microsoft, IBM; studies 2 and 3: IBM, Amazon). Added-Value Services comprise, for example, options for cancellation or refund, customer reviews, call-center support, and assistance with lost passwords. These are not provided in the scenarios of the "transaction-only" conditions. To create a realistic setting, BCES are described as allowing for savings of between 1.5% and 10% as compared to traditional intermediaries, depending on the service category (money transfer versus hotel booking) and the level of added-value services provided by the BCES. For example, the "startup / added-value services" condition for booking a hotel confronts respondents of study 1 with the scenario of a trip to Mexico. Respondents have the option of booking their hotel directly through a Blockchain-enabled app named "ITC Hotel Booking". It offers 7.5% savings over traditional booking platforms, access to hotel reviews, call center support and cancellation options under certain conditions.

In the "transaction-only" conditions, savings as compared to traditional online booking platforms are higher (10%), but no call center support, cancellation options, or hotel reviews are available. Timed page exposure ensure that respondents spend the required time reading the scenarios.

After each scenario, respondents indicate their attitude toward the BCES as well as their choice between BCES, their current provider, and other alternatives. Thereafter, open-ended questions inquire about the reasons of their choice. At the end of the survey, respondents answer questions on the specific risk of data breaches as well as their general internet privacy concerns (Hong and Thong, 2013). Risk of data breach is measured with a single item, "On a scale from 1 'no risk at all' to 7 'extremely high risk', how large would you rate the risk that someone unauthorized will get access to your private data when you use this service". Internet privacy concerns regarding data collection are measured with items adapted from the corresponding sub-scale of Hong and Thong's (2013) to be rated on a 7-point scale from 1 'strongly disagree' to 7 'strongly agree': "It often bothers me when commercial apps or websites ask me for personal information"; "When commercial apps or websites ask me for personal information, I always think twice before providing it."; and "I am concerned that commercial apps or websites are collecting too much personal information about me.". Control questions at the end of the questionnaire confirm a sufficient recall of scenario characteristics among respondents.

Study 1

Study 1 employs a sample of Amazon MTurk respondents in the US and Canada and manipulates both service level and the nature of the BCES provider to establish the effects of these two factors. It also serves as a preliminary test of H_2 and, in the open-ended answers, tests for the amount of privacy concerns raised actively and in an unsolicited manner by consumers in the general population.

Study 2

Study 2 uses a sample of male and female undergraduate students at a large Canadian university to manipulate the service level and the nature of provider to test H_1 to H_4.

Study 3

Study 3 focuses on BCES offered by startups and manipulates the service level provided. In a student sample at a large Canadian university we test H_1 and H_3.

We analyze each sample with multilevel regression models with random intercepts to account for correlated errors of two scenarios evaluated by the same respondent. We control for category usage, gender, age, prior familiarity with Blockchain technology, country of residence (Study 1) and international student status (Studies 2 and 3). All continuous variables are mean-centered and binary control variables are effect-coded, to minimize collinearity and ensure parameters to be estimated at sample means.

RESULTS AND DISCUSSION

Preliminary analyses provide support for hypotheses H_1 to H_3 and marginal support for hypothesis H_4. Final results will be presented at the workshop and discussed in their theoretical and managerial implications with a special focus on HCI.

REFERENCES

1. Bouveret, A. and Haksar, V. (2018) What Are Cryptocurrencies? A potential new form of money offers benefits while posing risks, *Finance & Development*, 55, 26–27.
2. Chang, H.H. and Chen, S. W. (2008) The Impact of Online Store Environment Cues on Purchase Intention: Trust and Perceived Risk as a Mediator, *Online Information Review*, 6, 818-841.
3. Clohessy, T., Acton, T., and Rogers, N. (2019) Blockchain Adoption: Technological, Organisational and Environmental Considerations In: *Business Transformation through Blockchain*, H. Treiblmaier and R. Beck (eds.) pp. 47–76. Palgrave Macmillan, Cham: Switzerland.
4. del Castillo, M. (2019) Binance CEO 'CZ' Reports $40 Million Bitcoin Hack, Forbes.Com, N.PAG-N.PAG, https://www.forbes.com/sites/michaeldelcastillo/2019/05/07/binance-ceo-cz-reports-40-million-bitcoin-hack/#2fea90866c3f, accessed 2 September 2019.
5. Ertemel, A.V. (2018) Implications of Blockchain Technology on Marketing, *Journal of International Trade, Logistics and Law*, 4, 35–44.
6. Feigenbaum, J. (2019) Encryption and surveillance *Communications of the ACM*, 62, 27–29. doi:10.1145/3319079
7. Feng, Q., He, D., Zeadally, S., Khan, M. K., and Kumar, N. (2019) A survey on privacy protection in blockchain system, *Journal of Network & Computer Applications*, 126, 45–58. doi:10.1016/j.jnca.2018.10.020
8. Ghose, A. (2018) What Blockchain Could Mean for Marketing, *Harvard Business Review*, 93, 3, 19-23.
9. Hong, W. and Thong, J. (2013) Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies, *MIS Quarterly*, 37, 1, 275–298.
10. Hughes, A., Park, A., Kietzmann, J., and Archer-Brown, C. (2019) Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms, *Business Horizons*, 62, 273–281. doi:10.1016/j.bushor.2019.01.002
11. Lemay, D. J., Doleck, T. and Bazelais, P. (2017) "Passion and concern for privacy" as factors affecting snapchat use: A situated perspective on technology acceptance *Computers in Human Behavior*, 75, 264–271.
12. Mamais, S. S. and Theodorakopoulos, G. (2017) Behavioural Verification: Preventing Report Fraud in Decentralized Advert Distribution Systems, *Future Internet*, 9, 88, 1- 23.
13. Meiklejohn, S., Pomarole, M., Jordan, G., Levcheko, K., McCoy, D., Voelker, G. M. and Savage, S. (2016) A fistful of Bitcoins: Characterizing payments among men with no names, *Communications of the ACM*, 59, 86–93. doi:10.1145/2896384
14. Morgan-Thomas, and Veloutsou (2013) Beyond technology acceptance: Brand relationships and online brand experience, *Journal of Business Research*, 66, 1, 21-27.
15. Miltgen, C. L., Popovič, A. and Oliveira, T. (2013) Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context, *Decision Support Systems*, 56, 1, 103–114.
16. Önder, I. and Treiblmaier, H. (2018) Blockchain and tourism: Three research propositions, *Annals of Tourism Research*, 72, C, 180–182. doi:10.1016/j.annals.2018.03.005
17. Rui Zhang, Rui Xue, and Ling Liu (2019) Security and privacy on Blockchain, *ACM Computing Surveys*, 52, 1–34. doi:10.1145/3316481
18. Sedgwick, K. (2019, March 6) A Forensic Analysis of Blockchain Surveillance Companies Bitcoin News. Retrieved from https://news.bitcoin.com/a-forensic-analysis-of-blockchain-surveillance-companies/, accessed 2 September 2019.
19. Strebinger, A. and Treiblmaier, H. (2004) E-Adequate Branding: Building Offline and Online Brand Structure within a Polygon of Interdependent Forces, *Electronic Markets*, 14, 1, 153–164.

20. Subramanian, H. (2018) Decentralized Blockchain-based electronic marketplaces, *Communications of the ACM*, 61, 78–84.

21. Tan, X., Li, Q., Kim, Y. and Hsu, J. (2012) Impact of privacy concern in social networking web sites, *Internet Research; Bradford*, 22, 2, 211–233.

22. Tapscott, D. and Tapscott, A. (2017) How Blockchain Will Change Organizations *MIT Sloan Management Review,* 58, 2, 10–13.

23. Treiblmaier, H. and Beck, R. (2019a) *Business Transformation through Blockchain - Volume I,* Palgrave Macmillan, Cham, Switzerland.

24. Treiblmaier, H. and Beck, R. (2019b) *Business Transformation through Blockchain - Volume II*. Palgrave Macmillan, Cham, Switzerland.

25. Treiblmaier, H. (2019) Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies *Frontiers in Blockchain*, 2, 1–15. doi:10.3389/fbloc.2019.00003

26. Vigna, P. (2016) Fund based on digital currency Ethereum to wind down after alleged hack, Wall Street Journal (Online), https://www.wsj.com/articles/investment-fund-based-on-digital-currency-to-wind-down-after-alleged-hack-1466175033, accessed 1 September 2019.

27. Wolfond, G. (2017) A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors *Technology Innovation Management Review,* **7**, 1, 35–40.

28. Zhou, T. (2011) The impact of privacy concern on user adoption of location-based services *Industrial Management & Data Systems; Wembley*, 111, 212–226.