DESIGNING BUSINESS REPUTATION ECOSYSTEMS— A METHOD FOR ISSUING AND TRADING MONETARY RATINGS ON A BLOCKCHAIN

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

Bobolz, Jan, University of Edinburgh, Edinburgh, UK, jan.bobolz@ed.ac.uk

Beverungen, Daniel, Paderborn University, Paderborn, GER, daniel.beverungen@upb.de

Blömer, Johannes, Paderborn University, Paderborn, GER, johannes.bloemer@upb.de

Abstract

Many market transactions are subject to information asymmetry about the delivered value proposition, causing transaction costs and adverse effects among buyers and sellers. Information systems (IS) research has investigated how review systems can reduce information asymmetry in business-to-consumer markets. However, these systems use textual data or star ratings that cannot be readily applied to business-to-business markets, are vulnerable to manipulation, and suffer from other conceptual shortcomings. Building on design science research, we conceptualize a new class of reputation systems based on using payments as monetary ratings for each transaction stored on a blockchain. We show that our system assures content confidentiality so buyers can share, sell, and aggregate their ratings selectively, establishing a reputation ecosystem. Our prescriptive insights advance the design of reputation systems and offer new paths to understanding how payments can be used as signals that reduce information asymmetry in B2B transactions.

Keywords: Buying decisions, business-to-business transactions, uncertainty, reputation system, blockchain.

1 Introduction

Business transactions presuppose buyers to trust that sellers will deliver a product or service as promised. However, before a transaction, buyers are often uncertain about a seller's ability and willingness to perform as expected (Truong, 2019). This uncertainty is particularly relevant for person-intensive, high-cost business services like consulting, recruitment, or individual software development (Cronin, Brady, and Hult, 2000; Lam et al., 2004). The uncertainty reflects an information asymmetry among buyers and sellers. Sellers know their abilities but often need to spend considerable effort to convince buyers to trust them, since new buyers cannot assess their quality in advance. Particularly for market transactions, buyers rely on publicly available market information and might still end up contracting low-quality sellers. This effect is known as the lemon market problem leading to adverse selection in a market, where high-quality offerings are pushed out of the market while low-quality offerings prevail (Akerlof, 1970).

Quality signals can contribute to leveling information asymmetries (Bauer et al., 2022). Among others, quality signals include brands, references, quality seals, or warranties. Reputation feedback is another quality signal that has the potential to solve the lemon market problem (Thierer et al., 2016). It is shared in reputation systems, which are information systems that systemically incentives and sanction trustworthy behavior and collect, distribute, and aggregate feedback (Resnick and Zeckhauser, 2002; Jøsang, 2016).

This work was partially supported by the German Research Foundation (DFG) within the Collaborative Research Centre On-The-Fly Computing (GZ: SFB 901/3) under the project number 160364472.

Setting the right economic incentives is crucial to make these systems work (Jurca and Faltings, 2009; Buechler et al., 2015), but if they do, reputation systems can provide better quality signals that correlate more with the underlying product quality when they are based on a blockchain (Bauer et al., 2022; Spychiger et al., 2022). Consistently, blockchain technology can be considered a breakthrough technology to design business reputation systems (Cai and D. Zhu, 2016; Pereira, Tavalaei, and Ozalp, 2019; Voshmgir and Zargham, 2020). With a blockchain-based reputation system, buyers reduce their risk of making bad buying decisions. High-quality sellers, on the other hand, can use these systems to signal the quality of their goods and services in the market, justify higher prices, gain new customers, and build a reputation (Ba and Pavlou, 2002; Moreno and Terwiesch, 2014).

Current IS research focuses on review systems—a sub-form of reputation systems—used frequently on commercial platforms such as Airbnb or Yelp. Review systems often use user-generated text and star ratings to allow customers to make better buying decisions, e.g., book a suitable vacation rental. Usually, all reviews are public and provided for free, providing immense value to platform owners while attracting additional customers due to the emergence of direct network effects. In business-to-business (B2B) markets, no comparable system is available due to a series of shortcomings: First, current systems suffer from profound limitations, e.g., rating fraud, insufficient incentives to provide honest ratings, and reliance on a central platform, among others (Subramanian, 2018; Jøsang, 2007). Second, sellers try to decrease transparency in B2B markets to differentiate their offerings from their competitors for dynamic pricing and capitalize on the value of sales (K. Zhu, 2002). Third, buyers are reluctant to share ratings about products or services publicly, drawing no advantage from it (Jurca and Faltings, 2003). Rivals might benefit from shared information, while some companies fear exposing their business data or revealing the quality of certain suppliers to competitors (K. Zhu, 2002).

In light of the potential benefits of such systems, related research has identified a strong need to design business reputation systems (Cai and D. Zhu, 2016; Catalini and Gans, 2016; Möhlmann, Teubner, and Graul, 2019; Dikow et al., 2015). Taking up these calls and in line with design science research (Hevner et al., 2004; Nunamaker, Chen, and Purdin, 1990); our research goal is to design a new method (March and Smith, 1995) that allows companies to share monetary-based ratings with other market participants selectively. The envisioned system enables buyers to 1) rate sellers with monetary payments for each business transaction, 2) selectively sell and buy ratings to identify high-quality sellers, and 3) make better buying decisions. Using monetary ratings might contribute to solving some of the shortcomings of reputation systems because monetary ratings reflect customers' value-in-use, encapsulate economic information, carry an inherent weight as a signal, allow portraying asymmetric risk relations (Hemmrich, 2023), are quantifiable and individually assessable, and are harder to fake due to their inherent monetary value. Our system enables buyers to sell rating information to other buyers, generating pay-ins that can offset their pay-offs associated with providing monetary ratings. Rating confidentiality is guaranteed by the built-in features of a blockchain. The method enables companies to hide, or share (and, thus, sell) their monetary-based ratings selectively with other market participants without having to disclose other details on their transactions. Selling ratings might provide an important incentive for buyers to share their ratings, while it allows sellers to build a reputation through receiving positive ratings. In regard to the conceptual weaknesses of rival systems used in B2C markets, we point out that trading monetary ratings can contribute to solving three major limitations. Fake ratings, lack of incentive to submit ratings and a controlling central instance. Also, our method can help to counteract other deficiencies, such as reciprocity issues and reputation inflation, without a need to rely on a trustworthy intermediary.

The paper is structured as follows. In Section 2, we discuss related research and briefly summarize the core principles of blockchain technology. In Section 3, we describe and justify our research method. In Section 4, we discuss deficiencies of current reputation systems primarily used in B2C markets. To remedy these deficiencies, we outline the design of a new type of reputation system, starting with a cryptographic method to hide and share ratings on a platform. This demonstration evidences that this artifact can be implemented in current blockchains. In Section 5, we discuss our contributions to theory and practice, before concluding the paper in Section 6.

2 Research background

2.1 Reputation systems

Focal points of research on reputation systems are examining and designing them (Dellarocas, 2005; Moreno and Terwiesch, 2014) and the related concepts of trust and markets (Jøsang, Ismail, and Boyd, 2007; Tadelis, 2016). However, IS-related research mainly discusses review systems (Gutt et al., 2019) or word-of-mouth systems (Cheung and Thadani, 2012). In computer science, related research proposed privacy-preserving techniques (Bazin et al., 2016; Blömer, Eidens, and Juhnke, 2018), which has also recently involved blockchain technology (Bellini, Iraqi, and Damiani, 2020; Camilo et al., 2020). Also, other works show how to secure the integrity of text reviews on a blockchain (Zulfiqar et al., 2021).

Related research has remained fragmented and has not developed reputation systems that can be used in B2B markets. While many papers motivate improvements that need to be made to current systems, e.g. (Dennis and Owen, 2015), monetary payments have not been considered as ratings, nor selling ratings to other stakeholders in a market. Still, designing reliable reputation mechanisms remains an open issue (Cai and D. Zhu, 2016; Tumasjan and Beutel, 2019; Voshmgir and Zargham, 2020).

First steps have been made on a path to establish monetary ratings in reputation systems. For instance, (DeFigueiredo and Barr, 2005) propose a reputation system based on monetary security deposits that another party could withdraw, but as proof of trust, refrains from doing so. Similarly, (Litos and Zindros, 2017) equate trust with risk to conceptualize a decentralized platform, on which trust is quantified with a monetary deposit issued among peers. By depositing money, the risk (and, thus, trust) becomes visible in the network to assess a subjective indirect trust relation (Litos and Zindros, 2017). However, in these systems money does not serve as a rating, but is considered as a security deposit to represent indirect trust. Also, both approaches do not consider that raters might sell *their* rating information to others.

In multi-agent simulations, selling reputation information is discussed as an incentive for sharing reputation information. Selling reputation information makes the reputation mechanism incentive-compatible to report ratings trustfully (Jurca and Faltings, 2003). While money can be an incentive to provide ratings (Buechler et al., 2015), monetary benefits are currently often granted by the seller that is rated itself, so ratings are often biased in the seller's favor (Fradkin et al., 2015; Neumann and Gutt, 2019a). Switching the benefactor of paying the ratings from a seller to a neutral prospective buyer might resolve this dilemma.

2.2 Blockchain technology

A blockchain is a distributed ledger in which data references can be distributed and securely stored in a network. The network nodes take the role of a distributed third party, bound to the rules of consensus protocols. A consensus protocol ensures that nodes agree about the transactions stored in each block, building a blockchain. After reaching a consensus, the data recorded on the blockchain becomes immutable (Pilkington, 2016). Blockchains are commonly used to implement cryptocurrencies (Nakamoto, 2008). The distributed ledger is used to record currency transactions, where the immutability property ensures that currency cannot be double-spent. Modern privacy-preserving cryptocurrencies—e.g., (Ben-Sasson et al., 2014; Fuchsbauer, Orrù, and Seurin, 2019)—use cryptography to hide transaction data from the blockchain while preserving the desired properties of a cryptocurrency (i.e., coins can only be spent by their owner, coins can only be spent once, transactions are publicly verifiable). Blockchain eliminates the need for a central trust authority to validate transactions (Lustig and Nardi, 2015).

Blockchain technology enables distributed applications—such as a reputation system for business, providing an openly accessible public ledger without a central trust instance—based on two essential features:

- *Manipulation resistance*: Information stored on a blockchain is secure and cannot be changed. This property ensures that no entity can manipulate a rating.
- *Proof of information*: Using cryptographic techniques, users can prove to possess some information without having to reveal it. This property allows to control which rating is disclosed.

2.3 Limitations in current review systems

Although review systems have been researched for more than a decade, some weak spots remain:

1) Only a small proportion of transactions are rated at all, while generating meaningful ratings is time-consuming and costly. Ratings usually rely on voluntary feedback, but buyers have little incentive to share their experiences with others (Dellarocas, 2005; Resnick, Zeckhauser, et al., 2006), and giving ratings comes with an effort (Jurca and Faltings, 2009). Thus, most users do not submit feedback. Especially, dissatisfied users refrain from giving ratings (Dellarocas and Wood, 2008). Accordingly, poor performance, cases of misconduct, or exploited business relations are not recorded, paving the way for opportunistic behavior. To stimulate the generation of high-quality feedback, platform operators or sellers try to incentive buyers to submit feedback in exchange for discounts (Jurca, Garcin, et al., 2010). However, when sellers attract customers with coupons, vouchers, or other rewards, ratings are usually biased in the seller's favor (Neumann and Gutt, 2019a). Luring raters with rewards makes them (feel) committed to submitting a good rating so that negative ratings become unlikely (Neumann and Gutt, 2019b). However, precisely the potential risk of not being rated positively signifies the high value of reputation (Kreps and Wilson, 1982).

2) Ratings can be manipulated easily or submitted intentionally incorrectly. Online rating fraud is a well-documented problem in B2C markets and undermines trust in these markets (Ansari and Gupta, 2021; Dellarocas, 2005; He, Hollenbeck, and Proserpio, 2022; Hu, Liu, and Sambamurthy, 2011; Ivanova and Scholz, 2017). Buying intentionally wrongly submitted ratings (fake ratings) is cheap and often easy (He, Hollenbeck, and Proserpio, 2022). It impacts the perceived trustworthiness of ratings significantly and harms the trust in the entire market (He, Hollenbeck, and Proserpio, 2022; Wu et al., 2020). Since ratings strongly affect buying decisions, sellers are inclined to manipulate ratings. Fake ratings can also be used to discriminate against competing buyers purposefully (Cui, J. Li, and Zhang, 2020; Lappas, Sabnis, and Valkanas, 2016; Mayzlin, Dover, and Chevalier, 2014). Since unfair ratings and discriminating behavior may be hard to distinguish from personal taste, there is a risk of moral hazard that must be encountered with sophisticated reputation mechanisms (Dellarocas, 2000).

3) Reciprocity and fear of retaliation cause reputation inflation. Well-intentioned reciprocity or fear of retaliation distorts reputation mechanisms (Bolton, Greiner, and Ockenfels, 2013). Reciprocal feedback helps to record mutually beneficial transactions between parties, but it can also distort ratings' actual quality (Bolton, Greiner, and Ockenfels, 2013). Fear of retaliation prevents parties from giving bad ratings, even if they do receive poor quality, either because they fear getting negative feedback in return, or fear that other parties would refrain from doing further business with them (Bolton, Greiner, and Ockenfels, 2013; Dellarocas and Wood, 2008; Luca, 2017). Often, this fear leads to strong rating distortion, with ratings becoming overly positive (Bolton, Greiner, and Ockenfels, 2013; Ert, Fleischer, and Magen, 2016; Resnick and Zeckhauser, 2002). This phenomenon is called reputation inflation (Filippas, Horton, and Golden, 2018) and deprive ratings of a reasonable basis for differentiation (Zervas, Proserpio, and Byers, 2021).

4) The change and the creation of new identities enable a forged reputation. Creating new fake identities or changing the identity allows users to manipulate ratings (Dellarocas, 2003). Fake identities are always an issue in open systems without a central, trusted authority (Douceur, 2002). Having control over many fake identities enables one to generate fake ratings and thus promote reputation, submit unfair ratings, and discriminate against competitors (Douceur, 2002; Friedman and Resnick, 2001). Also, leaving the system after one transaction (free-riding) as soon as the initial reputation declines and creating another clean identity can be a problem.

5) Informational value gets lost when reputation information is condensed into a global score. Many reputation systems condense reputation into a single trust score eliminating multiple contexts (Hendrikx, Bubendorfer, and Chard, 2015). However, reputation is represented more accurately by social embeddedness (Durkheim, 1960; Granovetter, 1985). By aggregating reputation information, a great deal of relevant context for trust decisions is lost. Therefore, cumulative measures seem not appropriate, since they lack contextual information (Bolton, Katok, and Ockenfels, 2004). The context is vital since reputation is a subjective phenomenon and is created from context (Mui, Mohtashemi, and Halberstadt, 2002; ur Rehman et al., 2019). Reputation might differ according to the observers' subject of interest (Huang et al., 2014). Knowing the context, information can be processed in more detail (Hirshleifer and Teoh, 2003) and informational value improves significantly (Filippi, 2016; Nissenbaum, 2004; Pavlou and Dimoka, 2006). For instance, aggregating reputation on the level of an entity is helpful as an individual estimate of trustworthiness but does not yield objective information about a product. Trust mediators, like the Better Business Bureau that assess the trustworthiness of an identity, are helpful but do not provide differentiated product ratings. Experiments in the B2B context also support the need to compile ratings in a unique fashion (Bolton, Katok, and Ockenfels, 2004; Ekstrom, Bjornsson, and Nass, 2005) presupposing a set of raw data to build subjective trust decisions on.

6) Privacy and data are exploited by platform intermediaries. Reputation systems are often offered on digital marketplaces and operated by a (more or less) trusted intermediary that owns the platform. While intermediaries generally mitigate some of the problems mentioned above—e.g., prevent fake identities, ballot stuffing, or whitewashing—they can also be weak spots (Subramanian, 2018). Intermediaries open up attack vectors to manipulate or remove data and can be bribed, while they are increasingly suffering from fake ratings (Wan and Nakayama, 2014; He, Hollenbeck, and Proserpio, 2022). They might be vulnerable to data breaches or censorship, while they sometimes charge high fees (Catalini and Gans, 2016). Also, some intermediaries are inclined to exploit their customers' data in their self-interest, irrespective of customers' desire for data privacy (Filippi, 2016; Lyon, 2014; Soska et al., 2016; Zyskind, Nathan, and Pentland, 2015).

By describing these problems—mainly drawing from related research on review systems—it becomes clear that the challenges concerning reputation systems are multifaceted. Therefore, we decided to focus on three particularly severe problems: a) cheap fake ratings can be bought, which we address with a monetary weight of ratings that can be traded and distinguished from purchased and cheap ratings; b) little incentive to submit rating information (especially in the B2B context), which we address through the opportunity to sell rating information to other buyers; c) dependence on a central platform provider, which we address by using blockchain technology.

2.4 Positioning this work as to designing reputation ecosystems

The purpose of this paper is to elucidate how a reputation system can be designed for a B2B market, enabling companies to perform monetary ratings on their business transactions. The ratings are stored confidentially and immutably on top of a blockchain, while they can be sold to inform other market participants. The pay-ins generated from the sale could level or exceed the pay-out for conducting ratings. Against the backdrop of current definitions of reputation systems (Resnick and Zeckhauser, 2002), we refer to this system class as an *ecosystem* (Jacobides, Cennamo, and Gawer, 2018).

Ecosystems are characterized by entities that co-create value while building complex relations among them to exchange value (Hein et al., 2020; Yoo, Henfridsson, and Lyytinen, 2010). The rating information constitutes this value for companies (e.g. monetary-based ratings, or text reviews). For sellers by building a reputation in an ecosystem based on complex relations among different entities. For buyers getting quality signals and trading (information about) these quality signals. Entities can select and aggregate rating data according to their needs.

Thus, following Resnick and Zeckhauser, 2002, we define this type of system as a *reputation ecosystem* that collects, and distributes feedback and helps to determine the feedback's trustworthiness, whereby entities can observe and communicate selectively about each other's signals, e.g., about their payments as ratings and aggregate this information selectively. Intending this system to work in a B2B market, we speak of a *business reputation ecosystem*. These systems can be blockchain-based and might comprise monetary-based features and other metrics, but they may also comprise other data, such as text or star ratings (cf. Figure 1). In contrast, review systems are typically free of charge and display ratings publicly, relying on qualitative data.

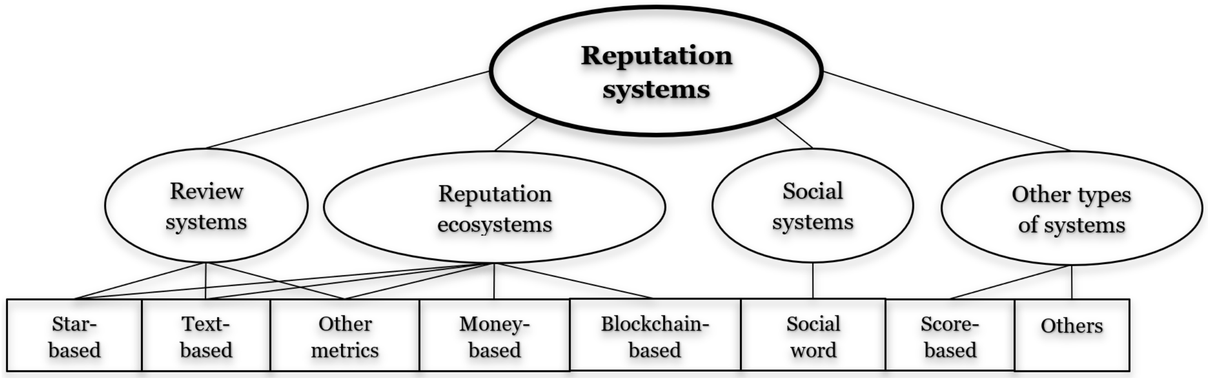
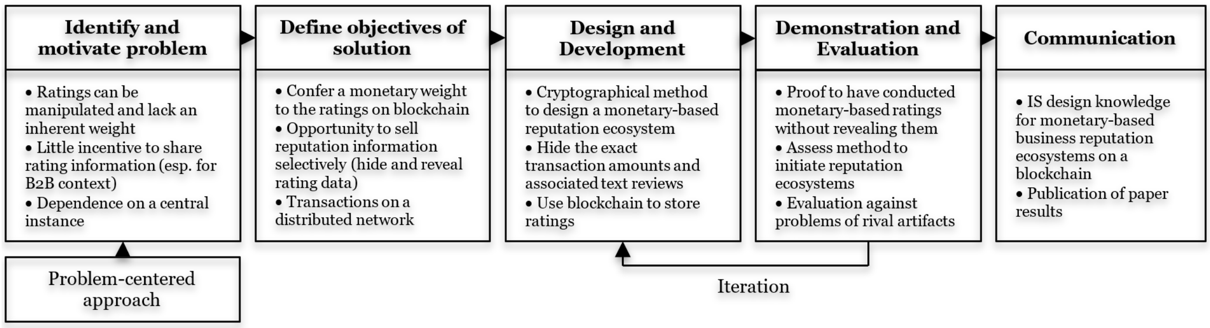


Figure 1. Reputation ecosystems as a particular class of reputation systems.

3 Research method

Sharing fair and honest ratings about a product or service in the business context is a yet "unsolved and important business problem" (Hevner et al., 2004, p. 82) and warrants a Design Science Research (DSR) approach (Nunamaker Jr et al., 2015). Generally, the DSR paradigm (Hevner et al., 2004; March and Smith, 1995; Nunamaker, Chen, and Purdin, 1990) seeks to identify relevant problems and build and evaluate meaningful artifacts to help to solve such problems (Gregor and Hevner, 2013; Lee, 2015). Establishing reputation feedback in B2B markets is important to mitigate information asymmetries, opposing the emergence of lemon markets (Akerlof, 1970; Thierer et al., 2016). Our method is a design science artifact (March and Smith, 1995) positioned as an improvement (Gregor and Hevner, 2013), since the solution maturity is low and the application domain maturity is high. Building on the design science research methodology (Peffers et al., 2008), we summarize our research method as follows (cf. Figure 2).

We took a problem-centered approach to identify and motivate the problem. Since no comparable reputa-


Identify and motivate problem

- Ratings can be manipulated and lack an inherent weight
- Little incentive to share rating information (esp. for B2B context)
- Dependence on a central instance

Problem-centered approach

Define objectives of solution

- Confer a monetary weight to the ratings on blockchain
- Opportunity to sell reputation information selectively (hide and reveal rating data)
- Transactions on a distributed network

Design and Development

- Cryptographical method to design a monetary-based reputation ecosystem
- Hide the exact transaction amounts and associated text reviews
- Use blockchain to store ratings

Demonstration and Evaluation

- Proof to have conducted monetary-based ratings without revealing them
- Assess method to initiate reputation ecosystems
- Evaluation against problems of rival artifacts

Iteration

Communication

- IS design knowledge for monetary-based business reputation ecosystems on a blockchain
- Publication of paper results

Figure 2. Overview of the research process, based on the DSR methodology (Peffers et al., 2008).

tion systems in business are described in research yet, we relate our concept mainly to the literature on rival artifacts in B2C markets, review systems. Three well-known limitations of these systems include fake ratings, missing incentives to submit honest ratings, and dependence on a platform provider. These limitations hinder current systems from being used in B2B markets to evaluate other companies' qualities, with which no transaction has taken place previously.

Our ultimate objective is to design a complete reputation system that can be used in a B2B market to establish payments as monetary ratings, establishing an ecosystem of trust among sellers and buyers. While buyers can trade their rating information with other buyers for money, sellers can document their ratings to establish a reputation and justify higher prices for their goods and services. Designing a profound incentive schema and elucidating users' acceptance are also important for establishing a prescriptive design theory (Jones and Gregor, 2007) for this new system class. While developing the full-scale system is, beyond the scope of this paper, we focus on designing a technically feasible method.

Buyers can use the method to hide and sell their rating information to other buyers. We build this method based on cryptographic commitments, privacy-preserving cryptocurrencies, and zero-knowledge proofs. Following the advice of (Vaishnavi, Kuechler, and Petter, 2017), we relate our method to no specific cryptocurrencies to make it applicable in different contexts. One can prove that ecosystems applying our method will work cryptographically securely. Consistently, we evaluate our method by providing cryptographic evidence for its correctness and security. This formal proof and logical reasoning represents the evaluation itself (Cleven, Gubler, and Hüner, 2009; Hevner et al., 2004; Sonneberg and vom Brocke, 2012; Venable, Pries-Heje, and Baskerville, 2016. To further evaluate the external validity of our method, we conceptually compare the system with other rival artifacts. The class of reputation ecosystems envisioned here provides core insights for managing and trading rating information in business networks that are subject to no or little trust. IS researchers and professionals can apply the resulting knowledge to guide design processes in more specific use cases (van Aken, 2004) or build on our results in other contexts.

4 Artifact description

4.1 Method overview and objectives of a solution

For designing a new class of business reputation ecosystems as another future artifact, we combine monetary-based ratings with the ability to share rating information without making them visible to others. Consider a *basic transaction* on a blockchain in which a buyer ("buyer 1") pays an amount v_{buy} to a seller ("seller 1") for a good or service, while seller 1 consents to being rated and allows buyer 1 to pass on the rating. Afterward, buyer 1 *rates* the quality positively in a second transaction (*rating transaction*) by paying an additional amount v_{rate} to seller 1 (Figure 3).

The ratio $v_{\text{ratio}} = v_{\text{rate}}/v_{\text{buy}}$ between the rating transaction v_{rate} and the basic transaction v_{buy} expresses buyer 1's satisfaction with the quality provided by seller 1. The higher v_{ratio}, the weightier the rating. For example, if buyer 1 is very satisfied, the rating transaction might be 10% of the buying price v_{buy}, i.e. $v_{\text{ratio}} = 0.1$. Vica versa, if buyer 1 pays nothing, i.e., $v_{\text{ratio}} = 0$, the rating reflects strong dissatisfaction.

Because ratings have an economic value (Wise and Morrison, 2000), and businesses are hesitant to share ratings with competitors, we design the system in a way that ratings remain *hidden*, enabling a buyer 1 to sell ratings only to selected peers (i.e., buyer 2). Buyer 1 can *choose* to whom to sell the rating, namely v_{ratio}, without a need to reveal v_{buy} or v_{rate}, hiding the exact payment amounts. Buyer 1 can also prove that the basic transaction amount v_{buy} passes some non-triviality threshold $v_{\min}$, i.e. $v_{\text{buy}} \geq v_{\min}$ to exclude insignificant ratings, without having to reveal the exact amount v_{buy}. Buyer 1 can *sell* this rating information (v_{ratio} and that $v_{\text{buy}} \geq v_{\min}$) about a seller to other potential buyers ("buyer 2") providing buyer 1 an economic incentive to share ratings. We assume from now on that buyer 1 is willing to sell ratings to earn money and buyer 2 is interested in buying them to support decision-making.

Based on buyer 1's identity, knowledge, and rating quality, buyer 2 can decide to buy rating information.

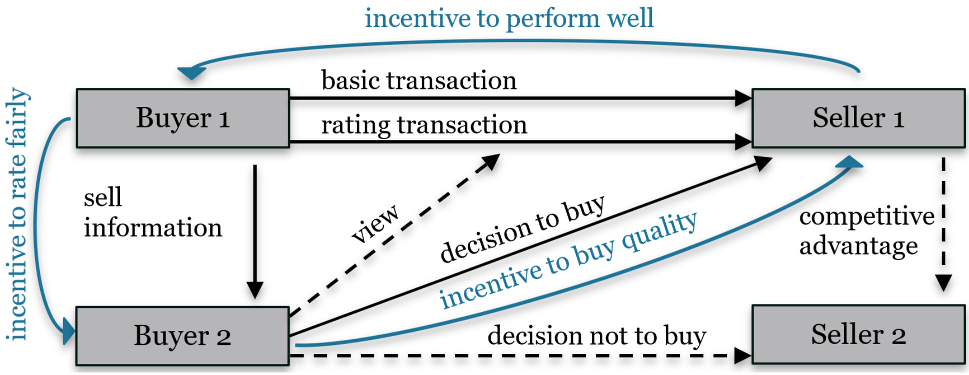


Figure 3. The reputation of seller 1 can be documented with quantified monetary ratings.

After a while, buyer 2 learns about the rating quality of a particular buyer 1 and can also compare bought ratings from different buyers. On this basis, buyer 2 will get a better basis for decision-making. We define four objectives of a solution, guiding the implementation of *secure* reputation ecosystems.

(O1) Ratings remain hidden until sold. All transaction data ($v_{\text{buy}}, v_{\text{rate}}, v_{\text{ratio}}$) is hidden from the public and is only known to buyer 1 and seller 1.

(O2) Selling rating data does not reveal exact values of v_{buy} or v_{rate}. When buyer 1 decides to reveal v_{ratio} and $v_{\min}$ to buyer 2, of course, buyer 2 learns that $v_{\text{buy}} \geq v_{\min}$ and $v_{\text{rate}}/v_{\text{buy}} = v_{\text{ratio}}$. However, buyer 2 is not able to infer anything about v_{buy} or v_{rate} beyond that (keeping prices confidential).

(O3) Buyer 1 cannot lie about the submitted rating data. After buyer 1 submits a rating as rating transaction, buyer 1 is committed to that rating. Buyer 1 is *unable* to prove inconsistent data $v'_{\text{ratio}} \neq v_{\text{rate}}/v_{\text{buy}}$ or $v_{\min} > v_{\text{buy}}$. In particular, neither buyer 1, nor a third party can change a rating (e.g., selectively reveal different ratings to different buyers 2). Also, buyer 1 cannot sell ratings for transactions that are not exceeding a trivial amount $v_{\min}$ (e.g., if the amount was so small to not even cover the typical price of a unit of the good/service, the rating should not be trusted).

(O4) Buyer 2 cannot resell buyer 1's rating information. After buyer 2 receives v_{ratio} (and $v_{\min}$) from buyer 1, it should be infeasible for buyer 2 to sell the information to a third party without involving buyer 1 (or seller 1).

Because we want the reputation ecosystem to work in an open environment—not requiring a central trusted instance—and ensure manipulation resistance, we build the ecosystem upon blockchain technology and several cryptographic concepts.

4.2 Cryptographic building blocks

Commitments. As presented above, the amounts $v_{\text{buy}}, v_{\text{rate}}$ transferred in basic/rating transactions must be hidden from the public. However, one still needs to record $v_{\text{buy}}, v_{\text{rate}}$ in a reliable way, to fulfill the requirement that buyer 1 must not be able to change their ratings once they have been submitted. Cryptographic *commitments* (Brassard, Chaum, and Crépeau, 1988) guarantee this. A commitment C is an object that (1) hides a unique value v that cannot be changed, while (2) not revealing any information about that value. Creating the commitment creates a secret *commitment key* k as a byproduct. With the commitment key k, one can efficiently check what value is hidden inside the commitment C, while everyone who does not know k cannot infer any information about v from C. One can think of a commitment as an encryption of v or a hash $H(v,k)$ for a random unpredictable commitment key k.

In order to record the transaction values $v_{\text{buy}}, v_{\text{rate}}$ securely on the blockchain, one can record a *commitment* C_{buy} to v_{buy} and a commitment C_{rate} to v_{rate} instead. By this C_{buy} and C_{rate} do not reveal any information about v_{buy} and v_{rate} publicly. Only the stakeholders involved in the transaction (buyer 1 and seller 1) can use the commitment key k to make sense of the commitments.

Privacy-preserving cryptocurrency. It is technically challenging to make the transactions conventional secure, e.g., prevent double-spending, because, in our desired setting, the blockchain validators do not even know what amounts are being transferred. However, this problem has been solved by privacy-preserving cryptocurrencies such as Zerocash (Ben-Sasson et al., 2014) and Mimblewimble (Fuchsbauer, Orrù, and Seurin, 2019). We do not focus on the specifics of these privacy-preserving cryptocurrencies because we want to make the system more universally usable to work with any cryptocurrency that fulfills those requirements. Therefore, our system works with any cryptocurrency that fulfills these *requirements*:

- The amount of coins transferred in any transaction is hidden from the public. Only the sender and receiver of a transaction know how many coins were transferred. This necessarily implies that the current account balances of senders and receivers are hidden as well.
- Every transaction contains a publicly available commitment C to the (hidden) number v ("value") of coins transferred. The sender and the receiver hold the commitment key k for C to read the transaction secured in the network.
- The identity of the sender and receiver in a transaction is publicly visible (while just the amount being transferred is hidden).

The first requirement is generally a feature of privacy-preserving cryptocurrencies (Ben-Sasson et al., 2014; Fuchsbauer, Orrù, and Seurin, 2019). Regarding the second requirement, not every cryptocurrency *directly* stores a commitment to the transfer amount v alongside a transaction. However, such a commitment can often be either (1) efficiently derived from all the other data (such as in Mimblewimble, using homomorphic properties of the commitment scheme) or (2) it is available in some commitment-like format (such as Zerocash). For simplicity, we assume that the commitment is directly available. With small modifications, our system works essentially for all (typical) privacy-preserving cryptocurrencies. Finally, the third requirement is not an explicit goal of privacy-preserving cryptocurrencies, but it is trivial to establish using standard techniques such as digital signatures. Buyer 1 can simply sign the transaction with a secret signing key to publicly establish the sender's role in the transaction. We omit the details here but conclude that all three requirements can be achieved by typical privacy-preserving cryptocurrencies.

Zero-knowledge proofs of knowledge (ZKPoK). As discussed above, it must be infeasible for a buyer 1 to lie about the submitted rating. With commitments, buyer 1 could simply reveal the commitment key k and allow buyer 2 to check that the revealed rating data $v_{\text{ratio}}, v_{\text{min}}$ is indeed consistent with what was recorded on the blockchain in the commitments C_{buy} and C_{rate}. However, at the same time, we want buyer 1 to be able to hide the exact values of $v_{\text{buy}}, v_{\text{rate}}$ from buyer 2 and the public, so this approach is not viable (since revealing the commitment key reveals the exact contents of C_{buy} and C_{rate}, namely v_{buy} and v_{rate}). Instead, buyer 1 will *prove* to buyer 2 that the information $v_{\text{ratio}}, v_{\text{min}}$ is correct *without* revealing $v_{\text{buy}}, v_{\text{rate}}$. This requirement can be enabled by *zero-knowledge proofs of knowledge* (ZKPoK) (Goldwasser, Micali, and Rackoff, 1985). A ZKPoK is an interactive protocol, where buyer 1 and buyer 2 exchange messages. This protocol allows buyer 1 to convince buyer 2 of some statement about hidden data $v_{\text{ratio}}, v_{\text{min}}$, without actually revealing the hidden data (Quisquater et al., 1990). However, 1) buyer 2 is not able to learn anything about the $v_{\text{ratio}}, v_{\text{min}}$ other than that the proven statement, i.e. the rating data, is correct (*zero-knowledge*), while 2) buyer 1 is not able to convince buyer 2 of a statement for which it does not know valid hidden data (*proof of knowledge*).

We will furthermore require our ZKPoK to have a third property: deniability (Pass, 2003). Deniability is a non-standard requirement of ZKPoK, which says that after buyer 2 has witnessed the execution of the ZKPoK protocol with buyer 1, buyer 2 *cannot* convince a third party that the proven statement is true. Standard constructions of ZKPoK do generally not have this property. Indeed, for non-interactive ZKPoK (such as SNARKs, STARKs, etc.), being *publicly* verifiable by *anyone* is even considered a feature, which is incompatible with deniability, which says that the proof must only be convincing for buyer 2, not to anyone else. However, one can generally modify any reasonable ZKPoK to provide deniability (Pass, 2003). Using deniability property prevents reselling of information: Because the proof is deniable, buyer 2 will not be able to convince any third party that the rating data is indeed correct.

4.3 Technical description of the method

Buying and rating. The basic transaction, in which buyer 1 pays seller 1 v_{buy} coins for a good or service, is executed via a privacy-preserving cryptocurrency. This results in a commitment C_{buy} to v_{buy} being written to the blockchain. Afterward, buyer 1 pays an additional v_{rate} coins to seller 1, again using the privacy-preserving cryptocurrency, resulting in a commitment C_{rate} to v_{rate} being written to the blockchain. A smart contract binds the two transactions together so that it is clear what basic transaction a rating transaction references. Note that even for a negative rating $v_{\text{rate}} = 0$, a rating transaction (over 0 coins) is submitted to the blockchain. The reason for this is that fully omitting the rating transaction for $v_{\text{rate}} = 0$ would *publicly* signal a negative rating, but the rating result must not be known publically.
The state of the blockchain after this process is depicted in Figure 4. Note that objective O1 (cf. Section 4.1) is fulfilled: $C_{\text{buy}}, C_{\text{rate}}$ are secure commitments, so they do not reveal any information about $v_{\text{buy}}, v_{\text{rate}}$. The privacy-preserving cryptocurrency also does not reveal any information about $v_{\text{buy}}, v_{\text{rate}}$ to the public.

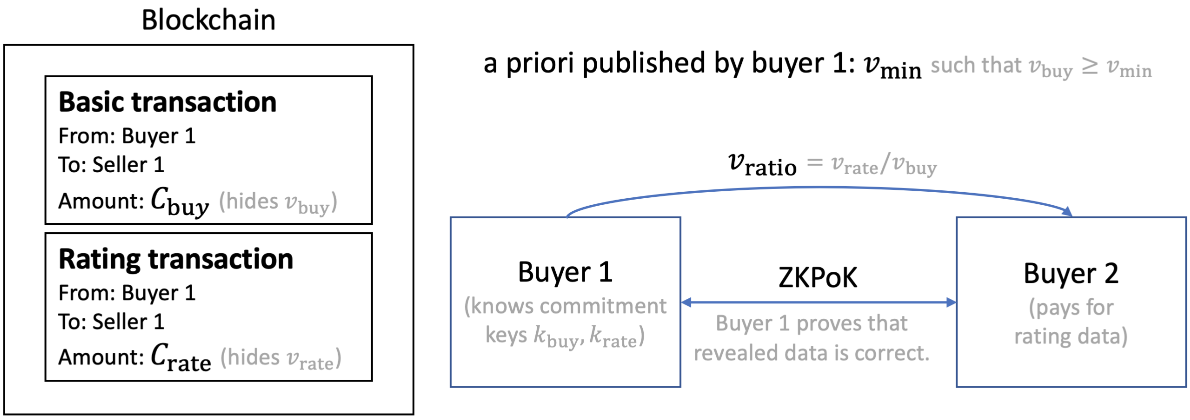

Blockchain
Basic transaction
From: Buyer 1
To: Seller 1
Amount: C_{buy} (hides v_{buy})
Rating transaction
From: Buyer 1
To: Seller 1
Amount: C_{rate} (hides v_{rate})
a priori published by buyer 1: v_{min} such that $v_{\text{buy}} \geq v_{\text{min}}$
$v_{\text{ratio}} = v_{\text{rate}}/v_{\text{buy}}$
Buyer 1
(knows commitment keys $k_{\text{buy}}, k_{\text{rate}}$)
ZKPoK
Buyer 1 proves that revealed data is correct.
Buyer 2
(pays for rating data)

Figure 4. The process of buyer 1 selling rating data to buyer 2, and proving the data's correctness.

Selling rating data. First, if buyer 1 wants to sell the rating information, buyer 1 needs to choose a value v_{min} of the basic transaction s.t. $v_{\text{buy}} \geq v_{\text{min}}$. In the simplest case, v_{min} is simply related to the price of a single unit of seller 1's service. In more complex cases, buyer 1 may explicitly advertise having bought a larger amount, e.g., for at least 1000 coins, in which case $v_{\text{min}} = 1000$ might be a reasonable choice. It is on buyer 1 to decide whether to choose v_{min} as high as possible (close to the paid v_{buy}), making the rating amount more exact, or to choose v_{min} relatively low, in which case buyer 1 reveals less information about the price paid for the basic transaction. We assume v_{min} is published to prospective buyers 2. When buyer 2 wants to buy rating data from buyer 1, buyer 2 approaches buyer 1 and points to buyer 1's transactions on the blockchain that buyer 2 wants to have revealed. If buyer 1 is willing to share rating data with buyer 2, buyer 2 pays buyer 1 for the rating (e.g., via traditional bank transfer or cryptocurrency). In that case, buyer 1 and buyer 2 then engage in the process depicted in Figure 4: Buyer 1 reveals $v_{\text{ratio}} = v_{\text{rate}}/v_{\text{buy}}$ to buyer 2 (as well as stating that $v_{\text{buy}} \geq v_{\text{min}}$). To provide authenticity of v_{ratio} and v_{min}, buyer 1 then uses the commitment keys $k_{\text{buy}}, k_{\text{rate}}$ to prove with a deniable ZKPoK, the following statements about buyer 1's hidden values $(v_{\text{buy}}, k_{\text{buy}}, v_{\text{rate}}, k_{\text{rate}})$ to be true to buyer 2:

- The commitment key k_{buy} shows that the commitment C_{buy} in the basic transaction hides v_{buy}.

- The commitment key k_{rate} shows that the commitment C_{rate} in the rating transaction hides v_{rate}.
- For the revealed value v_{ratio}, it indeed holds that $v_{\text{ratio}} = v_{\text{rate}}/v_{\text{buy}}$.
- For the public value $v_{\min}$ and the secret value v_{buy}, it indeed holds that $v_{\text{buy}} \geq v_{\min}$.

The ZKPoK has the zero-knowledge property, so it does not reveal the exact values of the hidden data v_{buy} or v_{rate}, fulfilling objective O2. With this ZKPoK, buyer 1 proves not to lie about the rating data, which is guaranteed with the proof of knowledge property, fulfilling objective O3 (cf. Section 4.1). Because the ZKPoK is deniable, buyer 2 is not able to resell buyer 1's rating convincingly, fulfilling objective O4.

5 Discussion

With our method, based on established cryptography, it becomes evident that we can build reputation ecosystems technically. With the designed method for storing and trading rating information on a blockchain and the sketched reputation ecosystem, we propose new solutions to resolve three major problems of reputation systems currently used in B2C markets, as summarized above.

a) Current reputation systems are compromised by cheap fake ratings. Fake ratings are a massive problem in review systems since sellers can mandate actors to generate fake reviews cheaply. Even if many of the current platforms struggled hard to prevent fake reviews, the problem prevails (He, Hollenbeck, and Proserpio, 2022). While we acknowledge this issue may cannot be solved completely in an open system (Douceur, 2002), our study might contribute to new approaches to make fake ratings less likely to occur. First, endowing ratings with monetary payments binds substantially more money to issue fake ratings. Second, buyer 1 cannot provide different ratings for different buyers 2, since it is not possible to manipulate a transaction after it has been committed to the blockchain—unless, of course, the blockchain is compromised itself. Third, the rating values are not aggregated immediately (like star ratings or reputation scores on review systems), but ratings can be aggregated and selected by buyer 2 individually. Accordingly, buyer 2 can choose to buy ratings only from other buyers that are considered trustworthy instead of relying on aggregated scores. Since many transactions on B2B markets are valuable, we posit that the effort to search and identify trustworthy buyers 1 is warranted by the additional benefit gained from this process. By accessing experience, own market information, comparing different ratings, and testing ratings submitted by other buyers, buyer 2 will learn over time which buyer 1 delivers useful data. Once buyer 2 identifies trustworthy addresses, they can refer to their ratings as trust anchors, which enables them to identify more honest actors/ratings in the network. In this way, an ecosystem of trust is established over time, reducing information asymmetry and uncertainty in the market. Fourth, since rating information has a high economic value in business (Wise and Morrison, 2000), we can expect information markets or institutions to emerge (Spychiger et al., 2022), which help the companies engaged in the market to identify honest actors in the reputation ecosystem.

Switching the perspective, we consider that buyer 1 might try to trick the system by selling fake ratings. However, such data would remain immutably stored on a blockchain, linked to the addresses that issued the data. Providing misleading ratings would sooner or later prompt buyer 2 quit further buying ratings that were issued by a fraudulent buyer 1. Even if this buyer 1 decides to re-enter the system with a new address and create new fake ratings, such an address would not be considered trustworthy as long as not enough ratings have been issued with other honest sellers. For this reason, connecting fake ratings to honest sellers would be difficult, since all sellers have to commit to being rated. We posit that honest seller 1 would avoid contracting with such addresses, fearing their loss of reputation.

Finally, setting up a bot network to promote a seller would be hard to accomplish, as soon as trustworthy addresses are known and networked. Fake addresses would need to be connected to honest addresses to indicate trustworthiness. This would be hard to accomplish, since honest sellers would refrain from associating with actors they have never transacted with. Once network effects set in, it will get increasingly hard for a malicious actor to submit plausible fake ratings. Buyer 1 can use sampling techniques to find trustworthy sellers regarding ratings of different buyers 1 to confirm the trustworthiness of a seller's address. In addition, as has already been touched on above, such fraudulent actions are prevented, because buyer 2 can select the addresses to buy information from and aggregate ratings individually.

b) Current reputation systems provide insufficient incentives to submit ratings. Current systems lack sufficient incentives for players in a market to submit ratings. Sellers entice buyers to submit ratings which leads to distorted ratings. Buyers usually have no incentive to share rating information in a business context (Jurca and Faltings, 2003). Adding an incentive directly to buyer 1 to sell ratings and earn money should compensate, or even exceed, the effort associated with providing trustworthy ratings. Also, our system incentives buyer 1 to provide ratings for buyer 2 (while ratings might not be in favor of seller 1) to sell more ratings. While this system will work in non-competitive environments, competitors might mutually refuse to exchange ratings (K. Zhu, 2002). Still, solutions might be found to align conflicting interests e.g., involving trusted institutions (see also c)). Furthermore, the ability of sellers to sell ratings themselves can undermine the profits of a buyer 1 and might be reflected in prior negotiations between buyer 1 and seller 1. Still, buyer 1 may have more information to offer. For instance, text reviews that give further information (Zulfiqar et al., 2021; Shaker, Shams Aliee, and Fotohi, 2021). The quality of ratings might affect the price a buyer 1 can charge when selling a rating, strengthening the incentive to submit meaningful ratings. Since the system promises advantages for buyers 1 (get a trust signal, and potentially earn money) and high-quality sellers 1 (build reputation, justify higher prices, and win new buyers), we posit that sufficient incentives may exist for the ecosystem to work.

c) Current reputation systems depend on a commercial platform provider. Current review systems are subject to platform providers that operate a digital platform. Their centralized governance, however, opens up attack vectors that might compromise the system. Manipulation, censorship, or the unwarranted exploitation of user-generated data are risks worth noting. To avoid the manipulation of sensitive rating data, we posit that a blockchain provides a profound infrastructure on which a reputation ecosystem can be built. A core feature of blockchains is the immutability of the stored data (Catalini and Gans, 2016; Tumasjan and Beutel, 2019). Still, we acknowledge, the proposed system could be implemented without a blockchain, however, losing the advantages a blockchain offers.

Next to potentially resolving three conceptual problems of current review systems, we also contribute other improvements for designing reputation ecosystems. First, proposing money as ratings, a buyer 1 thinks twice about giving a positive rating because every positive transaction costs money. Therefore, reciprocity can be diminished, counteracting reputation inflation, and ratings become differentiable and quantifiable. Second, expecting positive ratings, seller 1 might compensate buyer 1 with a price discount. Hence, a buyer 1 can buy a product cheaper, whereby he is rewarded for advertising. For this, buyer 1 ensures this with its credibility, while seller 1 can excel with a higher reputation. This construction turns the dynamic into that a seller also must trust a buyer (Hemmrich, 2023). Introducing trust as a concept for rating submission has hardly been discussed so far (F. Li et al., 2012). Third, since a rating transaction has to be committed from both sides and blockchain data can be analyzed, discriminating ratings are reduced. Every discriminatory behavior will be recorded. Finally, monetary ratings are much faster submitted than writing a review.

Current research on reputation systems considering the B2B context is very limited (Dikow et al., 2015; Gutt et al., 2019). While we frame this kind of system for personal-intense business services, it might also work in other scenarios. It seems to make sense, especially in cases when the uncertainty about the performance is high, enough transactions take place and the players are willing to sell ratings or exchange them for their own ratings. In a business reputation ecosystem, buyer 2 can request ratings and buyer 1 has more control over whom to share them, increasing the willingness to share this information (Boissieu et al., 2021). However, seller 1 can try to promote oneself with fake ratings, at least in an open system, or prompt buyer 1 to rate only certain transactions to hide sensitive data from competitors. Taking the fact that business environments have competitors as well as non-competitive buying peers, institutions, decentralized autonomous organizations (DAOs) (Buterin, 2014), or other mechanisms might play a major role in determining the trustworthiness of rating sellers and organizing the sharing of rating information (Möhlmann, Teubner, and Graul, 2019).

Conventionally, buyers 2 choose familiar, trusted sellers that have not yet built up expertise in the pertaining field (Uzzi, 1997), since they do not know which other sellers suit them. An ecosystem can change this circumstance by affecting matching and resource allocation in a market. Particularly, low-cost sellers can profit through their cost efficiency from such systems, preferring transparency, while high-cost sellers choose opaque environments to hide their costs (K. Zhu, 2002). We expect that in a functioning system, high-quality sellers achieve a competitive edge over weak-performing competitors, promoting good service quality. Ultimately, this system may reduce marketing efforts for capable sellers when they show positive ratings from different buyers, which would be more credible than promoting themselves through marketing. Testing ratings become a cheaper economical means than actually buying a product. This would shift testing a non-digital product to testing digital ratings, or thought-ahead testing certain credentials. Lastly, such systems could also bring risks, such as increased performance pressure, fear of retaliation when rating, inadvertently leaked data, or others.

6 Conclusion

We designed and evaluated a method that enables stakeholders to build business reputation ecosystems. The core idea is to use monetary payments as ratings, stored and made accessible on a blockchain.

We posit that these core features make our system more suitable for B2B markets, since buyers might have a compelling incentive to submit truthful ratings, can better control and share their rating information, and can rely on transparent relations and immutable data that encourage honest behavior, on which ratings can be tested and analyzed without relying on a commercial platform owner. Moreover, our approach exhibits four main differences compared to rival systems. First, ratings become inherent parts of business transactions, whereas rival systems disconnect buying transactions from ratings. Second, ratings are carried out with payments, making the ratings quantifiable. Third, using payments as ratings, bind capital when building up a bot network impeding some attack scenarios. Fourth, reputation is not condensed into one global score and buyers can select ratings according to transparent transaction history and compare them with one another. Furthermore, this system class may lead to a professionalization of business rating submissions and requests, compensate uncertainty of buyers for engaging with sellers, and be used as a marketing tool by delivering a profound data basis.

With this paper we provide a first essential building block for designing reputation ecosystems. We posit that our method can serve well to solve some of the major conceptual problems that prevent using current review systems from a B2C market on B2B markets. Even if our method cannot solve the emergence of fake ratings in open systems completely, we argue that our system makes such fraudulent behavior much more costly and unlikely to occur when such a data set is analyzed. That said, the mechanisms proposed here can only work in a reasonably large network of companies submitting ratings, providing a start for reputation ecosystems to emerge. These initial steps might be hard to take, since digital platforms usually suffer from cold-start problems.

We see our research as an impetus for our community to research the design of business reputation ecosystems. Monetary ratings are novel in research, and by demonstrating this method, we raise more questions than we provide answers. We call for economic, empirical, and practical-oriented research on the proposed system. Technical-oriented research can investigate to prove and reveal the distribution of ratings, implementing DAOs, ratings about ratings, or other decentralized oracle solutions to sort and rank ratings. An interesting research question is whether a seller can be prevented from passing on monetary-based ratings. Other research might investigate different variations of conducting payments as ratings, mapping performance metrics or content of ratings, or the influence on business relationships.

References

Akerlof, G. A. (1970). “The Market for “Lemons”: Quality Uncertainty and the Market Mechanism.” *The Quarterly Journal of Economics* 84 (3), 488–500. ISSN: 00335533. DOI: 10.2307/1879431.

Ansari, S. and S. Gupta (2021). “Review Manipulation: Literature Review, and Future Research Agenda.” *Pacific Asia Journal of the Association for Information Systems* 13 (4), 97–121.

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

Bauer, I., J. Parra-Moyano, K. Schmedders, and G. Schwabe (2022). “Multi-Party Certification on Blockchain and its Impact in the Market for Lemons.” *Journal of Management Information Systems* 39 (2), 395–425.

Bazin, R., A. Schaub, O. Hasan, and L. Brunie (2016). “A Decentralized Anonymity-Preserving Reputation System with Constant-Time Score Retrieval.” *IACR Cryptol. ePrint Arch.* 2016.

Bellini, E., Y. Iraqi, and E. Damiani (2020). “Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey.” *IEEE Access* 8, 21127–21151. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2969820.

Ben-Sasson, E., A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza (2014). “Zerocash: Decentralized Anonymous Payments from Bitcoin.” In: *2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014*. IEEE Computer Society, pp. 459–474. DOI: 10.1109/SP.2014.36. URL: https://doi.org/10.1109/SP.2014.36.

Blömer, J., F. Eidens, and J. Juhnke (2018). “Practical, Anonymous, and Publicly Linkable Universally-Composable Reputation Systems.” In: *Cryptographers’ Track at the RSA Conference 2018*, pp. 470–490.

Boissieu, E. de, G. Kondrateva, P. Baudier, and C. Ammi (2021). “The Use of Blockchain in the Luxury Industry: Supply Chains and the Traceability of Goods.” *Journal of Enterprise Information Management* (34), 1318–1338. ISSN: 1741-0398.

Bolton, G., B. Greiner, and A. Ockenfels (2013). “Engineering Trust: Reciprocity in the Production of Reputation Information.” *Management Science* 59 (2), 265–285. DOI: 10.1287/mnsc.1120.1609.

Bolton, G., E. Katok, and A. Ockenfels (2004). “How Effective are Electronic Reputation Mechanisms? An Experimental Investigation.” *Management Science* 50 (11), 1587–1602. DOI: 10.1287/mnsc.1030.0199.

Brassard, G., D. Chaum, and C. Crépeau (1988). “Minimum Disclosure Proofs of Knowledge.” *J. Comput. Syst. Sci.* 37 (2), 156–189. DOI: 10.1016/0022-0000(88)90005-0. URL: https://doi.org/10.1016/0022-0000(88)90005-0.

Buechler, M., M. Eerabathini, C. Hockenbrocht, and D. Wan (2015). “Decentralized Reputation System for Transaction Networks.” *Technical report, University of Pennsylvania, Tech. Rep.*

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

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

Camilo, G. F., G. A. F. Rebello, L. A. C. de Souza, and O. C. M. Duarte (2020). “A Secure Personal-Data Trading System Based on Blockchain, Trust, and Reputation.” In: *2020 IEEE International Conference on Blockchain (Blockchain)*. IEEE, pp. 379–384. ISBN: 0738104957.

Catalini, C. and J. S. Gans (2016). *Some Simple Economics of the Blockchain*. DOI: 10.3386/w22952. URL: http://www.nber.org/papers/w22952.

Cheung, C. M. K. and D. R. Thadani (2012). “The Impact of Electronic Word-Of-Mouth Communication: A Literature Analysis and Integrative Model.” *Decision Support Systems* 54 (1), 461–470. ISSN: 01679236.

Cleven, A., P. Gubler, and K. M. Hüner (2009). "Design Alternatives for the Evaluation of Design Science Research Artifacts." In: *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, pp. 1–8.

Cronin, J. J., M. K. Brady, and G. T. M. Hult (2000). "Assessing the Effects of Quality, Value, and Customer Satisfaction on Consumer Behavioral Intentions in Service Environments." *Journal of Retailing* 76 (2), 193–218.

Cui, R., J. Li, and D. J. Zhang (2020). "Reducing Discrimination With Reviews in the Sharing Economy: Evidence From Field Experiments on Airbnb." *Management Science* 66 (3), 1071–1094.

DeFigueiredo, D. d. B. and E. T. Barr (2005). "TrustDavis: A Non-Exploitable Online Reputation System." In: *Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC'05)*. IEEE, pp. 274–283. ISBN: 0769522777. DOI: 10.1109/ICECT.2005.98..

Dellarocas, C. (2000). "Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior." In: *Proceedings of the 2nd ACM Conference on Electronic Commerce (EC00)*, pp. 150–157.

— (2003). "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms." *Management Science* 49 (10), 1407–1424.

— (2005). "Reputation Mechanism Design in Online Trading Environments with Pure Moral Hazard." *Information Systems Research* 16 (2), 209–230. DOI: 10.1287/isre.1050.0054.

Dellarocas, C. and C. A. Wood (2008). "The Sound of Silence in Online Feedback: Estimating Trading Risks in the Presence of Reporting Bias." *Management Science* 54 (3), 460–476.

Dennis, R. and G. Owen (2015). "Rep on the Block: A Next Generation Reputation System Based on the Blockchain." In: *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, pp. 131–138. ISBN: 978-1-9083-2052-0. DOI: 10.1109/ICITST.2015.7412073. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7412073&isnumber=7412034.

Dikow, H., O. Hasan, H. Kosch, L. Brunie, and R. Sornin (2015). "Improving the Accuracy of Business-to-Business (B2B) Reputation Systems through Rater Expertise Prediction." *Computing* 97 (1), 29–49. ISSN: 0010-485X. DOI: 10.1007/s00607-013-0345-x.

Douceur, J. R. (2002). "The Sybil Attack." In: *Peer-to-Peer Systems*. Ed. by P. Druschel, F. Kaashoek, and A. Rowstron. Lecture Notes in Computer Science. Berlin: Springer, pp. 251–260. ISBN: 978-3-540-44179-3.

Durkheim, É. (1960). *The Division of Labor in Society: Simpson G., trans.* 4th Edition. Glencoe: Free.

Ekstrom, M. A., H. C. Bjornsson, and C. I. Nass (2005). "A Reputation Mechanism for Business-To-Business Electronic Commerce that Accounts for Rater Credibility." *Journal of Organizational Computing and Electronic Commerce* 15 (1), 1–18. ISSN: 1091-9392.

Ert, E., A. Fleischer, and N. Magen (2016). "Trust and Reputation in the Sharing Economy: The Role of Personal Photos in Airbnb." *Tourism Management* 55, 62–73. ISSN: 02615177.

Filippas, A., J. J. Horton, and J. Golden (2018). "Reputation Inflation." In: *Proceedings of the 2018 ACM Conference on Economics and Computation*, pp. 483–484. ISBN: 9781450358293. DOI: 10.1145/3219166.3219222.

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

Fradkin, A., E. Grewal, D. Holtz, and M. Pearson (2015). "Bias and Reciprocity in Online Reviews: Evidence From Field Experiments on Airbnb." In: *Proceedings of the 16th ACM Conference on Economics and Computation*. Vol. 15, pp. 15–19.

Friedman, E. J. and P. Resnick (2001). "The Social Cost of Cheap Pseudonyms." *Journal of Economics & Management Strategy* 10 (2), 173–199. ISSN: 1058-6407.

Fuchsbauer, G., M. Orrù, and Y. Seurin (2019). "Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble." In: *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany,* *May 19-23, 2019, Proceedings, Part I*. Ed. by Y. Ishai and V. Rijmen. Vol. 11476. Lecture Notes in Computer Science. Springer, pp. 657–689. DOI: 10.1007/978-3-030-17653-2_22. URL: https://doi.org/10.1007/978-3-030-17653-2%5C_22.

Goldwasser, S., S. Micali, and C. Rackoff (1985). "The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract)." In: *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, Rhode Island*. Ed. by R. Sedgewick. ACM, pp. 291–304. DOI: 10.1145/22145.22178. URL: https://doi.org/10.1145/22145.22178.

Granovetter, M. (1985). "Economic Action and Social Structure: The Problem of Embeddedness." *American Journal of Sociology* 91 (3), 481–510. ISSN: 0002-9602.

Gregor, S. and A. R. Hevner (2013). "Positioning and Presenting Design Science Research for Maximum Impact." *MIS Quarterly* 37 (2), 337–355. DOI: 10.25300/MISQ/2013/37.2.01.

Gutt, D., J. Neumann, S. Zimmermann, D. Kundisch, and J. Chen (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. DOI: 10.1016/j.jsis.2019.01.004.

He, S., B. Hollenbeck, and D. Proserpio (2022). "The Market for Fake Reviews." *Marketing Science*. DOI: 10.1287/mksc.2022.1353.

Hein, A., M. Schreieck, T. Riasanow, D. S. Setzke, M. Wiesche, M. Böhm, and H. Krcmar (2020). "Digital Platform Ecosystems." *Electronic Markets* 30 (1), 87–98. DOI: 10.1007/s12525-019-00377-4.

Hemmrich, S. (2023). "Business Reputation Systems Based on Blockchain Technology—A Risky Advance." In: *Proceedings of the 31st European Conference on Information Systems (ECIS)*.

Hendrikx, F., K. Bubendorfer, and R. Chard (2015). "Reputation Systems: A Survey and Taxonomy." *Journal of Parallel and Distributed Computing* 75, 184–197. ISSN: 0743-7315. DOI: 10.1016/j.jpdc.2014.08.004.

Hevner, A. R., S. T. March, J. Park, and S. Ram (2004). "Design Science in Information Systems Research." *MIS Quarterly* 28 (1), 75–105. DOI: 10.2307/25148625.

Hirshleifer, D. and S. H. Teoh (2003). "Limited Attention, Information Disclosure, and Financial Reporting." *Journal of Accounting and Economics* 36 (1-3), 337–386. ISSN: 0165-4101.

Hu, N., L. Liu, and V. Sambamurthy (2011). "Fraud Detection in Online Consumer Reviews." *Decision Support Systems* 50 (3), 614–626. ISSN: 01679236.

Huang, L., C.-H. Tan, W. Ke, and K.-K. Wei (2014). "Do we Order Product Review Information Display? How?" *Information & Management* 51 (7), 883–894.

Ivanova, O. and M. Scholz (2017). "How Can Online Marketplaces Reduce Rating Manipulation? A New Approach on Dynamic Aggregation of Online Ratings." *Decision Support Systems* 104, 64–78. ISSN: 01679236. DOI: 10.1016/j.dss.2017.10.003.

Jacobides, M. G., C. Cennamo, and A. Gawer (2018). "Towards a Theory of Ecosystems." *Strategic Management Journal* 39 (8), 2255–2276.

Jones, D. and S. Gregor (2007). "The Anatomy of a Design Theory." *Journal of the Association for Information Systems* 8 (5), 312–335. DOI: 10.17705/1jais.00129.

Jøsang, A. (2007). "Trust and Reputation Systems." In: *Foundations of Security Analysis and Design IV*. Ed. by A. Aldini and R. Gorrieri. Lecture Notes in Computer Science. Berlin: Springer, pp. 209–245. ISBN: 978-3-540-74809-0.

— (2016). *Subjective Logic: A Formalism for Reasoning Under Uncertainty*. Cham: Springer. ISBN: 978-3-319-42335-7. DOI: 10.1007/978-3-319-42337-1.

Jøsang, A., R. Ismail, and C. Boyd (2007). "A Survey of Trust and Reputation Systems for Online Service Provision." *Decision Support Systems* 43 (2), 618–644. ISSN: 01679236. DOI: 10.1016/j.dss.2005.05.019n.

Jurca, R. and B. Faltings (2003). "An Incentive Compatible Reputation Mechanism." In: *International Conference on E-Commerce (CEC 2003)*. Los Alamito: IEEE, pp. 285–292. ISBN: 0-7695-1969-5.

— (2009). "Mechanisms for Making Crowds Truthful." *Journal of Artificial Intelligence Research* 34, 209–253.

Jurca, R., F. Garcin, A. Talwar, and B. Faltings (2010). "Reporting Incentives and Biases in Online Review Forums." *ACM Transactions on the Web (TWEB)* 4 (2), 1–27. ISSN: 1559-1131.

Kreps, D. M. and R. Wilson (1982). "Reputation and Imperfect Information." *Journal of Economic Theory* 27 (2), 253–279. ISSN: 0022-0531.

Lam, S. Y., V. Shankar, M. K. Erramilli, and B. Murthy (2004). "Customer Value, Satisfaction, Loyalty, and Switching Costs: An Illustration from a Business-to-Business Service Context." *Journal of the Academy of Marketing Science* 32 (3), 293–311.

Lappas, T., G. Sabnis, and G. Valkanas (2016). "The Impact of Fake Reviews on Online Visibility: A Vulnerability Assessment of the Hotel Industry." *Information Systems Research* 27 (4), 940–961. DOI: 10.1287/isre.2016.0674.

Lee, A. S. (2015). "Retrospect and Prospect: Information Systems Research in the Last and Next 25 Years." In: *Formulating Research Methods for Information Systems*. Ed. by L. Willcocks, C. Sauer, and M. C. Lacity. Vol. 28. New York: Palgrave Macmillan, pp. 19–47. ISBN: 978-1-137-50983-3. DOI: 10.1057/9781137509857$\backslash$textunderscore.

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

Litos, O. S. T. and D. Zindros (2017). "Trust is Risk: A Decentralized Financial Trust Platform." In: *21st International Conference on Financial Cryptography and Data Security (FC 2017)*. Security and Cryptology, pp. 340–356. ISBN: 978-3-319-70971-0.

Luca, M. (2017). "Designing Online Marketplaces: Trust and Reputation Mechanisms." *Innovation Policy and the Economy* 17 (1), 77–93. ISSN: 1531-3468.

Lustig, C. and B. Nardi (2015). "Algorithmic Authority: The Case of Bitcoin." In: *48th Hawaii International Conference on System Sciences (HICSS)*, pp. 743–752. ISBN: 978-1-4799-7367-5. DOI: 10.1109/HICSS.2015.95.

Lyon, D. (2014). "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big data & society* 1 (2), 2053951714541861. ISSN: 2053-9517.

March, S. T. and G. F. Smith (1995). "Design and Natural Science Research on Information Technology." *Decision Support Systems* 15 (4), 251–266. ISSN: 01679236. DOI: 10.1016/0167-9236(94)00041-2.

Mayzlin, D., Y. Dover, and J. Chevalier (2014). "Promotional Reviews: An Empirical Investigation of Online Review Manipulation." *American Economic Review* 104 (8), 2421–2455.

Möhlmann, M., T. Teubner, and A. Graul (2019). "Leveraging Trust on Sharing Economy Platforms: Reputation Systems, Blockchain Technology and Cryptocurrencies." In: *Handbook of the Sharing Economy*. Ed. by R. Belk, G. M. Eckhardt, and F. Bardhi. Cheltenham: Elgar, pp. 290–302. ISBN: 978 1 78811 053 2.

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

Mui, L., M. Mohtashemi, and A. Halberstadt (2002). "Notions of Reputation in Multi-Agents Systems." In: *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems Part 1 (AAMAS)*, pp. 280–287. ISBN: 1581134800. DOI: 10.1145/544741.544807.

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

Neumann, J. and D. Gutt (2019a). "He Who Pays the Piper Calls the Tune: Online Review Elicitation by Sellers and Third-Party Platforms in B2B Markets." In: *ECIS 2019 Proceedings*.

— (2019b). "Money Makes the Reviewer Go Round–Ambivalent Effects of Online Review Elicitation in B2B Markets." In: *25th Americas Conference on Information Systems (AMCIS)*, pp. 1–10.

Nissenbaum, H. (2004). "Privacy as Contextual Integrity." *Wash. L. Rev.* 79, 119.

Nunamaker, J. F., M. Chen, and T. D. M. Purdin (1990). "Systems Development in Information Systems Research." *Journal of Management Information Systems* 7 (3), 89–106.

Nunamaker Jr, J. F., R. O. Briggs, D. C. Derrick, and G. Schwabe (2015). "The Last Research Mile: Achieving Both Rigor and Relevance in Information Systems Research." *Journal of Management Information Systems* 32 (3), 10–47.

Pass, R. (2003). "On Deniability in the Common Reference String and Random Oracle Model." In: *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara*. Ed. by D. Boneh. Vol. 2729. Lecture Notes in Computer Science. Springer, pp. 316–337. DOI: `10.1007/978-3-540-45146-4\_19`. URL: `https://doi.org/10.1007/978-3-540-45146-4%5C_19`.

Pavlou, P. A. and A. Dimoka (2006). "The Nature and Role of Feedback Text Comments in Online Marketplaces: Implications for Trust Building, Price Premiums, and Seller Differentiation." *Information Systems Research* 17 (4), 392–414. DOI: `10.1287/isre.1060.0106`.

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

Pereira, J., M. M. Tavalaei, and H. Ozalp (2019). "Blockchain-Based Platforms: Decentralized Infrastructures and its Boundary Conditions." *Technological Forecasting & Social Change* 146, 94–102. ISSN: 00401625. DOI: `10.1016/j.techfore.2019.04.030`.

Pilkington, M. (2016). "Blockchain Technology: Principles and Applications." In: *Research Handbook on Digital Transformations*. Edward Elgar Publishing, pp. 225–253.

Quisquater, J.-J., M. Quisquater, M. Quisquater, M. Quisquater, L. Guillou, M. A. Guillou, G. Guillou, A. Guillou, G. Guillou, and S. Guillou (1990). "How to Explain Zero-Knowledge Protocols to your Children." In: *Conference on the Theory and Application of Cryptology*. LNCS 435. Springer, pp. 628–631.

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

Resnick, P., R. Zeckhauser, J. Swanson, and K. Lockwood (2006). "The Value of Reputation on eBay: A Controlled Experiment." *Experimental Economics* 9 (2), 79–101. ISSN: 1573-6938.

Shaker, M., F. Shams Aliee, and R. Fotohi (2021). "Online Rating System Development Using Blockchain-Based Distributed Ledger Technology." *Wireless Networks* 27 (3), 1715–1737. ISSN: 1572-8196.

Sonneberg, C. and J. vom Brocke (2012). "Evaluations in the Science of the Artificial–Reconsidering the Build-Evaluate Pattern in Design Science Research." In: *International Conference on Design Science Research in Information Systems (DESRIST 2012)*. Berlin: Springer, pp. 381–397.

Soska, K., A. Kwon, N. Christin, and S. Devadas (2016). "Beaver: A Decentralized Anonymous Marketplace with Secure Reputation." *IACR Cryptol. ePrint Arch.*

Spychiger, F., C. J. Tessone, L. Zavolokina, and G. Schwabe (2022). "Incentivizing Data Quality in Blockchain-Based Systems—The Case of the Digital Cardossier." *Distributed Ledger Technologies: Research and Practice* 1 (1), 1–27. ISSN: 2769-6480.

Subramanian, H. (2018). "Decentralized Blockchain-Based Electronic Marketplaces." *Communications of the ACM* 61 (1), 78–84. ISSN: 0001-0782. DOI: `10.1145/3158333`.

Tadelis, S. (2016). "Reputation and Feedback Systems in Online Platform Markets." *Annual Review of Economics* 8 (1), 321–340.

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

Truong, D. (2019). "Distrust Issues in Business-to-Business E-Procurement Decisions." *Journal of Enterprise Information Management* 32 (6), 1071–1087. ISSN: 1741-0398. DOI: `10.1108/JEIM-01-2019-0020`.

Tumasjan, A. and T. Beutel (2019). "Blockchain-Based Decentralized Business Models in the Sharing Economy: A Technology Adoption Perspective." In: *Business Transformation through Blockchain*. Ed. by H. Treiblmaier and R. Beck. Cham: Palgrave Macmillan, pp. 77–120. ISBN: 978-3-319-98910-5.

ur Rehman, M. H., K. Salah, E. Damiani, and D. Svetinovic (2019). "Trust in Blockchain Cryptocurrency Ecosystem." *IEEE Transactions on Engineering Management* 67 (4), 1196–1212. ISSN: 0018-9391.

Uzzi, B. (1997). "Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness." *Administrative Science Quarterly* 42 (1), 35–67.

Vaishnavi, V., B. Kuechler, and S. Petter (2017). *Design Science Research in Information Systems*. URL: `http://www.desrist.org/design-research-in-information-systems/..`

van Aken, J. E. (2004). "Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules." *Journal of Management Studies* 41 (2), 219–246. DOI: `10.1111/j.1467-6486.2004.00430.x`.

Venable, J., J. Pries-Heje, and R. Baskerville (2016). "FEDS: A Framework for Evaluation in Design Science Research." *European Journal of Information Systems* 25 (1), 77–89. DOI: `10.1057/ejis.2014.36`.

Voshmgir, S. and M. Zargham (2020). "Foundations of Cryptoeconomic Systems." PhD thesis. Vienna: WU Vienna University.

Wan, Y. and M. Nakayama (2014). "The Reliability of Online Review Helpfulness." *Journal of Electronic Commerce Research* 15 (3), 179–189. ISSN: 1938-9027.

Wise, R. and D. Morrison (2000). "Beyond the Exchange-The Future of B2B." *Harvard Business Review* 78 (6), 86–96.

Wu, Y., E. W. T. Ngai, P. Wu, and C. Wu (2020). "Fake Online Reviews: Literature Review, Synthesis, and Directions for Future Research." *Decision Support Systems* 132, [113280]. ISSN: 01679236. DOI: `10.1016/j.dss.2020.113280`.

Yoo, Y., O. Henfridsson, and K. Lyytinen (2010). "Research Commentary –The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research." *Information Systems Research* 21 (4), 724–735. DOI: `10.1287/isre.1100.0322`.

Zervas, G., D. Proserpio, and J. W. Byers (2021). "A First Look at Online Reputation on Airbnb, Where Every Stay is Above Average." *Marketing Letters* 32 (1), 1–16. ISSN: 1573-059X. DOI: `10.1007/s11002-020-09546-4`.

Zhu, K. (2002). "Information Transparency in Electronic Marketplaces: Why Data Transparency May Hinder the Adoption of B2B Exchanges." *Electronic Markets* 12 (2), 92–99.

Zulfiqar, M., F. Tariq, M. U. Janjua, A. N. Mian, A. Qayyum, J. Qadir, F. Sher, and M. Hassan (2021). "EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds." *Computers & Security* 100, 102094. ISSN: 0167-4048.

Zyskind, G., O. Nathan, and A. '. Pentland (2015). "Decentralizing Privacy: Using Blockchain to Protect Personal Data." In: *IEEE Symposium on Security and Privacy Workshops (SPW)*. IEEE Computer Society, pp. 180–184. ISBN: 978-1-4799-9933-0. DOI: `10.1109/SPW.2015.27`.