5-2-2023

BUSINESS REPUTATION SYSTEMS BASED ON BLOCKCHAIN TECHNOLOGY—A RISKY ADVANCE

Simon Hemmrich
Paderborn University, simon.hemmrich@upb.de

BUSINESS REPUTATION SYSTEMS BASED ON BLOCKCHAIN TECHNOLOGY—A RISKY ADVANCE

Research in Progress

Simon Hemmrich, Paderborn University, Paderborn, Germany, simon.hemmrich@upb.de.

Abstract

Reputation is indispensable for online business since it supports customers in their buying decisions and allows sellers to justify premium prices. While IS research has investigated reputation systems mainly as review systems on online platforms for business-to-consumer (B2C) transactions, no proper solutions have been developed for business-to-business (B2B) transactions yet. We use blockchain technology to propose a new class of reputation systems that apply ratings as voluntary bonus payments: Before a transaction is performed, customers commit to pay a bonus that is granted if a service provider has performed a service properly. As opposed to rival reputation systems that build on cumulated ratings or reviews, our system enables monetized reputation mechanisms that are inextricably linked with online transactions. We expect this system class to provide more trustworthy ratings, which might reduce agency costs and serve quality providers to establish a reputation towards new customers, building on second-order trust.

Keywords: Trust, Risk, Reputation System, Blockchain Technology, Business Reputation System.

1 Introduction

Online business requires buyers to trust that sellers will deliver a product or service as promised. However, buyers have incomplete information about the seller's capabilities and are exposed to the risk of not being satisfied as expected. A way to reduce this uncertainty is to establish trust (Luhmann, 2017) or reputation (Jøsang et al., 2007), increasing the buyer's confidence in a buying decision (Sullivan & Kim, 2018). Trust is a social construct and refers to "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al., 1995, 712). Reputation is an observable public opinion about an entity standing out from a group (Jøsang et al., 2007). It can be established with reputation systems that are information systems (IS).

Reputation systems reliably collect, store, and distribute information about an entity's past behavior (Cai & Zhu, 2016; Resnick et al., 2000). An entity might refer to a person, a group, or an organization. Reputation systems purvey reputation to provide objectified measures to assess trustworthiness subjectively (Jøsang et al., 2007; Jøsang, 2016), particularly to select trustworthy entities for buying decisions based on ratings from unknown agents (Resnick & Zeckhauser, 2002). Thus, reputation systems include ratings or reviews to inform third parties. Review systems feature plain text reviews and other metrics, while in rating systems, a product or service is rated typically, e.g., with a star rating. Both types are often used in a B2C context to indicate a seller's reputation (Gutt et al., 2019; Moreno & Terwiesch, 2014). Well-known examples that integrate both types are amazon.com and yelp.com.

Reputation has been proven to play an important role in business deals, supporting buying decisions and allowing sellers to achieve higher prices (Ba & Pavlou, 2002; Moreno & Terwiesch, 2014). Many value propositions in a B2C context are rated every day, including products, accommodations, shares, rideshares, mini-jobs, and more. However, although these systems are designed to reflect reputation and

establish trust, they are also infused with "spam, tampered ratings, and reviews, and paid reviews" (Subramanian, 2018, p. 81), since ratings are disconnected from the actual transaction.

Surprisingly, no global reputation system is available for companies to rate each other's products or services on a daily basis. Since millions of transactions are performed among companies every day using digital technologies, a profound basis for rating other companies' performance would be available. However, very few efforts have been made to design such systems (Dikow et al., 2015; Gutt et al., 2019), even though "creating a reliable, trustworthy distributed record system, or ledger, may be fundamental to how we organize interpersonal and inter-organizational relationships" (Beck et al., 2017, p. 381). Reputation systems help to solve the famous lemon market problem (Thierer et al., 2016), where asymmetric information between providers and customers leads to an adverse selection of bad products while driving good products out of the market (Akerlof, 1970).

Blockchain technology is discussed to deliver a missing link to design better and robust reputation systems (Cai & Zhu, 2016; Catalini & Gans, 2016; Möhlmann et al., 2019). Blockchain technology is known to establish trust between economic actors without the need to install a trustworthy intermediary. A blockchain is built on a distributed peer-to-peer network to provide a reliable, public, and tamper-proof infrastructure to conduct trustworthy and secure transactions (Nakamoto, 2008). This technology defines new ways to trust each other, prompting IS research to revisit trust as a construct (Beck et al., 2016; Ostern, 2018). Related research views this technology as a trust-free transaction system (Beck et al., 2016) or a trusted code (Simser, 2015). Research on blockchain-based reputation systems currently focuses on designing algorithmically secure and anonymous systems (e.g., Bag et al., 2018; Bazin et al., 2017). However, purely technological approaches struggle to induce reliable data on-chain from the outside world (Greenspan, 2016), disregarding off-chain reputation mechanisms.

We posit that reputation is a subjective phenomenon that builds on social relations, so off-chain trust mechanisms must be considered alongside technological mechanisms. However, until now, the trust perspective on blockchain technology is rarely addressed in top IS journals (Ostern, 2018), although IS research can explain how to establish trust with this technology (Risius & Spohrer, 2017; Seidel, 2018). While there have been calls for finding design mechanisms to build reliable blockchain-based reputation systems (Voshmgir & Zargham, 2020), an unresolved challenge is to enable individualized reputation and design proper incentive mechanisms (Pereira et al., 2019). Thus, we derive the research question: How can we use the trust concept for designing business reputation systems?

Therefore, we set out to revisit the trust construct and explain how the closely related concept of risk can be combined with blockchain-secured transactions to establish trust in B2B transactions. Our approach aims to represent trust relations backed with safeguards to help others to trust. Based on our initial findings, we provide two core contributions to this research-in-progress paper. First, we review and clarify the role of trust concerning blockchain technology. Second, we introduce the idea of leveraging a risky advance as a trust signal by a service provider offering a price discount while getting paid with voluntary bonuses, thereby demonstrating its capability and building a reputation. This idea is innovative since it breaks with established approaches to review or rate a seller retrospectively after transactions have been concluded. Monetary payments as ratings have three advantages. They allow us as researchers to conceptualize a system with a tangible risky advance representing one-sided trust relations. The amount of payments allows us to differentiate the significance of ratings as a parameter. The economic value of ratings is likely to increase the expressiveness of positive ratings since they cost money and might mitigate reciprocity issues.

In Section 2, we review the core concepts of trust, risk, and reputation, along with their role in existing reputation systems, before reviewing key properties of blockchain technology. We summarize and justify our research method in Section 3. In Section 4, we sketch out the idea for designing a blockchain-based B2B reputation system using the reputation mechanism of a risky advance that helps to ease trust between unknown business agents. Section 5 discusses the research contribution and concludes the paper, sketching the path ahead for a new class of reputation systems.

2 Related Research

2.1 Trust and Risk, System Trust, and Reputation

Trust is a multidimensional social construct studied extensively in the social context. It refers to various aspects of cognition, emotion, and behavior. Trust is highly subjective and varies depending on the purpose and context. It is indispensable for social interactions and reduces decision uncertainty. As a social lubricant, trust also enables fluid business exchange (Arrow, 1974; Sun, 2010).

In general, trust is an expectation about the actions to be performed by others—unlike calculus, and it starts before it is possible to monitor the actions of another actor (Williamson, 1993). As a priori concept, trust always comes with the risk that trust is unwarranted (Luhmann, 2017). It goes hand in hand with a voluntary willingness to take a risk, to lose something that appears valuable, even if a trustor does not expect to be disappointed (Deutsch, 1958; Mayer et al., 1995; Schoorman et al., 2007). Thus, there must be something at stake for trust to be built (Kee & Knox, 1970; Schoorman et al., 2007), indicating a constitutive relation between risk and trust (Chetty et al., 2021; Siegrist, 2021). When one makes a voluntary risky advance in a certain matter, it eases giving trust of the other party particularly (Gambetta, 1988; Luhmann, 2017).

System trust is decisive in reputation systems (Pennington et al., 2003). It is independent of a person's risk tendency or motives (Shapiro, 1987). As a form of distributed trust, it emerges in social systems and is based on explicit and organized control mechanisms, according to concrete requirements. These concrete requirements include safeguards built into the system to preserve the fragility of trust by sanctioning adverse behavior (Luhmann, 2017). In this way, a reputation system works as a collaborative sanction system that discourages untrustworthy behavior (Jøsang et al., 2007).

Trust is closely related to reputation. It is a positive, cognitive assessment by an individual towards another individual or entity, while reputation relates to a group's positive, distributed opinion (Bromley, 2001; Jøsang et al., 2007). Like trust, reputation is contextual, valuable, takes time to build, and is destroyed quickly (Dasgupta, 1988). Reputation occurs only compared to other potential trustees and can help foster trusting a specific trustee. When there is not enough information on whom to trust, peers that have already built trust are consulted—even if they are strangers—as long as they are in a similar position as the trust seeker. Demonstrating to have trusting customers representing a reputation can cause new, yet uncertain customers to trust (Moreno & Terwiesch, 2014).

Trusting in fellow customers who, themselves, trust a provider creates a transitive relation of trust. Trust transitivity states that trusting a third person depends mainly on what extent a referral is trusted (Jøsang et al., 2007; Jøsang, 2016) (Figure 1). First-order trust refers to trusting a recipient directly, while reputation is a form of second-order trust derived from observing peers' first-order trust.

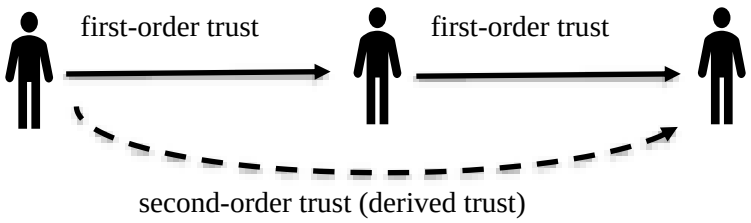

Figure 1. Trust transitivity principle (modified from Jøsang et al. 2007).

2.2 Trust and Risk Inscribed in Information Systems

Early research in IS investigates reputation in game-theoretical settings, splitting up into research on reputation systems to model trustworthiness between (computational) network nodes and research to assess the trustworthiness of sellers/service providers in e-commerce, e.g., through review systems.

Trust and reputation have been ascribed to network nodes (e.g., computer nodes, companies) as well as to things (e.g., vehicles), departing from their original conceptualization as emotional or cognitive

concepts. Since trust is inherently based on cognitive processes, modeling trust has no solid validation point in the computational context. Still, modeling trust in these systems has its raison d'être for designing reliable and secure IS (Jøsang, 2016). Computational trust—a quantity or score— refers to an online node's technical capabilities and network contribution from calculated propagated ratings (Jøsang et al., 2007). See Bellini et al. (2020) for a comprehensive view of current reputation systems.
For e-commerce, Jøsang et al. (2007) recognize risk as an inherent characteristic of reputation systems, distinguishing classes of trust according to the risk context. Risk includes, for instance, the risk of not making a good buying decision (decision trust), not being satisfied with a service or product (provision trust), not being part of an honest system (system trust), having no sufficient control mechanisms (reliable trust), and the risk to select false identities (identity trust). However, the concept of risk is often considered a sideline phenomenon in reputation systems (F. Li et al., 2012), even provided that conceptualizing risk shifts the underlying trust mechanism in reputation systems drastically (Litos & Zindros, 2017). For computational reputation networks, risk conceptions are often considered implicitly as a computational network score. However, this also has the disadvantage that reputation is not specifically but globally condensed, which contradicts the social view of trust as an individual construct. Integrating risk in rating processes is hardly discussed in online marketplaces (e.g., Amazon.com or eBay.com) or other business reputation systems. This faint consideration of risk in reputation mechanism might be a reason for false reviews, fraud, and customers' reluctance to trust ratings provided on online marketplaces since a seller and buyers have nothing to be risked in the rating process. Therefore, we conceptualize a reputation system with a risky advance to strengthen buyers' ratings, and make it at the same time easier for trustworthy sellers to win over new customers.

2.3 Blockchain Technology as an Enabler of Reliable Trust

A blockchain is a distributed ledger recording digital transactions between nodes in a network securely. Transactions are hashed, stored in blocks, and appended to a previous block, establishing an ever-growing chain of blocks, in which transactions can hardly be changed (Buterin, 2014). Every node holds a copy of the current state of the blockchain, representing an immutable ledger that is stored in the distributed network (Nakamoto, 2008). Transactions are transparent in the network, and parties can verify them easily. Based on this, smart contracts can be committed on a blockchain, providing a reliable basis for automated business exchange (Buterin, 2014). Blockchains shift trust away from the contractor to the entire blockchain network if the network and the smart contracts are deemed reliable (Kim, 2020; X. Li et al., 2008; Seidel, 2018). A blockchain can help foster trust, as it has the following features:

- *Immutability* refers to reliable transactions secured as (relative) tamper-proof records in a blockchain. Parties can verify executed transactions themselves, eliminating the need for a central authority to validate transactions. In a blockchain-based reputation system, ratings can be stored reliably, and no single actor can change, nor disavow a rating (Cai & Zhu, 2016).
- *Distributed trust* in a blockchain network (Seidel, 2018) is a form of system trust. System trust is established with a series of control mechanisms, comprising validation mechanisms in the network to approve transactions, so that reputation ratings (as transactions) can be verified.
- *Decentralization* lowers an intermediary's ability to restrict and control activities in a system (Filippi, 2016). A decentralized blockchain network with many independent validators makes most attack scenarios virtually impossible. Manipulating blockchain-secured ratings of transactions is highly unlikely.
- *Transparency* relates to the visibility of transactions, including transaction content, limited to protecting users' privacy. Privacy also allows pseudo-anonymity so that users can decide with whom to share private data. For reputation systems, parties can apply different pseudonyms that cannot be linked, signing a transaction with different personal keys (Filippi, 2016).

These features imply that contractual agreements cannot be changed without the approval of the counterparty, reducing the need to monitor or check the contractors' actions. In this way, a blockchain can reduce agency costs by providing a basis of reliable trust for business exchange (Murray et al., 2019) and prevent strategic lying about ratings. Similarly, rating agreements can be secured on a blockchain.

3 Method

In this research-in-progress paper, we conceptualize a reputation system for the B2B context. Our idea is based on theoretical literature on trust. Implementing a risky advance mechanism in blockchain-secured transactions, which serve as an immutable, trusted, decentralized, and transparent ledger can help to build second-order trust represented as reputation.

Conceptual research is a non-empirical research method (Mora et al., 2008) for developing a theory based on reflecting on existing theoretical concepts. This paper's theoretical concepts comprise different types of trust and risk. Based on these concepts and core properties of blockchain technology, we conceptualize how a risky advance can be implemented in an IS to ease decision trust in B2B settings. Additionally, we implement control to safeguard the risky advance of a service provider.

The conceptual findings build the first steps of a more comprehensive design science research project (Peffers et al., 2008), in which we plan to build and evaluate a blockchain-based reputation system that instantiates the findings presented in this paper. For this endeavor, the theoretical concepts discussed here will be used as kernel theories to develop, implement, and evaluate an innovative IS artifact (Kuechler & Vaishnavi, 2008). We use our theoretical perspective on trust and known problems in related reputation systems to build design principles for implementing a software prototype. Other researchers can build on these design principles and integrate risk (and thus trust) in the rating process of sellers.

4 Conceptualizing Blockchain-Based B2B Reputation Systems

4.1 Requirements and Design Principles

Related literature summarizes six main problems related to current reputation systems (Bellini et al., 2020; Jøsang et al., 2007): (1) low incentive for evaluation, (2) positive and reciprocal evaluations, (3) too many ratings (ballot-stuffing), (4) change of identity (whitewashing), (5) unfair valuations, and (6) discrimination (bad-mouthing). Revising how trust as a construct works (observation, selection, and risk assignment in a systemic context) (Luhmann, 1995, 2017), we build on these problems to identify requirements and design principles (Gregor et al., 2020) to design a blockchain-based business reputation system (Table 1).

	Requirements	**Design Principles**
a)	Business relationships	A reputation system should represent the true socioeconomic relationship of the transacting parties.
b)	Economic commitment	A reputation system should give evidence of the economic commitment between the transacting parties.
c)	Information contextualization	A reputation system should provide non-cumulated information and allow contextual information to be filtered and selected.
d)	Performance differentiation	A reputation system should allow for portraying performance differentiation among service providers.
e)	Linkable services	A reputation system should allow linking different service objects.
f)	Selection of ratings	A reputation system should allow a buyer to select which ratings are forwarded.
g)	Open system	A reputation system should be open to new participants.
h)	Raters' fairness	A reputation system should allow responding to a rater's bad rating.
i)	Systemic fairness	A reputation system should support a system equilibrium of fair ratings.
j)	Peer-to-peer system	A reputation system should be based on a distributed system, avoiding a single powerful gatekeeper that can influence the ratings.

Table 1. Requirements and Design Principles for a Business Reputation Systems.

4.2 Concept

We investigate reputation systems to establish trust based on transactions between business parties, while we do not consider reputation systems on the blockchain validation layer itself. We will now briefly explain how the idea works, in general, before building on the identified design principles. We propose establishing bonus payments between the transacting parties, enabling a service customer SC(x) to pay a part of the liabilities only if they are satisfied with the service delivered by a service provider SP. With this risky advance, we integrate risk in the transaction, since a SP risks a loss of profit by not receiving the bonus share; but also risks reputation, since the transaction can be visible to others. In this way, we consider what we learned about trust in theory, which is that trust and, thus reputation, can be created more effectively by exposing oneself to being vulnerable (Mayer et al., 1995). In doing so, SP also raises the trust expectation of a SC(x) to fulfill a service as promised, encouraging prospective customers' SC(p) decisions to do business with this SP. If not satisfied, a SC(x) can decide to pay only a basic payment (trans(y)) to the SP, but no bonus payment (trans(x)). If satisfied, the SC(x) might pay trans(x) to acknowledge proper service provision (Figure 2).

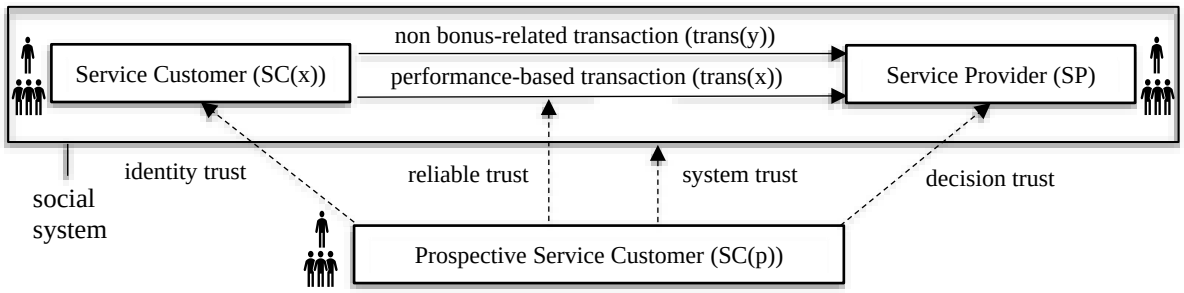

Figure 2. Trust in a performance-based reputation system.

The payment transactions are visible for other SC(p)s, who use the payment history of a SP as a basis to decide if they want to transact with this SP. The SC(p) will interpret the received trans(x) (in relation to trans(y)) as a rating of the SP's past performance. The SC(p) can compare a requested service with (similar) services rated. We can expect that the willingness of SC(p) to conduct business with SP would increase when the SP receives trans(x) from different SC(x) on a regular basis since this points to several satisfied SC(x). Vice versa, a SP can demonstrate receiving trans(x), gaining a trust advantage over competing SPs that received fewer transactions or lower bonuses. The SP will unlikely make a risky advance and enter into a business with a SC(x) that pays bonuses infrequently or whom he does not trust. Therefore we will introduce a safeguard to indicate exploitive SC(x) (see *h); i)*). Observing the transaction history, a SP can assess the risk of not receiving a trans(x) from a SC(x), which prevents him from engaging with exploitive SC(x)s.

Based on the information provided by SC(x), a SC(p) can decide to engage with a SP. Therefore, a SC(p) needs to trust in the SC(x)'s identity (identity trust), in the immutability of the transaction (reliable trust), and that the SC(x) and SP do not conspire (system trust), before trusting a SP (decision trust). Identity trust can be achieved by verifying identities that are deemed trustworthy; reliable trust is obtained with an immutable ledger. System trust relies on establishing systemic mechanisms rooted in business parties' economic self-interest. We posit that our system needs to be built on the following design principles:

a) Business relationship: Each transaction is recorded on a blockchain, providing a full picture of reputation. The lack of an incentive to elicit ratings (Neumann & Gutt, 2019) is fixed by deriving reputation from every on-chain transaction. Only metadata is public, while transaction details are hidden.

b) Economic Commitment: The parties establish a smart contract that specifies the bonus payments and is made visible to others. This clear economic commitment is quantified with the payment value and the

money at risk for a SP. The smart contract also enables the integration of a counter-rating mechanism for ratings perceived as unjustified, controlling who can give a counter-rating (see *h)*).

c) Information contextualization: Blockchain data can be filtered to identify services fitting a SC(p)'s purchase intent. The SC(p) selects relevant metadata according to a service description supplied in a smart contract and may apply additional evaluation metrics. Importantly, the selection choice of SC(p) includes that the raters' identity (SC(x)) is known or deemed trustworthy, based on verifiable ratings.

d) Performance differentiation: Services are described in a smart contract to indicate different value propositions. In particular, the trans(x) payment amount can be contracted on different levels, depending on how much risk a SP is willing to take for building a reputation.

e) Linkable services: A SP can create one or more seller identities, representing various service categories (Blömer et al., 2018; Zhai et al., 2016). Positive ratings of a service linked to an address/identity can promote customers' trust in the corresponding service provider's service.

f) Selection of ratings: A SC(x) is able to decide with whom to share ratings and not to disclose sensitive information to a competitor. This can be achieved with privacy-preserving techniques to hide the exact transaction amounts (Hemmrich et al., 2023). Equally, the SC(p) decides which rating to pick up to prevent being tricked by a fraudulent SC(x) or SP. Viewing a transparent transaction history, a SC(p) can learn over time which identities are trustworthy. After a sufficient information basis exists, SC(p) might place trust in specialized intermediaries to filter for honest addresses that fit his own assessment.

g) Open system: In a public blockchain network, parties can always join and leave the reputation system. Private spaces might be set up to exchange information about services conducted between SC(x) and SP to inform a SC(p). A SC(p) might pay the SC(x) for additional information to achieve an information advantage (e.g., for knowing SC(x)s true identity, and service details) to reduce the risk of engaging with a bad SP. A SC(x) can prove to have this information without revealing it.

h) Raters fairness: To overcome the problem that a SC(x) exploits the risky advance offered by SP, we propose a counter-rating mechanism. When a SC(x) does not pay a trans(x), the SP receives a one-time certificate to counter-rate the SC(x). This certificate allows a SP to rate to what extent the SP considered the omission of a trans(x) rating justified. For this counter-rating, a star-based rating might be used, revealing more information about the exchange relationship for another observing SP to decide whether to offer a risky advance for a particular SC(p).

i) Systemic fairness: Even if the quality of a service is good, an opportunistic SC(x) always has no interest in paying a trans(x). To establish fairness for counter-ratings, we propose a systems balance mechanism, making unpaid trans(x) visible depending on a threshold. Bad ratings get revealed if a SC(x) regularly decides not to pay trans(x). We suggest defining a threshold (e.g., 90%), at which counter-ratings become visible, as determined by the blockchain protocol rules shared in the network. This display incentives SC(x)s to pay trans(x) to at least 90% to SPs that offered a risky advance because else the exploitive behavior of a SC(x) becomes visible in the reputation system. Consequently, a SC(x) would try to stay below this threshold in order to continue doing business with SPs and being trusted. However, once revealed, every SP can view counter-ratings as revealing a SC(x) excessive exploiting behavior. Intuitively, SPs will pick SC(x)s, who can prove to pay trans(x) regularly to other SPs. This serves as a safeguard for SPs' risky advance, building trust (Luhmann, 2017). Avoidance of a SC(x) to pay too much (unobservable down to the threshold) and selective SP probably lead to a fair system equilibrium, filtering bad actors. Lastly, the threshold should correspond to the quality distribution in a market, at which counter-ratings would be visible to separate high-quality SPs from bad-quality SPs.

j) Peer-to-peer system: Blockchain technology builds on a distributed network that replaces the need for an intermediary, alleviating problems like data breaches, censorship, fraud, or high commission fees.

5 Discussion and Conclusion

We proposed an incentive scheme for reputation systems based on a risky advance of a service provider to his customer, thereby, using safeguards built on a blockchain to establish decision trust. We expect that this system can provide high-quality SPs with a competitive advantage over weaker-performing competitors, promoting good service quality. Compared with existing rival systems, our approach exhibits five main differences. First, ratings become an inherent part of business transactions, whereas current systems disconnect transactions from ratings. Second, ratings are carried out with payments, making the ratings quantifiable. Third, implementing the system with blockchain facilitates reliable trust, since ratings are immutable, transparent, trustworthy secure. Fourth, we propose a performance differentiation threshold to set incentives and sanction mechanisms aiming to establish a systemic equilibrium. Fifth, services can be rated quicker than writing a review, and service ratings can be differentiated regarding different services.

Blockchain technology can help to make these new reputation mechanisms feasible, paving the way for a new system class of reputation systems. Blockchain-based reputation systems provide control mechanisms to select and verify information service customers and service providers provide. Modifying ratings and strategic lying about ratings, e.g., when selling rating information, is impossible, presupposing a reliable blockchain network. Selecting trustworthy ratings is essential, but might be challenging initially, reflecting a cold-start problem. However, we assume that a marketplace for trading information about the trustworthiness of ratings will form since rating information has an economic value.

We acknowledge that this system might also be applied without blockchain technology. However, we posit that blockchain technology makes particular sense here because rating information is sensitive data, and centralized instances are always exposed to the risk of being compromised, among other disadvantages (Locher et al., 2018; Subramanian, 2018). However, please note that with this technology comes a limitation regarding conflict resolution. Some conflicts are hard to solve since data is stored immutably on the blockchain. However, we assume that a seller who allows himself to be rated accepts this and has a positive relationship with a rating service customer, expecting positive ratings.

Limiting attacks would also be important, and possible attack scenarios should be comprehensively researched to find eventual weak spots in the incentive scheme. Sending trust signals in the form of a risky advance, which is safeguarded through making bad behavior visible, can probably make a positive outcome for both, the service provider and the service customer, more likely. This is because customers want to get or stay in the position of getting trust signals (through the risky advance), while a service provider can expect positive ratings. However, a customer is able to give bad ratings, but, viewed from an overall system perspective, would do it as a rational actor (to stay in the system) only to a limited degree. If he decides otherwise, probably no seller would want to interact with him anymore. Parameters for disclosing bad rating customers need to be adjusted accordingly to the quality distribution in the market.

We assume that agency costs (e.g., monitoring a service provider's actions, searching for trustworthy service providers, and committing to trustworthy service customers) can be reduced with this system. We build this concept primarily for one-time business deals, making it more attractive to switch business partners. However, this concept might be adjusted to repeated business transactions extending its usefulness.

The multilateral design of incentives provided with this reputation system might result in a system equilibrium. Indeed, we see it as a potential solution to the famous lemon market problem (Akerlof, 1970). Developing such systems might be helpful to counteract adverse selection in business markets. A blockchain can help secure reputation systems, preventing business parties from compromising them. Thus, our blockchain-based system might level information asymmetries by establishing trust and reputation on a systems level promoting good service quality. Whether a system equilibrium is realized with our system needs to be explored in more profound settings, like game theory or lab experiments. This would contribute to complementing the design and evaluation of the proposed system.

6 References

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

Arrow, K. J. (1974). *The Limits of Organization*. *The Fels Lectures on Public Policy Analysis*. Norton.

Ba, S., & Pavlou, P. A. (2002). Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Quarterly*, *26*(3), 243–268. https://doi.org/10.2307/4132332

Bag, S., Azad, M. A., & Hao, F. (2018). A Privacy-Aware Decentralized and Personalized Reputation System. *Computers & Security*, *77*, 514–530. https://doi.org/10.1016/j.cose.2018.05.005

Bazin, R., Schaub, A., Hasan, O., & Brunie, L. (2017). Self-Reported Verifiable Reputation with Rater Privacy. In *Proceedings of the 11th IFIP International Conference on Trust Management (IFIPTM)*, Gothenburg.

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business & Information Systems Engineering*, *59*(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain - The Gateway to Trust-Free Cryptographic Transactions. In *Proceedings of the 24th European Conference on Information Systems (ECIS)*, Istanbul.

Bellini, E., Iraqi, Y., & Damiani, E. (2020). Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey. *IEEE Access*, *8*, 21127–21151. https://doi.org/10.1109/ACCESS.2020.2969820

Blömer, J., Eidens, F., & Juhnke, J. (2018). Practical, Anonymous, and Publicly Linkable Universally-Composable Reputation Systems. In *Cryptographers' Track at the RSA Conference 2018,* San Francisco.

Bromley, D. B. (2001). Relationships Between Personal and Corporate Reputation. *European Journal of Marketing*, *36*(3/4), 316–334.

Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. https://ethereum.org/en/whitepaper/

Cai, Y., & Zhu, D. (2016). Fraud Detections for Online Businesses: A Perspective from Blockchain Technology. *Financial Innovation*, *2*(1), 1–10. https://doi.org/10.1186/s40854-016-0039-4

Catalini, C., & Gans, J. S. (2016). *Some Simple Economics of the Blockchain* (Working Paper 22952). National Bureau of Economic Research. http://www.nber.org/papers/w22952 https://doi.org/10.3386/w22952

Chetty, R., Hofmeyr, A., Kincaid, H., & Monroe, B. (2021). The Trust Game Does Not (Only) Measure Trust: The Risk-Trust Confound Revisited. *Journal of Behavioral and Experimental Economics*, *90*, 101520. https://doi.org/10.1016/j.socec.2020.101520

Dasgupta, P. (1988). Trust as a Commodity. In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (pp. 49–72). Blackwell.

Deutsch, M. (1958). Trust and Suspicion. *Journal of Conflict Resolution*, *2*(4), 265–279.

Dikow, H., Hasan, O., Kosch, H., Brunie, L., & Sornin, R. (2015). Improving the Accuracy of Business-to-Business (B2B) Reputation Systems through Rater Expertise Prediction. *Computing*, *97*(1), 29–49. https://doi.org/10.1007/s00607-013-0345-x

Filippi, P. de (2016). The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies. *Journal of Peer Production*(7).

Gambetta, D. (1988). Can We Trust Trust? In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (pp. 213–237). Blackwell.

Greenspan, G. (2016). *Why Many Smart Contract Use Cases Are Simply Impossible*. https://www.coindesk.com/three-smart-contract-misconceptions

Gregor, S., Kruse, L. C., & Seidel, S. (2020). Research Perspectives: The Anatomy of a Design Principle. *Journal of the Association for Information Systems*, *21*(6), 1622–1652. https://doi.org/10.17705/1jais.00649

Gutt, D., Neumann, J., Zimmermann, S., Kundisch, D., & Chen, J. (2019). Design of Review Systems – A Strategic Instrument to Shape Online Reviewing Behavior and Economic Outcomes. *The Journal of Strategic Information Systems*, *28*(2), 104–117. https://doi.org/10.1016/j.jsis.2019.01.004

Hemmrich, S., Bobolz, J., Beverungen, D., & Blömer, J. (2023). Designing Business Reputation Ecosystems—A Method for Issuing and Trading Monetary Ratings on a Blockchain. In *Proceedings of the 31st European Conference on Information Systems (ECIS)*, Kristiansand.

Jøsang, A. (2016). *Subjective Logic: A Formalism for Reasoning Under Uncertainty*. Springer. https://doi.org/10.1007/978-3-319-42337-1

Jøsang, A., Ismail, R., & Boyd, C. (2007). A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, *43*(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019n

Kee, H. W., & Knox, R. E. (1970). Conceptual and Methodological Considerations in the Study of Trust and Suspicion. *Journal of Conflict Resolution*, *14*(3), 357–366. https://doi.org/10.1177/002200277001400307

Kim, J. W. (2020). Blockchain Technology and Its Applications: Case Studies. *Journal of System and Management Sciences*, *10*(1), 83–93. https://doi.org/10.33168/JSMS.2020.0106

Kuechler, B., & Vaishnavi, V. (2008). On Theory Development in Design Science Research: Anatomy of a Research Project. *European Journal of Information Systems*, *17*(5), 489–504. https://doi.org/10.1057/ejis.2008.40

Li, F., Pieńkowski, D., van Moorsel, A., & Smith, C. (2012). A Holistic Framework for Trust in Online Transactions. *International Journal of Management Reviews*, *14*(1), 85–103. https://doi.org/10.1111/j.1468-2370.2011.00311.x

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do We Trust New Technology? A Study of Initial Trust Formation with Organizational Information Systems. *The Journal of Strategic Information Systems*, *17*(1), 39–71. https://doi.org/10.1016/j.jsis.2008.01.001

Litos, O. S. T., & Zindros, D. (2017). Trust is Risk: A Decentralized Financial Trust Platform. In *21st International Conference on Financial Cryptography and Data Security (FC 2017)*, Sliema.

Locher, T., Obermeier, S., & Pignolet, Y. A. (2018). When can a Distributed Ledger Replace a Trusted Third Party? In *Proceedings of the 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. 1069–1077). IEEE.

Luhmann, N. (1995). *Social Systems*. Stanford Universitiy.

Luhmann, N. (2017). *Trust and Power* (C. Morgner & M. King, Trans.). Polity.

Mayer, R., Davis, J., & Schoorman, D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.2307/258792

Möhlmann, M., Teubner, T., & Graul, A. (2019). Leveraging Trust on Sharing Economy Platforms: Reputation Systems, Blockchain Technology and Cryptocurrencies. In R. Belk, G. M. Eckhardt, & F. Bardhi (Eds.), *Handbook of the Sharing Economy* (pp. 290–302). Elgar.

Mora, M., Gelman, O., Paradice, D., & Cervantes, F. (2008). The Case for Conceptual Research in Information Systems. In *Proceedings of the International Conference on Information Resources Management (CON-FIRM)*.

Moreno, A., & Terwiesch, C. (2014). Doing Business with Strangers: Reputation in Online Service Marketplaces. *Information Systems Research*, *25*(4), 865–886. https://doi.org/10.1287/isre.2014.0549

Murray, A., Kuban, S., Josefy, M., & Anderson, J. (2019). Contracting in the Smart Era: The Implications of Blockchain and Decentralized Autonomous Organizations for Contracting and Corporate Governance. *Academy of Management Perspectives.* Advance online publication. https://doi.org/10.5465/amp.2018.0066

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Neumann, J., & Gutt, D. (2019). Money Makes the Reviewer Go Round–Ambivalent Effects of Online Review Elicitation in B2B Markets. In *25th Americas Conference on Information Systems (AMCIS)*, Cancun.

Ostern, N. (2018). Do You Trust a Trust-Free Transaction? Toward a Trust Framework Model for Blockchain Technology. In *Proceedings of the International Conference on Information Systems (ICIS)*, San Francisco.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pennington, R., Wilcox, H. D., & Grover, V. (2003). The Role of System Trust in Business-To-Consumer Transactions. *Journal of Management Information Systems*, *20*(3), 197–226.

Pereira, J., Tavalaei, M. M., & Ozalp, H. (2019). Blockchain-Based Platforms: Decentralized Infrastructures and its Boundary Conditions. *Technological Forecasting & Social Change*, *146*, 94–102. https://doi.org/10.1016/j.techfore.2019.04.030

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation Systems. *Communications of the ACM*, *43*(12), 45–48.

Resnick, P., & Zeckhauser, R. (2002). Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. In M. R. Baye (Ed.), *The Economics of the Internet and E-Commerce* (11th ed., pp. 127–157). JAI.

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There. *Business & Information Systems Engineering*, *59*(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *The Academy of Management Review*, *32*(2), 344–354.

Seidel, M. D. L. (2018). Questioning Centralized Organizations in a Time of Distributed Trust. *Journal of Management Inquiry*, *27*(1), 40–44. https://doi.org/10.1177/1056492617734942

Shapiro, S. P. (1987). The Social Control of Impersonal Trust. *American Journal of Sociology*, *93*(3), 623–658. https://doi.org/10.1016/j.ijinfomgt.2017.12.008

Siegrist, M. (2021). Trust and Risk Perception: A Critical Review of the Literature. *Risk Analysis*, *41*(3), 480–490. https://doi.org/10.1111/risa.13325

Simser, J. (2015). Bitcoin and Modern Alchemy: In Code We Trust. *Journal of Financial Crime*, *22*(2), 156–169. https://doi.org/10.1108/JFC-11-2013-0067

Subramanian, H. (2018). Decentralized Blockchain-Based Electronic Marketplaces. *Communications of the ACM*, *61*(1), 78–84. https://doi.org/10.1145/3158333

Sullivan, Y. W., & Kim, D. J. (2018). Assessing the Effects of Consumers' Product Evaluations and Trust on Repurchase Intention in E-Commerce Environments. *International Journal of Information Management*, *39*, 199–219. https://doi.org/10.1016/j.ijinfomgt.2017.12.008

Sun, H. (2010). Sellers' Trust and Continued Use of Online Marketplaces. *Journal of the Association for Information Systems*, *11*(4), 182–211.

Thierer, A., Koopman, C., Hobson, A., & Kuiper, C. (2016). How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the Lemons Problem. *U. Miami L. Rev.*, *70*(3), 830–878.

Voshmgir, S., & Zargham, M. (2020). *Foundations of Cryptoeconomic Systems* (Working Paper Series) [, WU Vienna University, Vienna]. RIS.

Williamson, O. E. (1993). Calculativeness, Trust, and Economic Organization. *The Journal of Law and Economics*, *36*(1), 453–486. https://doi.org/10.1086/467284

Zhai, E., Wolinsky, D. I., Chen, R., Syta, E., Teng, C., & Ford, B. (2016). Anonrep: Towards Tracking-Resistant Anonymous Reputation. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI)* (pp. 583–596). USENIX.