Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

PHD IN MANAGEMENT

Ciclo 33

Settore Concorsuale: 13/B2 – ECONOMIA E GESTIONE DELLE IMPRESE

Settore Scientifico Disciplinare: SECS-P/08 – ECONOMIA E GESTIONE DELLE IMPRESE

FROM TRUST WHO TO TRUST WHAT. A FRESH PERSPECTIVE ON TRUST IN THE ERA OF BLOCKCHAIN

Presentata da: Maria Sciarra

Coordinatore Dottorato

Riccardo Fini

Supervisore

Cristina Boari

Co-Supervisore

Stefano Mengoli

Esame finale anno 2022

ABSTRACT

In the last few years, a remarkable technological revolution has been taking place around the world. Such a technological revolution is not just a means to the end of improving efficiency, but an important end of social order. In this work, I show that blockchain is one important example. I discuss that the success of a disintermediated transaction is conditioned on the level of trust in the rules-of-code. In what follows, the dissertation is organized in three studies. Study 1 is a theoretical paper where I present and discuss a model of how blockchain-like technologies can automate and algorithmically dictate the nurturing of trust. Based on study 1, study 2 is aimed to develop and validate a quantitative scale to measure each component of the proposed trust model. Lastly, study 3 is intended to investigate how telematic equipment can affect individual trusting behavior under condition of information asymmetry. The introduction of black box in the Italian automobile insurance market is the set of this study. Overall, the dissertation offers some major contributions for theory and practice about the dynamics underlying the development of trust in the rising era of blockchain transactions.

Keywords: Code-based Trust, Rules-of-code, Institution-based Trust, Rule-governed Behavior, Credibility, Information asymmetry, Blockchain technology, Digital economy

SUMMARY

INTRODUTION

In the last few years, a remarkable technological revolution has been taking place around the world (Lumineau et al, 2021; Cong, & He, 2019; Davidson et al., 2018; Manski, 2017; Kosba et al., 2016). All firms have moved or are trying to move in the direction of the digital economy by integrating advanced technological solutions (including artificial intelligence and machine learning, robotic process automation, edge computing) in their business models. These advanced technological solutions are not just a means to the end of improving efficiency but an important end of social order (Lumineau et al, 2021; Cong, & He, 2019; Davidson et al., 2018; Ølnes et al., 2017; Zhao et al., 2016). They have the capacity to meet a fundamental human desire for feeling security against opportunism in economic transactions.

The need for a transparent and equal informative ground is required in all economic transactions involving the exchange of valued assets. This is expected to have an impact on the progress of transactions and how trust is developed. Trust is difficult to emerge when there is no assurance about the real intentions of others. In view of such poor information, the use of powerful intermediaries (like banks, governments, and big technology companies) become prevalent to validate the counterpart, thus establishing and maintaining trust between economic actors (Tapscott, & Tapscott, 2016).

Now for the first time ever, there is an alternative way to achieve trust. Trust is not achieved through intermediaries but through the rules-of-code as a matter of digital law (Wright, & De Filippi, 2015; Lessig, 2003; 2006). By reducing the transaction costs associated with information search, coordination and contracting, they define a code-based trust protocol in which trust is the result of a decentralized process without having any prior face-to-face contacts between the economic actors. As this work will show, blockchain is one important example (De Filippi et al., 2020; Mendling et al., 2018; Sas, & Khairuddin, 2017; Lewenberg et al., 2015; Wilson, & Ateniese, 2015; Antonopoulos, 2014; Maurer et al., 2013). Through blockchain, we can apply the rules-of-code strategically to do a variety of economic transactions in security with unknown traders (Nakamoto, 2008). Once virtually everything of value is immutably recorded in the digital ledger, economic actors receive instructions of the right thing to do, making them trustworthy regarding their good intentions.

One of the most important lessons we can learn from an examination of economic life is that the success of a transaction is conditioned on the level of trust inherent in the rules-of-code. Trusting the deterministic computation of blockchain rules-of-code can instill a feeling of being in control, which is in line with the frequently cited recommendation not to trust but verify first and then develop a code-based trust (De Filippi et al., 2020; Weber et al., 2016; Lustig, & Nardi, 2015; Wilson, & Ateniese, 2015). This argument, in my view, requires a deeper exploration in terms of theory building and managerial implications for practice. In the present dissertation, I take on this challenge, discussing the mechanisms through which the rules-of-code can sustain the development of trust under conditions of information asymmetry. The core meaning of such work is coherent with the fact that the emergence of rules-of-code as new organizational forms of economic transactions is an opportunity to reappraise earlier debates on trust (De Filippi et al., 2020; Hawlitschek et al., 2018). In what follows, the dissertation is organized in three studies.

Study 1 comprises the theoretical basis of the entire discussion. It is a theoretical paper where I present and discuss a model of how blockchain-like technologies can automate and algorithmically dictate the nurturing of trust within a digital environment. The model illustrates the causes, nature, and effects of trusting code-based systems to execute economic transactions as an original contribution to the existing literature on trust. I position the present work into the wider research inquiry of institution-based trust and supplement it with the psychological theory of rule-governed behavior. The theory of rule-governed behavior is helpful to frame the code-based trust model within a psychological dimension as a key to capture some unique elements distinguishing between trusting beliefs, attitudes, intentions, behaviors, and other boundary factors. As I proceed in this way, at a structural level, I trace the causal structure of Mayer et al. (1995) model of relation-based trust and substitute key components with technology-oriented concepts. Attention is given to the conceptualization of new identified constructs: characteristics of technology credibility, trust in the rules-of-code and code-based trust. This includes substituting individual characteristics of credibility (ability, integrity, and benevolence) with characteristics of technology credibility. Further, an extensive cross-disciplinary review of literature is presented to identify the micro-manifestations of trusting attitudes and beliefs at the origins of this technology-mediated trust building process.

Based on study 1, study 2 is aimed to develop and validate a quantitative scale to measure each component of the proposed code-based trust model. This is expected to offer one important step in empirical research of trust in blockchain-mediated transactions with possible extension to other types of technologies (such as artificial intelligence and machine learning, robotic process automation, edge computing) with appropriate adaptations. The method employed is based on De Vellis, & Thorpe (2021). Scale development involved three basic steps: item selection, pre-testing and refinement, and scale validation. I first performed a content domain sampling of literature to select best candidate items for the initial item pool. Next, I submitted the initial item pool to expert judges (both academicians and IT practitioners) for item refinement. Feedbacks were then incorporated into the initial item pool. For the scale validation phase, I crafted a short video-tutorial to introduce respondents to a real-life blockchain-like application. This helped respondents to contextualize the purposes of the scale more effectively. Due to the pandemic restrictions, I used Prolific to recruit respondents both for the pilot test and the confirmatory study. Respondents were randomly selected and received compensation for their effort. Finally, statistical test like EFA (factor and reliability analysis) and CFA (convergent, discriminant and nomological validity) were carried out using SPSS and AMOS software packages, respectively. Interpretation of statistical results provided the best reliable combination of items. The final trust scale was composed of sixty-items, providing a combination of conceptual clarity, reliability, and validity.

Study 3 completes my research project. It is an empirical paper within the domain of financial services. The work is intended to investigate how new technology can affect trusting behavior under conditions of information asymmetry. Because blockchain-like technologies are supposed to provide a fully auditable and valid ledger of data, they are going to be adopted as a signaling device to confirm claims of real honesty and promote the development of trust. Literature on information asymmetry is the main reference for the conceptual development and set of main hypotheses. Specifically, I draw my attention to the insurance car market which is particularly well suited to my investigation. In the last few years, insurance firms have been adopting black box as a telematic equipment to collect more accurate data on driving behavior. The introduction of black box is expected to confirm claims of trustworthiness by the policyholders, thus accessing the real driving risk profile to cause an accident. For the present study, I used secondary data from an Italian insurance company and integrated it with other data from public repositories to control for other potentially explanatory factors and endogeneity issues. A series of logit models was developed to test the initial hypothesis for statistical significance on the likelihood of accident. STATA was the tool to conduct the statistical analysis. Findings revealed that the adoption of black box can confirm the actual policyholder' claims of trustworthiness in high-traffic areas, thus sustaining the trust-building process from the perspective of an insurance firm. Surprisingly, I obtained an opposite result for policyholders who were from the group of women and more experienced drivers. I discuss the overconfidence bias as a possible explanation. Finally, I conduct robustness checks to support my argument against self-selection and endogeneity.

In summary, the dissertation offers some major contributions for theory and practice. First, I contribute to the academic debate by proposing a code-based trust model which can capture the dynamics underlying the development of trust in technology-mediated transactions. Study 1 is an important step forward in general organizational research. In so doing, it aims to parallel the interaction-based trust of the original Mayer's model. Next, study 2 provides a measurement tool to empirically test the expected relations among each model component. Research moves head more quickly when a measurement tool is well defined in terms conceptual clarity, reliability, and validity (Schwab 1980; Kaplan 1964). With study 3, I examine the role of technology in a realistic scenario of information asymmetry. I show that it is particularly useful to confirm claims of trustworthiness because information is on parity. Lastly, there are practical managerial implications. I give a few valuable perspectives for those practitioners that are wondering about an enhanced understanding of implications of blockchain-like technology for digital transactions (Hawlitschek et al., 2018; Seidel, 2018; Glaser, 2017; Beck et al., 2016).

BLOCKCHAIN-BASED TRUST SYSTEMS: AN INTEGRATIVE MODEL OF HOW RULES OF CODE CAN BUILD TRUST IN DIGITAL ECONOMIC TRANSACTIONS

Blockchain has received a growing interest from research. This article draws attention to the implications of blockchain for the trust- building process. This paper, precisely, deals with the causes, nature, and outcomes of trusting code-based systems at the micro-level. Literature on institution-based trust provides a fundamental theoretical background that I supplement with the psychological theory of rule-governed behavior. I believe that the psychological dimension is key to capturing some unique elements of trust in the rules-of-code. Following this approach, I construe trust in the rules-of-code and present a complete model of code-based trust. The empirical evidence of blockchain supports the entire discussion.

Keywords: Institution-based Trust, Rule-governed Behavior, Credibility, Blockchain technology, Digital economy

INTRODUCTION

In the recent past, blockchain has emerged as technological and social innovation for supporting secure and transparent economic transactions in the digital environment (Lumineau et al, 2020; Cong, & He, 2019; Davidson et al., 2018; Manski, 2017; Kosba et al., 2016). It is essentially an immutable system of data recording that is particularly appealing to prevent dishonest behavior between unknown traders, without the intervention of a trusted intermediary (Nakamoto, 2008). Since its beginning in 2008, blockchain has drawn the attention of organizational researchers (e.g., Lumineau et al, 2020; Davidson et al., 2018; Miller, & Griffy-Brown, 2018; Seidel, 2018; Seidel, & Greve, 2017; Werbach, 2016; Kosba et al., 2015). Early organizational studies of blockchain have observed that a system of this sort is a more efficient way to manage economic transactions and control self-interest, compared to the decision to rely on relational governance mechanisms of self-enforcement (Lumineau et al., 2020; Cong, & He, 2019; Davidson et al., 2018; Ølnes et al., 2017; Zhao et al., 2016). Because the rules-of-code form the foundation of blockchain to provide a secure framework for transactions, the modus of interaction is standardized to ensure that users behave in a pre-planned manner (Davidson et al., 2018; Hsieh, & Vergne, 2018; Tschorsch, & Scheuermann, 2016; Okhuysen, & Bechky, 2009). Similar to an institution, the rules-of-code can support procedural and structural coordination between parties.

Definition of blockchain as institutional technology (Davidson et al., 2018; Atzori, 2017; Mayer-Schonberger, & Cukier, 2013; Steiner, 2012; Pariser, 2011) asks for a reflection on the adaptability of the relational trust-model by Mayer et al. (1995). In Mayer et al.' s model the notion of trust is based upon face-to-face experience with other individuals. Although this model has been widely accepted in many empirical studies of trust in relationships (Schoorman et al., 2007), it appears less applicable when economic transactions are automatically executed upon the rules-of-code (De Filippi et al., 2020). The blockchain rules-of-code creates a more impersonal form of trust which is constitutively embedded in the rules-of-code. It leads to a shift from trusting people to trusting the rules-of code as a mental state of perceived security that things will go well because the rules-of-code do something important for the users (De Filippi et al., 2020; Sas, & Khairuddin, 2017; Weber et al., 2016; Lewenberg et al., 2015; Wilson, & Ateniese., 2015; Antonopoulos, 2014; Maurer et al., 2013). Some researchers however have lamented that the present argumentation of a code-based trust model is poorly meaningful in providing a comprehensive theoretical contribution for the academic debate (Lumineau et al., 2020; Rikken et al., 2019; Hawlitschek et al., 2018). Without a clear specification, the quote “trust in the rules-of-code” is likely to remain a vague concept with limited theoretical foundations. In this study, I address this gap and examine what trust in the rules-of-code is, which are its antecedents and with which implications for the trust-building process.

To answer these questions, I start positioning my line of inquiry within the literature of institution-based trust (Bachmann, & Inkpenn 2011; Bachmann, & Zaheer 2008; Child, & Möllering, 2003; Bachmann 2001; Lane and Bachmann 1996; Zucker, 1986). This literature assumes that the trust-building process is a macro-level phenomenon involving considerations of security one feels about a situation because of structural safeguards and guarantees (McKnight et al., 1998; Shapiro, 1987; Zucker, 1986). This perspective is helpful to shed light on how individuals place themselves under the influence of institutions (Zucker 1986). But in this perspective, the inclusion of micro-level factors such as trusting attitudes and beliefs is usually not recognized as essential to describing the feeling of security about outcome in institution-mediated relationships (Bachmann, & Inkpenn 2011). On the contrary, I believe that a feeling of security can be hardly manifested without having prior perceptions that a specific institution can do something important. Therefore, I discuss trust in the rules-of-code at the micro-level integrating the literature of institution-based trust with the psychological theory of rule-governed behavior. In this theory, the perceived credibility of rules is a key concept to believe that rules are trusted to create an environment where individuals feel safe and secure about the future outcome (Hayes et al., 2001; Hayes, Zettle & Rosenfard, 1989; Zettle & Hayes, 1982; Skinner, 1966).

A few studies in the field of blockchain technology have already shown that the credibility of rules-of-code is a critical aspect to uncovering preferences for technology-mediated transactions when users do not have direct experience with one another (De Filippi et al., 2020; Lumineau et al., 2020; Hawlitschek et al. 2018). I further dig into credibility by identifying the characteristics of the technology. Three characteristics appear to reflect trusting beliefs and affect the willingness to trust the rules-of-code and decision to follow a rule-governed behavior: functionality, fairness, and responsiveness. They are identified through a systematic literature review of organizational studies on the general class of institutions which are exactly the rules of the game in society (Bachmann, & Inkpenn, 2011; North, 1990; Zucker, 1986). Thus, I discuss each of these characteristics and link them to the agent's propensity to trust and other trusting factors to conceptualize trust in the rules-of-code. A discussion of antecedents to trust in the rules-of-code, trust in the rules-of-code itself, and outcomes leads to a comprehensive code-based trust model. In presenting such a model, I adapt the original structure of Mayer et al.'s model on relational trust to code-based trust.

Our contribution is threefold. First, I deal with the challenge to rethink how new digital technologies are impacting social phenomena like trust. Having considered blockchain a type of institution, I provide some useful insights to interpret how the general category of institutional technology can alter the way economic agents interact and build trust within a digital environment.

Second, my study is a more general contribution to the established literature of institution-based trust. As I argue throughout the paper, the psychology-oriented literature of rule-governed behavior provides an innovative way to investigate the role of institutions in the trust-building process. In my view, the psychological dimension helps target the definition of an impersonal form of trust through its antecedents (beliefs and attitudes). Specifically, the identification of characteristics of technology credibility is a major novelty I introduce for the study of trust in the rule-of-code and its causes. Thus, my model can be reasonably considered to be supplementary to Mayer et al. (1995) in the realm of institution-mediate relationships.

Lastly, my study has practical managerial implications. I give a valuable perspective for those practitioners that are wondering about an enhanced understanding of implications and benefits of blockchain-like technology for contracting and corporate governance practices in digital transactions (Hawlitschek et al., 2018; Seidel, 2018; Glaser, 2017; Beck et al., 2016).

The study is structured as follows. First, I introduce the novel challenges for the trust-building process posed by blockchain technology and other digital technology supporting transactions. I then provide a brief literature review of the terms and concepts concerning the institution-based trust literature as the main theoretical foundation of this study. Following that, I introduce the theory of rule-governed behavior and describe its fundamental aspects, focusing on how it helps define the quote “trust in the rules-of-code” and build a model of code-based trust. Then I describe each structural component of the model, providing illustrations concerning blockchain technology. Finally, the last part is dedicated to discussing theoretical contributions and directions for future research.

TRUST BUILDING IN CODE-DRIVEN TRANSACTIONS

From the interaction-based trust to the emergence of code-based systems of trust

Prior research defines trust as a status of mind which derives from the optimistic expectation that another party can be relied on according to norms of fair and honest behavior (Rousseau et al., 1998; Mayer et al., 1995). Trust allows empathizing with the partner for a collective benefit above any self-gain (Gulati, & Sytch, 2008). Among scholars in management and general business, the trust-building model by

Mayer et al. (1995) is a reference point to theorize in the face of interaction-based contacts. They employ a psychological perspective to propose a process model which differentiates between trusting beliefs, attitudes, intentions, and behaviors as important factors to the development of trust of one individual for another (Figure 1).

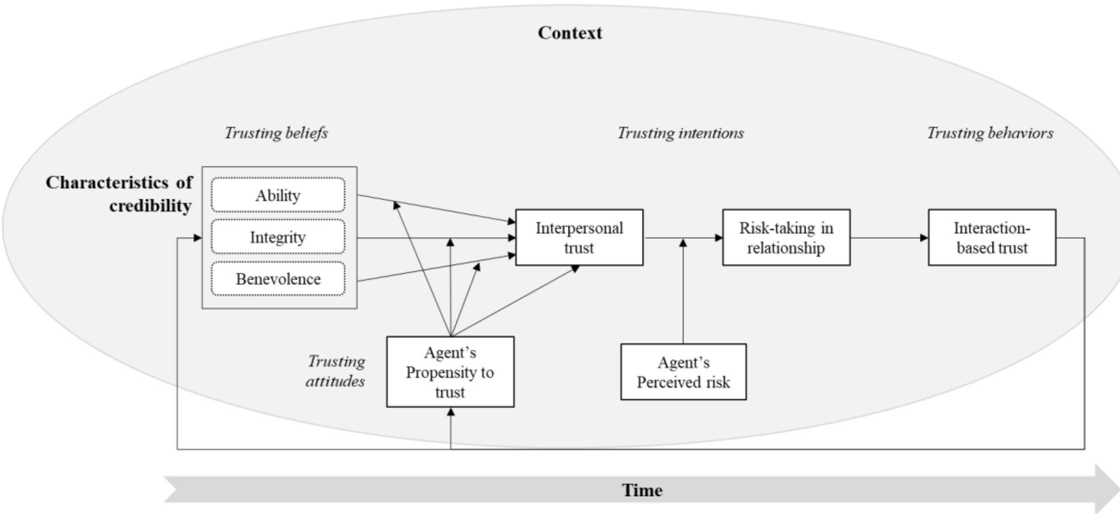

Figure 1 – Model of interaction-based trust (Mayer et al., 1995)

In Mayer et al., trusting someone originates from perceptions of the other party's credibility characteristics (ability, integrity, and benevolence). These perceived characteristics determine if a person can be more or less trusted. Trust-building, however, can be different for agents with a low versus high propensity to trust. Rotter (1972) defines propensity to trust as a personal trait that leads to a generalized willingness to confidently rely on across situations. This construct comes from dispositional psychology to reflect the effect of personality characteristics and experiential factors (Sitkin, & Pablo, 1992). Although such a dispositional tendency cannot perfectly predict the volition to trust (Mayer, Davis, & Schoorman, 1995), it is alike in coloring perceptions of credibility and influences the amount of trust for a specific other (Mallard et al., 2014; Braithwaite, 2002; Kagan & Scholz, 1984). As illustrated in Figure 1, the right side of the trust-building process model concerns trust itself and its outcome under the moderation of perception of risk. Perceived risk is an essential component of a model of trust and involves consideration of the context (Mayer, Davis, & Schoorman, 1995). It is about the assessment of uncertainty for things out of control that have the potential to realize significant and/or disappointing outcomes from the exchange. Thus, only if the level of trust exceeds the perception of risk, one is prepared to engage in a relationship built upon face-to-face interactions. Such a behavioral manifestation of trust is not static but evolves. This implies that repeated interactions lead to a continuous re-evaluation of the decision to trust in light of previous first-hand personal experiences (Gulati, & Sytch, 2008).

Interaction-based trust has always been the main form of trust. The most recent potentials of digital technologies, however, are challenging such an idea and proposing new forms of trust (Lumineau, Wang, & Schilke, 2020; Rikken et al., 2019; Hawlitschek et al., 2018). For example, consider how insurance firms deal with the information mismatch between the insurer and the insured (Riley, 2001; Rothschild, & Stiglitz, 1976; Spence, 1973). When a policy for an insurance premium is undersigned upfront, the insured typically has to trust that the insurance company has clear contractual conditions and will pay the indemnity for the damage one might suffer in the future. On the other hand, the insurance company has to trust that the insured will not cheat, given the impossibility of perfectly observing the actual behavior. Such difficulties are all the greater given the few interactions, limited to the annual renewal of the policy. Under these conditions the lack of quantifiable information prevents distinguishing real truthful parties from those who claim to be, thus creating occasions for opportunistic behavior (Williamson, 1985).

The use of digital technology may thus obviate the risk for opportunistic behavior because the interaction is automatically executed, controlled, and documented upon a set of pre-established rules-of-code without the intervention of a trusted intermediary (Gatteschi et al., 2018). The computational logic of the rules-of-code has the merit to provide a unified view of the true state of reality which is credible in the eyes of all parties (Davidson et al., 2018). This can solve the problem of trust misplacing, especially in those business relationships that would be characterized by weak strategies to mitigate the risk of dishonest traders (Manski, 2017; Kosba et al., 2016). A scenario as such is exactly what blockchain technology intends to achieve, thus radically transforming the trust-building process (Lumineau, Wang, & Schilke, 2020; Rikken et al., 2019; Davidson et al., 2018; Hawlitschek et al., 2018). In doing blockchain-mediated transactions, users subject themselves to the technology, reducing (in most cases eliminating) the need for learning about the partner and for trust emerging from interpersonal interactions (Schneier, 2019;

Antonopoulos, 2014). This means that interaction-based trust is likely to be substituted by code-based systems of trust.

Blockchain as institutional technology for trust-building

Blockchain is a decentralized and distributed record-keeping system to enable secure and real-time exchanges of valued assets without the intervention of a trusted authority (Tapscott, & Tapscott, 2016; Nakamoto, 2008). In the blockchain, digital transaction records are organized in a growing list of blocks, forming a permanent chain that is maintained by a distributed peer-to-peer network of computing systems. Each block contains valid time-stamped data of transactions and is protected by a highly secure mechanism of immutability (Friedlmaier et al. 2018; Ølnes, 2016). Because no centralized authority exists, the rules-of-code determine the scope of blockchain in validating and maintaining transaction data around a true state with verifiable properties (Hsieh, & Vergne 2018; Ølnes et al., 2017; Crosby et al., 2016; Tapscott & Tapscott, 2016; Tschorsch, & Scheuermann, 2016; Zhao et al., 2016; Zyskind et al., 2015). Rules-of-code are a written logical instance of computing law reflecting what is good, equitable, and just in a step-by-step process to accomplish a task (Wright, & De Filippi, 2015; Lessig, 2003; 2006).

As Davidson et al (2018) emphasize in their work, the effect of blockchain is not limited to improvements in the productive efficiency of economic transactions but it also involves gains for economic governance. It determines what one can appropriately do as a consequence of the algorithmically driven construction of public immutable knowledge, thus regulating individual behavior (Lumineau & Oliveira, 2020). By furthering a sense of good faith and fair dealing behavior, any unilateral deviations from expected behavior are more easily detectable by the rules-of-code of blockchain. They serve a social function about the coordination of individual behavior which becomes more predictable information (Lumineau & Oliveira, 2020; Davidson et al., 2018; Al Khalil et al., 2017; Ahangama, & Poo, 2016; Lustig, & Nardi, 2015; De Filippi, & Mauro, 2014). In these circumstances, a better way to portray blockchain is to think of blockchain as an institutional technology that combines practical application of methods, systems, and devices for coordination purposes of economic transactions (Lumineau et al., 2020; Davidson et al., 2018).

Institutions as governance mechanisms exist to constrain human behavior into a priori acceptable actions as part of a world-known (Zhou, & Xu, 2012; Poppo et al., 2008; Bachmann, 2006; Zaheer, McEvily, & Perrone, 1998). This means the sources of hazards are reduced even in the face of very limited trusting involvement, leading to a reasoned willingness to securely engage any kind of relationship which scholars call institution-based trust (Mishra, & Mishra, 2013; Bachmann, & Inkpen, 2011; Pavlou, & Gefen, 2004; Child, & Mollering, 2003; Bachmann 2000; McKnight et al., 1998; Zucker, 1986; Kagan, & Scholz, 1984). As a result, institutions may instill a certain level of perceived situational normality and structural assurance. Situational normality stems from the appearance that things are customary and in proper order to feel comfortable enough to make transactions (Baier, 1986; Lewis, & Weigert, 1985; Garfinkel, 1963). Structural assurance, on the other hand, refers to the security one feels because of protective structures and safeguards (Williamson, 1993; Shapiro, 1987; Zucker, 1986).

All that is needed is a minimal amount of trust in the institution's capability to offer behavioral guidelines that cannot be ignored for the achievement of social and economic goals (Child, & Mollering, 2003; Sztompka, 1999; Fukuyama, 1995; Barber, 1983). Institutional trust is a status of mind that breaks down at the microlevel in the context of economic transactions (Bachmann, 2006; North, 1998; 1997; 1990; Elster, 1989). It is essentially a matter of perceptions about the credibility of institutions to impose compliance without discrimination (Bachman, & Inkpen, 2011; Smith, 2010; Nooteboom, 2007; O' Hara, 2004; Hardin, 1999; Harré, 1999; Offe, 1999; Sztompka, 1999) Having defined institutional trust in such a way, institution-based trust is one consequent behavior (Mishra, & Mishra, 2013; Bachmann, & Inkpen, 2011; Pavlou, & Gefen, 2004; Child, & Mollering, 2003; McKnight et al., 1998; Zucker, 1986). Because of favorable perceptions about institutions to reach the attainment of structural and normal conditions, people securely rely on others without having any prior personal experience in dealing with one another (Bachmann, & Inkpen, 2011; Nooteboom, 2007; Pavlou, & Gefen, 2004; Child, & Mollering, 2003; Currall, & Inkpen, 2001; McKnight et al., 1998).

Within the same perspective, scholars claim that institutional technology requires trusting in advance the rules-of-code (Al Khalil et al., 2017; Sas, & Khairuddin, 2017; Lustig, & Nardi, 2015). The quote "trust in the rules-of-code" is used to describe the reconfiguration of trust in the face of an institutional technology which is different from trusting an e-commerce platform in a technological perspective (Rikken et al., 2019; Schneier, 2019; Atzori, 2017; Antonopoulos, 2014). The latter implies that a company provides a platform which is trusted because of the trust in the company itself (Mcknight et al., 2002). In trust in the rules-of-code, this shift of trust from people to the rules-of-code as the primal source of trust raises some questions regarding the trust-building process model. I am in front of an impersonal form of trust, which is found on technology-like characteristics, rather than on personal characteristics such as ability, integrity, and benevolence (De Filippi et al., 2020; Lumineau et al., 2020; Hawlitschek et al. 2018) or on some platform provider (like e-commerce platform). Although a growing body of literature states that a different trusting framework is required in the case of blockchain and other similar technologies, research has not clarified yet what trust in the rules-of-code is and how it comes from.

We believe that to understand the causes, nature, and effects of trust in the rule-of-code I should adopt a psychological perspective that is outside the sphere of institution-based trust literature. By incorporating some elements from the theory of rule-governed behavior (Zettle, & Hayes, 1982; Skinner, 1966) into institution-based trust literature, I break down the building process of trust distinguishing factors that contribute to trusting the rules-of-code, trust in the rules-of-code itself, and its outcomes.

Rule-governed behavior and trust in the rule-of-code

A very large body of research in psychology demonstrates that individuals rely on various kinds of behavioral rule systems to help them assess problems and make sense of reality (Kramer, 2006). To take an example from outside the sphere of business, children's education can be seen as an important system of rules. To protect children from costly mistakes and to provide relational frames of societal coordination, parents transmit codified rules of good behavior as cultural and societal heritage. For example, upon the rule "Tell the truth, and you'll be fine", the child learns that telling the truth is the right thing to do for having positive consequences (Törneke, Luciano, & Valdivia, 2008). A rule is said to work in the eyes of the child if it is possible to monitor compliance and deliver consequences (Zettle, & Hayes, 1982). It is in these circumstances that a child takes a rule-governed behavior. The concept of rule-governed behavior was first introduced by Skinner (1966) to account for a voluntary response to a discriminative stimulus of instructional control. The individual decision to follow a system of rules is influenced by the amount of trust that rules can provide stability and order in the world around (Skinner, 1966). This trust, however, is conditional on a set of beliefs about the specific rule's credibility (Törneke, Luciano, & Valdivia, 2008).

Credibility is a topic that has been addressed in the fields of psychology to understand why a given party will have a greater or lesser amount of trust for another party (Tseng, & Fogg, 1999; McCroskey, & Young, 1981). Traditionally, scholars have viewed credibility as a perceived quality of being truthful. It is not an inherent property, but rather it results from evaluating multiple dimensions simultaneously (Fogg, 2003; Self, 1996). Indeed, the concept of credibility encompasses the evaluation of trustworthiness and competence (Hovland, Janis, & Kelley, 1953). Trustworthiness is a core dimension to capture perceptions of being right and free from bias (Mayer, Davis, & Schoorman, 1995). It also involves the commitment to keep promises and care about the interest of others. For rules being trustworthy means that there is a regular correspondence between what the rules say and what they do each time for things to go well, as a consequence of continuous reinforcements (Hayes et al., 2001; Hayes, Zettle & Rosenfard, 1989; Zettle & Hayes, 1982). Competence, on the other hand, reflects perceptions of being performative (Barber, 1983). For a rule to be competent, it must stand for something useful in the repertoire of individuals (Skinner, 1966). This would mean that it can offer a fluent and effective track of behavior in social coordination (Törneke, Luciano, & Valdivia, 2008; Skinner, 1966).

If one believes in the credibility of rules about trustworthiness and competence, this constitutes a reason to trust (Skinner, 1966). Examples of this matter are pretty much everywhere in the realm of the digital economy. Let us consider, for example, the insurtech industry.

In the insurance industry, the use of blockchain could have a relevant impact on fraud prevention during the underwriting and payouts (Gatteschi et al., 2018). Because all data is stored on the blockchain, the terms of the agreement are transcribed in the code and automatically enforced, without human interference. As a consequence, both parties can see logged transactions and do not lose agreement information. A scenario such as the one depicted, however, could be difficult to realize without involving primarily perceptions about the credibility of the rules-of-code. Perceptions of credibility fundamentally evoke a kind of belief that rules-of-code are robust to circulate correct information of each transaction without discrimination (Murray et al., 2019; Nesbitt, 2019; Mallard, Méadel, & Musiani, 2014; Grinberg, 2011). Empirical evidence has shown that those beliefs are a fundamental precondition if the blockchain rules-of-code are to be trusted about their ability to mitigate the risk of manipulation and increase transparency (Tschorsch, & Scheuermann, 2016; Antonopoulos, 2014; Mauer et al., 2013). Based on the insights from the theory of rule-governed behavior about the relevance and role of rule credibility, I clarify the concepts of trust in the rules-of-code, its antecedents, and outcomes.

A MODEL OF CODE-BASED TRUST

A model of code-based trust which applies to blockchain-mediated transactions is presented in Figure 2. At a structural level, the model traces the causal structure of Mayer et al. 's (1995) to hold a widely accepted approach to trust which is presented in straightforward terms.

In line with the objectives of present discussion, I substitute key components with technology-oriented concepts. This includes substituting individual characteristics of credibility (ability, integrity, and benevolence) with characteristics of technology credibility. In line with Mayer's model, my model distinguishes between trusting beliefs, attitudes, intentions, behaviors, and other boundary factors. A literature review is organized to clearly identify the diverse conceptualizations of each trusting component. As presented in Table 1, the literature review is conflated within a concept matrix. The matrix is organized by research field (e.g. psychology, strategy and management, sociology, economics, and management information systems) and divides the literature contributions by trusting attitudes, beliefs, intentions, and behaviors.

	Attitudes	**Beliefs**	**Intentions**	**Behaviors**	**Time & Context**	**Research field**
Agarwal, & Karahanna, 2000; Agarwal, & Praasad, 1998	x					Strategy & management
Ahangama, & Poo, 2016					x	Management information systems
Arrighetti et al., 1997; 1997		x				Strategy & management
Arvanitidis, 2020		x				Strategy & management
Bachman, & Inkpen, 2011; Bachmann, 2006; Bachmann 2001; Lane and Bachmann 1996		x	x	x		Strategy & management; Sociology
Barber, 1983				x		Strategy & management
Biais et al., 2018			x			Management information systems
Biermann, 2007; Botchway, 2001		x				Strategy & management; Sociology

	Attitudes	Beliefs	Intentions	Behaviors	Time & Context	Research field
Bühlmann & Kunz, 2011		x				Sociology
Chanley et al., 2000		x				Strategy & management
Child and Möllering, 2003		x				Strategy & management
Coleman, 1990					x	Strategy & management
Davidson et al., 2018		x				Management information systems
Davis, 1989; Davis et al., 1989	x					Psychology; Strategy & management
De Filippi, Mannan, & Reijers, 2020		x	x	x		Management information systems
Dirks, & Ferrin, 2002		x				Psychology
Espinal et al., 2006		x				Strategy & management
Fukuyama, 1995; Elster, 1989			x			Economics
Gambetta, & Hamill, 2005; Bacharach, & Gambetta, 2001		x				Strategy & management
Giddens		x				Sociology
Gulati, & Sytch, 2008					x	Strategy & management
Hardin, & Offe, 1999				x		Economics
Harré, 1999				x		Economics; Psychology
Hayes et al., 2001; Hayes, Zettle & Rosenfard, 1989; Zettle & Hayes, 1982		x				Psychology
Ho, 2018; 2014; 2006		x				Strategy & management
Hodgson, 2006		x				Economics
Hsu, & Lu, 2004	x					Management information systems
Hurley, 2006, 2012		x				Strategy & management
Husted, & Folger, 2005		x				Strategy & management
Igbaria et al., 1995	x					Management information systems
Kramer, 1994	x					Strategy & management

	Attitudes	Beliefs	Intentions	Behaviors	Time & Context	Research field
Kumlin, 2004		x				Economics; Sociology
La Porte & Metlay, 1996; La Porte, 1994		x				Economics; Sociology
Lankton et al., 2014					x	Management information systems
Levi, & Stoker, 2000; Levi, 1998		x				Economics; Sociology
Lewenberg et al., 2015			x			Management information systems
Lippert, & Forman, 2006; Lippert, 2007	x					Management information systems; strategy & management
Luhmann 1988; 1979		x			x	Sociology
Lumineau et al., 2020					x	Strategy & management
Lustig, & Nardi, 2015	x	x	x		x	Management information systems
Manski, 2017		x			x	Management information systems
Maurer et al., 2013					x	Management information systems
McKnight et al., 2011	x	x		x	x	Management information systems
Mcknight, & Kacmar, 2007; McKnight, & Chervany, 2005; McKnight et al, 2002; McKnight, & Chervany, 2001; McKnight et al., 1998	x	x		x		Management information systems; Strategy & management
McKnight, & Chervany, 2006					x	Management information systems; Strategy & management
Mishler & Rose, 1997		x				Sociology
Mishra, & Mishra, 2013		x				Strategy & management
Mollering, 2006; Lane, 1998				x		Strategy & management
Möllering, 2001	x					Strategy & management
Murphy, 2004		x				Sociology
Murray et al., 2019		x			x	Management information systems
Nooteboom, 2007		x		x		Strategy & management

	Attitudes	Beliefs	Intentions	Behaviors	Time & Context	Research field
North, 1998; 1997; 1990		x	x			Economics
O' Hara, 2004		x		x		Sociology; Management information systems
Offe, 1999				x		Sociology
Orren, 1997		x				Sociology
Parasuraman, 2000	x					Management information systems
Pavlou, & Gefen, 2004; Gefen, 2000	x	x				Strategy & management; Management information systems
Pero, & Smith, 2008		x				Economics; Sociology
Rikken et al., 2019			x			Management information systems
Roeck et al., 2019					x	Management information systems
Rogers, 1995	x					Psychology; Strategy & Management
Rosenberg, 1957	x					Economics; Sociology
Rotter, 1971	x					Psychology
Sas, & Khairuddin, 2017; 2015	x	x			x	Management information systems
Sato, 1988	x					Economics; Sociology
Schillewaert et al., 2005	x					Management information systems
Schoorman et al., 2007					x	Strategy & management
Schuette, 2021		x				Management information systems
Schutz,1964		x				Economics
Seidel, 2018		x				Management information systems
Shapiro, 1987			x			Strategy & management
Sheppard et al. 1992		x				Strategy & management
Sitkin, & Pablo, 1992					x	Psychology
Skinner, 1966		x				Psychology
Smith, 2011; 2010		x		x		Economics; Sociology

	Attitudes	Beliefs	Intentions	Behaviors	Time & Context	Research field
Sztompka, 1999		x	x			Strategy & management; Sociology
Tapscott, & Tapscott, 2017		x				Management information systems
Törneke, Luciano, & Salas, 2008	x					Psychology
Tschorsch, & Scheuermann, 2016					x	Management information systems
Tullberg, 2007	x					Strategy & management; Sociology
Tyler, 1997; Tyler & Degoey, 1996; Tyler & Lind, 1992; Lind & Tyler, 1988		x				Strategy & management; Psychology
van der Heijden, 2004	x					Management information systems
Van Dyne et al., 2000	x					Strategy & management
van Esterik-Plasmeijer & van Raaij, 2017		x				Management information systems
Wang et al., 2016		x				Management information systems
Weber et al., 2016		x		x		Management information systems
Williamson, 1993; 1991		x				Strategy & management; Economics
Wilson, & Ateniese, 2015		x		x		Management information systems
Wright, & De Filippi, 2015; De Filippi, & Mauro, 2014		x				Management information systems
Yamagishi et al., 1998			x			Sociology
Zaheer, McEvily, & Perrone, 1998		x				Strategy & management
Zhao et al., 2016		x				Management information systems
Zucker, 1986		x		x		Sociology

Table 1 – Concept matrix of code-based trust model

In the following sections, I present and discuss all the components and causal relationships. Particular attention is given to the conceptualization of newly identified constructs: characteristics of technology credibility, trust in the rules-of-code, and code-based trust.

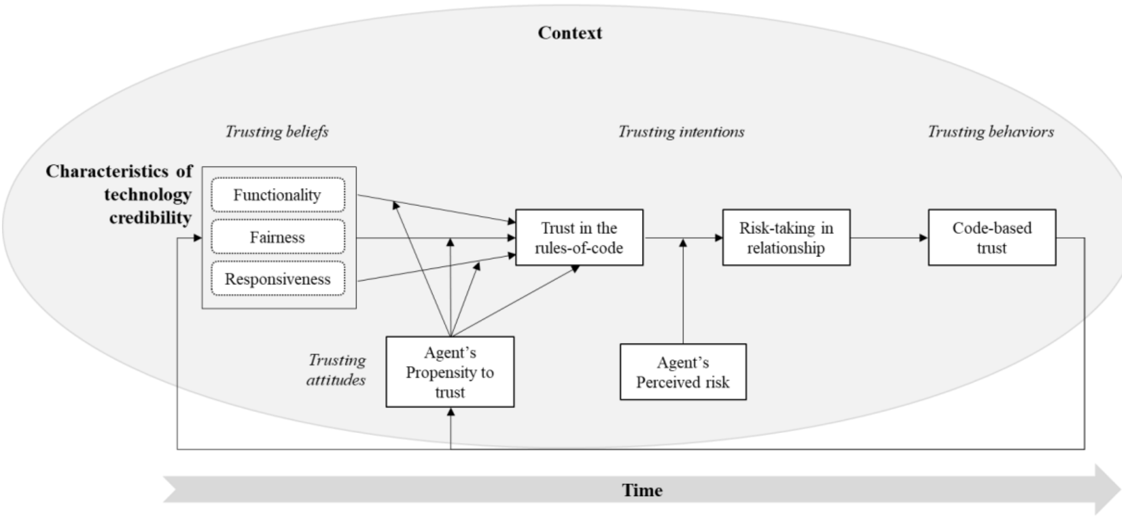

Figure 2 – Model of code-based trust

Trust in the rules-of-code and code-based trust

This section provides a conceptualization of trust in the rules-of-code as trusting intention, meaning that one intends to depend on, even though unpleasant consequences are possible. The definition of trust in rules-of- code proposed in this study is precisely the willingness to be vulnerable to the actions of rules-of-code, based on the positive expectation that they will constrain living behaviors to unharmful patterns. Making oneself vulnerable to the rules-of-code means that one is prepared to accept the risk of computational faults. I claim that trust in the rules-of-code is fundamentally a complex psychological phenomenon representing the subjective probability that the rules-of-code will provide stable step-by-step instructions for a predictable pattern of behavior. Having trust in the rules-of-code so defined, I relate trust to situations characterized by a certain degree of risk

(Schoorman et al., 2007; Mayer et al., 1995; Williamson, 1993; Coleman, 1990; Johnson-George, & Swap, 1982; Rotter, 1967; Deutsch, 1958). Transactions that are governed by the blockchain rules-of-code are at risk of being invalidated in the event of competing forks (De Filippi, Mannan, & Reijers, 2020; Rikken et al., 2019; Biais, Bisière, Bouvard, & Casamatta, 2018; Lewenberg et al., 2015). A fork is an important change to the blockchain rules-of-code that makes previously valid blocks and transactions invalid, thus generating doubts about the true state of reality. In these conditions, blockchain may appear a less secure exchange platform which does put a user at risk.

In many ways, this definition of trust in the rules-of-code echoes that one of institutional trust (Child, & Mollering, 2003; Sztompka, 1999; Yamagishi et al., 1998; Fukuyama, 1995; Shapiro, 1987; Barber, 1983). Institutional trust denotes the belief that an institution may lend meaning to the events and provide patterns of behavior as a part of a world in common (Bachmann, 2006; North, 1998; 1997; 1990; Elster, 1989). Such a conceptual similarity is not surprising since rules-of-code are a specific instance of institutions. I know from earlier studies that institutional trust is very conductive to institution-based trust (Bachman, & Inkpen, 2011; Smith, 2010; Nooteboom, 2007; O’ Hara, 2004; Hardin, 1999; Harré, 1999; Offe, 1999; Sztompka, 1999). Institution-based trust is a derivative form of trust in others because credible institutions provide sufficient motives to engage in business transactions with a feeling of relative security (Bachmann, & Inkpen, 2011; Mollering, 2006; Lane, 1998; Zucker, 1986). Although the lack of emotional involvement may suggest a weak expression of trust-related behavior, it offers considerable benefits regarding the success of economic transactions (Bachmann, & Inkpenn, 2011; Bachmann 2001; Lane and Bachmann 1996). In the same vein, where trust in the rules-of-code of blockchain exists, code-based trust is one consequence. Within my model, code-based trust becomes a trusting behavior, which parallels the interaction-based trust of the original Mayer's model. It represents the willingness to engage in disintermediated transactions with others (De Filippi et al., 2020; Hawlitschek et al., 2018Sas, & Khairuddin, 2017; Lustig, & Nardi, 2015). The deterministic computation of blockchain rules-of-code can instill a feeling of being in control, which is in line with the frequently cited recommendation not to trust but verify first and then develop a code-based trust (De Filippi et al., 2020; Weber et al., 2016; Lustig, & Nardi, 2015; Wilson, & Ateniese, 2015).

Characteristics of technology's credibility

When an individual makes trust judgments, they look for cues that provide a reason to trust (Gambetta, & Hamill, 2005; Bacharach, & Gambetta, 2001; Sztompka, 1999). Previously I have presented that one approach to understanding why people build a greater or lesser amount of trust in a rule-governed system is to consider the attributes of credibility (Törneke, Luciano, & Salas, 2008). While building on the theory of rules-of-governed behavior as a theoretical foundation to conceptualize credibility as the antecedent to trust in the rules-of-code, I recognize that characteristics of institutional credibility have been considered repeatedly in the literature of social science (e.g., Mishra, & Mishra, 2013; Bachmann, & Inkpen, 2011; Nooteboom, 2007; Hodgson, 2006; Williamson, 1993). They are manifestations representing the acceptance of an institution as a rule-governed system based on positive perceptions it can act in a competent and trustworthy fashion to provide social support (Ho, 2018, 2014; Pero, & Smith, 2008; Gambetta, & Hamill, 2005; Bacharach, & Gambetta, 2011; Offe, 1999; Sztompka, 1999; Zucker, 1986). From my systematic literature review (see Appendix A), I identify three distinct characteristics: functionality, fairness, and responsiveness (see Table 1). As I discuss later, they match the two components of credibility described in the theory of rule-governed behavior: competence and trustworthiness. Precisely, functionality is just an expression of competence, while fairness and responsiveness relate to trustworthiness. Moreover, they can parallel Mayer et al. (1995) human-like trusting characteristics in interpersonal relationships (i.e., ability, integrity, and benevolence). Functionality can be mapped to ability, fairness to integrity, and benevolence to responsiveness. In the remainder of this section, the three characteristics are examined in more detail.

Functionality

Functionality is the distinctive characteristic to serve a purpose effectively. All authors in rule-governed behavior considered functionality an essential element of rule credibility (Hayes et al., 2001; Hayes, Zettle & Rosenfard, 1989; Zettle & Hayes, 1982). It is a quality to signal a sense of being in good hands because of a certain degree of correspondence between what the rule itself is supposed to do and the way the environment is then arranged. This generalized comforting belief may be thought of positively affecting the idea that a transaction is bound under structural assurance (McKnight et al., 1998). My review indicates that terms like effectiveness, formality, reliability, consistency or performance (e.g., Kumlin, 2004; Murphy, 2004; Levi, & Stoker, 2000; Sztompka, 1999; Levi, 1998; Arrighetti et al., 1997; Lane & Bachmann, 1996, 1997; Mishler & Rose, 1997; Orren, 1997; La Porte & Metlay, 1996; Tyler & Degoey, 1996; La Porte, 1994; Tyler & Lind, 1992; North, 1990; Giddens, 1990) are all facets of the same dimension, each one relating exactly to what researchers in rule-governed behavior construe as functionality. The domain of the functionality is specific. Rules may be highly effective in some environmental situations but not in others. In the domain of blockchain, the rules-of-code are evaluated primarily about their correct functioning to protect the record of all prior transactions from unexpected events and external tampering (Sas, & Khairuddin, 2017; Zhao et al., 2016; Lustig, & Nardi, 2015). Interviews with blockchain users indicate that the cost (in computation and equipment) required for verifying transactions and coordinating the exchange of valued assets is a guarantee for the functionality of the blockchain technology to work properly (Lustig, & Nardi, 2015). The blockchain correct functioning is limited to most elementary types of transactions (like digital currency exchanges, land title rights) that can be expressed by simple rules (Murray et al., 2019; Davidson et al., 2018; Manski, 2017;

Wang et al., 2016; Wright, & De Filippi, 2015). More complex transactions would require a greater number of resources to consider all possible contingencies.

Fairness

Another important aspect of rule credibility involves fairness. From the rule-governed behavior theory, I learn that individuals are sensitive to aspects related to the building principles of procedures. They look for rules that are perceptually fair in providing procedural norms and structural constraints of socially mediated consequences so that they give the feeling of being in control and informed (Hayes, Zettle, & Rosenfard, 1989). Fairness, indeed, refers to the perception that rules establish a procedure that is clear and compatible with what is considered right and just (Sheppard et al. 1992). A few social scientists have focused on similar concepts to describe the institutional commitment to impartial and just treatment, using synonyms like openness and transparency (Smith, 2011; Pavlou and Gifen, 2004), formality and clarity (Espinal et al., 2006; Kumlin, 2004; Murphy, 2004; Chanley et al., 2000; Zaheer, McEvily, & Perrone, 1998; Mishler, & Rose, 1997), neutrality and impartiality (O’Hara, 2004; Child and Möllering, 2003; Tyler, 1997; Tyler, & Degoey 1996; Tyler, & Lind, 1992; Luhmann 1988; 1979; Zucker 1986), and accountability (Smith, 2011; Biermann, 2007; Botchway, 2001). Beliefs that rules are treating fairly are conductive to perceptions of situation normality (Husted, & Folger, 2005; McKnight, & Chervany, 2005; Dirks, & Ferrin, 2002; Levi, 1998; McKnight et al., 1998; Tyler, 1997; Tyler &

Degoey, 1996; Lind & Tyler, 1988; Schutz,1964). In the case of blockchain, perhaps, the relationship between fairness and trust is established once a certain level of functionality is recognized. Fairness is evaluated in terms of the robustness of rules-of-code to operate without discrimination and prejudice and penalize misbehavior (Lewenberg et al., 2015; Lustig and Nardi, 2015; Wright, & De Filippi, 2015). One of the core characteristics of blockchain is that all transactions can be reviewed and verified, increasing the user control of information (De Filippi et al., 2020; Davidson et al., 2018; Wang et al., 2016; Lustig and Nardi, 2015; Wright, & De Filippi, 2015; Zyskind et al., 2015). Moreover, because the rules-of-code are characterized by mathematical rigor, they are assumed to be hardly corruptible (Szabo, 2017; Mauere et al. 2013).

Responsiveness

Skinner (1966) argued that rules can perform in responsive ways. When rules prove to be helpful and supportive in providing temporal and causal frames of proper behavior in the best interest of individual and collective needs, they hold the characteristic of responsiveness (Törneke et al., 2008; Hayes, Zettle, & Rosenfarb 1989; Zettle, & Hayes, 1982). Responsiveness refers to the capability to offer active support. For example, if some disturbances affect the usual practices of social coordination, rules may help restore uncontested behavioral frames for the survival of social interactions (Williamson, 1991; North, 1990). This idea of doing good is also recurring in the literature about the positive orientation of institutions towards collective well-being.

Researchers have proposed concepts like delivering on promises (e.g., King, 2012; Espinal et al., 2006; Ho, 2006), sensitiveness to moral concern, and social interest (e.g., Schuette, 2021; Arvanitidis, 2020; van Esterik-Plasmeijer & van Raaij, 2017; Bühlmann & Kunz, 2011; Smith, 2011; Hurley, 2006, 2012). In the same vein, the emergence of blockchain has paved the way for a technological commonwealth in which social coordination is sustained by an ethic of individual behavior replacing inefficient institutions (Manski, 2017; Tapscott, & Tapscott, 2017; Lustig and Nardi, 2015; Wright, & De Filippi, 2015; De Filippi, & Mauro, 2014). Applications of blockchain to certain questioned sectors of the global economy (like finance, supply chain, food) have the potential to support individual responsibility and group cooperation, increase user control of information, and maintenance of high-quality and accurate data (Murray et al., 2019; Seidel, 2018; Sas and Khairuddi, 2017; Manski, 2017; Wang et al., 2016).

Functionality, fairness, and responsiveness are all equally important to trust in the rules-of-code. The level of trust should not be thought to be either trustworthy or not trustworthy. It varies along the continuum depending on how characteristics of technology credibility are perceived. Perceptions of technology's credibility characteristics are related to each other, but each one varies independently. Consider, for example, the case of Decentralized Autonomous Organization (DAO). A DAO is an internet-native organization made of a computer program enforced on the blockchain (Murray et al., 2018; DuPont, 2017; Leonhard, 2017; Jentzsch, 2016). In the original design, characteristics of technology's credibility were all perceived to be high, thus highly trusted to solve the principal-agent problem (Davidson et al., 2018; Murray et al., 2018). After the first launch in 2016, the DAO was nearly immediately hacked due to vulnerabilities in its codebase. This contributes to undermining the principle of security to create a theoretical immutable chain which is a core tenet of the blockchain functionality (Murray et al., 2018). Nevertheless, while the functionality of blockchain becomes questionable, perceptions regarding fairness and responsiveness are still high to sustain a minimum level of trust in decentralized autonomous organizations.

Agent's propensity to trust

Consideration of credibility characteristics is by itself insufficient for understanding the amount of trust. Mayer et al. (1995) have already shown the propensity to trust impacting interpersonal trust directly (see Figure 1). The same is true also for trust in the rules-of-code (Sas, & Khairuddin, 2017; 2015; Lustig, & Nardi, 2015). Propensity to trust is a stable trait representing the individual disposition to trust in general, across various situations (Van Dyne et al., 2000; Sato, 1988; Rotter, 1971; Rosenberg, 1957). As unconditional attitude (Möllering, 2001; Kramer, 1994), it colors the interpretation of unfamiliar situations in more meaningful judgments based on life experiences, personality types, and cultural background (Tullberg, 2007; McKnight, & Chervany, 2001). In the field of information technology, this propensity to trust relates to general technology. It is comprised of two subconstructs, personal innovativeness, and experience with technology. Personal innovativeness means one shows an inclination to try out new technologies (Agarwal, & Karahanna, 2000; Agarwal, & Praasad, 1998; Rogers, 1995). In other words, it describes the individual attitude to be a technology pioneer (Schillewaert et al., 2005; Parasuraman, 2000). On the other hand, experience with technology is about previous practical contacts, knowledge, and feelings of usefulness and ease of use regarding technological systems (Hsu, & Lu, 2004; van der Heijden, 2004; Igbaria et al., 1995; Davis, 1989; Davis et al., 1989). Earlier experience with other technological systems helps generate more realistic expectations that something should be in a certain way. Because personal innovativeness and experience with technology both relate to a priori optimistic assumptions about technology' attributes, they precede trusting beliefs (McKnight et al., 2011; Lippert, 2007; Mcknight, & Kacmar, 2007; Lippert, & Forman, 2006; Pavlou, & Gefen, 2004; McKnight et al, 2002; Gefen, 2000). Hence, personal innovativeness and experience with technology, in general, are expected to influence the perceived value of blockchain and the volition to ultimately depend on. Empirical studies of blockchain corroborate this position, providing evidence that users make prior trust-related assumptions based on whatever they already know about technology (Sas, & Khairuddin, 2015).

Context and time

Earlier scholars have highlighted the importance of context in influencing the willingness to trust (McKnight et al. 2011; Schoorman et al., 2007). Context is characterized by several factors, such as familiarity with the domain, level of control systems, and social attachment (Sitkin, & Pablo, 1992). These factors have an impact on the assessment of the likelihood of positive and negative transaction outcomes, given all possible interpretations of the risk involved (Coleman, 1990; Bierman et al., 1969). For example, the context of blockchain is characterized by numerous key items, including technological skills, technical challenges, comprehensibility of the underlying the rules-of-code, unsettled corporate regulation, cyber security, and privacy (Murray et al., 2019; Manski, 2017; Sas, & Khairuddin, 2017; Ahangama, & Poo, 2016; Tschorsch, & Scheuermann, 2016; Lustig, & Nardi, 2015; Maurer et al., 2013). Among these items, advanced computer skills requirements may generate a technological divide, suggesting blockchain serves only the interests of technological adepts (Manski, 2017; Sas, & Khairuddin, 2017; Lustig, & Nardi, 2015). This indeed would imply resistance to consider blockchain dependable as a credible institutional technology. In my model, all these contextual aspects affect trusting beliefs, intentions, and behaviors in light of the specific perceived risks. Perceived risk relates to issues associated with electronically transmitting credit cards, sharing personal information, and legal outcomes (Sas, & Khairuddin, 2017; 2015). It is not a direct antecedent of trusting beliefs, but it would influence behavioral intentions directly. The decision to take a code-based trust behavior will be realized only if the total level of trust in the rules-of-code results surpasses perceived risk.

Another critical aspect is the process by which trust evolves in time. Several theorists have suggested that trust is an active process of continuous reevaluation (Lankton et al., 2014; Gulati, & Sytch, 2008; Schoorman, 2007; McKnight, & Chervany, 2006; Mayer et al., 1995; Luhmann, 1979). The proposed model, indeed, incorporates that active nature of trust in the rules-of-code as represented by the feedback loop in Figure 2. If the decision to trust the rules-of-code leads to a favorable outcome eventually, perception of technology credibility is enhanced in magnitude to sustain future usage of blockchain. Likewise, perceptions decline when trust leads to the direct and/or indirect observations of unfavorable conclusions. At the very beginning, trust in the rules-of-code might be fragile and may be rather tentative (Sas, & Khairuddin, 2017; Lustig, & Nardi, 2015). Trust is fragile because it is supported by little experience which makes perceived risk high. The lack of experience leads to poorly meaningful perceptions, which implies that some time is needed before a conclusive evaluation. Perceptions of functionality and fairness are more salient early when external sources (user reviews, surveys, proof of concepts, or certification) may help assess the credibility of the blockchain (Lumineau et al., 2020; Murray et al., 2019; Roeck et al., 2019; Sas, & Khairuddin, 2017). As familiarity with blockchain is increased, more accurate evaluations are developed also including considerations about responsiveness. Perceptions of responsiveness take more time and their effect increases as the blockchain promise to establish technological commonwealth is gradually confirmed by practical and qualitative observations of emergent uses in various businesses (Manski, 2017).

DISCUSSIONS

In the recent literature, some have observed that the notion of trust in the rules-of-code (Schneier, 2019; Antonopoulos, 2014) represents a potentially fruitful area of advancing research about technology in society (Lumineau et al., 2020; Rikken et al., 2019; Hawlitschek et al., 2018). In this study, I answer the call by providing several theoretical insights for the study of trust in the context of digitally mediated transactions. Assuming blockchain as exemplary institutional technology (Davidson et al., 2018; Atzori, 2017; Mayer-Schonberger, & Cukier, 2013; Steiner, 2012; Pariser, 2011), I present a definition of trust in the rule-of-code within the framework of institution-based trust literature (Bachmann, & Inkpenn, 2011; Bachmann, 2006; Zucker, 1986). Although institution-based trust literature deals with the mechanisms through which institutions influence the trust-building process, I acknowledge that it ignores important psychological substrata that should be at the basis of trust. Therefore, I integrate this stream of literature with the theory of rule-governed behavior (Zettle, & Hayes, 1982; Skinner, 1966). By using the theory of rule-governed behavior, I propose a model of code-based trust which recognizes the causal structure of Mayer et al.'s (1995) with the integration of new elements from the context of digitally mediated transactions.

First, my primary contribution is to clarify what trust in the rules-of-code is and how it comes from. My model is predictive based upon complete causal relationships between trusting beliefs, attitudes, intentions, and behaviors. The model has clear lines of focus on the cognitive substrata underlying micro dynamics of trust within an institutional environment. All things together, my model should represent an important step forward in general organizational research. Authors interested in investigating other institutional technologies similar to the blockchain (such as artificial intelligence and machine learning, robotic process automation, edge computing) can use the present code-based trust model as a theoretical basis. My model, indeed, has the potential to be adapted to any way of organizing economic transactions. The fundamentals (structure and components) of the model are not tailored upon the blockchain specifications but they are derived from a longstanding debate on the role of institutions for the trust building process.

Second, I propose a set of characteristics of technology's credibility (functionality, fairness, and responsiveness) as antecedents to describe the volition to trust the rules-of-code. Having derived these characteristics from a systematic literature review of different streams that have not been linked previously, they are an important contribution to examining trust mechanisms. Third, I contribute to practice. For practice, I increase understanding of how to build trust in the rules-of-code. I explicitly examine three specific characteristics of technology's credibility which may affect the decision to engage a technology-mediated transaction by a code-based trusting behavior. This is consistent with the actual trends of moving away from offline to digital transactions (Lumineau et al., 2020; Constantinides, & Parker, 2017; Simonite, 2016; Hanseth, & Lyytinen, 2010; Tilson et al., 2010).

This study raises several issues for future research of trust within the domain of digital transactions. First, the goal of the study is limited to studying the effect of rules-of-code on trust. Thus, contribution to understanding the role of code-based trust in economic prosperity is beyond my scope. I am aware that this avenue is very promising, and more work needs to be done to obtain a dominant thesis that could explain any correlation between trust in the rules-of-code and the persistence of economic success. In particular, an important area for future research is the mechanism through which such trust accumulates and depreciates within the borders of societal culture or value systems (De Filippi et al., 2020; Lumineau et al., 2020; Rikken et al., 2019; Hawlitschek et al., 2018). Second, the proposed model neglects the process by which trust in the rules-of-code interfaces relational trust, meaning whether competing forms of trust may take a considerable complementarity rather than fostering a substitution effect. I believe it would be of interest to explore the optimal combinations of trust in the rules-of-code and relational trust in the context of digital trading. Finally, my effort is limited to providing a more complete theoretical foundation of trust in the rules-of-code, and I do not deal with the operationalization and the full test of the model. I think that the operationalization of this model would be beneficial. One way is to identify the relevant measures through a survey-based approach which provides valuable insights and has been largely used in trust literature

(Schoorman et al., 2007). I invite scholars to take on this challenge using this or other different qualitative and quantitative methodologies available for the target.

REFERENCES

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. MIS quarterly, 665-694.

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. Information systems research, 9(2), 204-215.

Aguinis, H., & Glavas, A. (2012). What we know and don’t know about corporate social responsibility: A review and research agenda. Journal of management, 38(4), 932-968.

Ahangama, S., & Poo, D. C. C. (2016). Credibility of Algorithm Based Decentralized Computer Networks Governing Personal Finances: The Case of Cryptocurrency. In International Conference on HCI in Business, Government, and Organizations (pp. 165-176). Springer, Cham.

Al Khalil, F., Butler, T., O’Brien, L., & Ceci, M. (2017). Trust in smart contracts is a process, as well. In International Conference on Financial Cryptography and Data Security (pp. 510-519). Springer, Cham.

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.".

Arrighetti, A., Bachmann, R., & Deakin, S. (1997). Contract law, social norms and inter-firm cooperation. Cambridge journal of economics, 21(2), 171-195.

Arvanitidis, P., Economou, A., Grigoriou, G., & Kollias, C. (2020). Trust in peers or in the institution? A decomposition analysis of Airbnb listings' pricing. Current Issues in Tourism, 1-18.

Atzori, M. (2017). Blockchain governance and the role of trust service providers: the TrustedChain® network. Available at SSRN 2972837.

Bachmann, R. (2001). Trust, power and control in trans-organizational relations. Organization Studies, 22, 337–365.

Bachmann, R. (2006). 22 Trust and/or power: towards a sociological theory of organizational relationships. Handbook of trust research, 393.

Bachmann, R., & Inkpen, A. C. (2011). Understanding institutional-based trust building processes in inter-organizational relationships. Organization studies, 32(2), 281-301.

Bachmann, R., & Zaheer, A. (2006). Handbook of trust research. Cheltenham: Edward Elgar.

Bacharach, M., & Gambetta, D. (2001). Trust in society, 148.

Baier, A. (1986). Trust and antitrust. ethics, 96(2), 231-260.

Barber, B. (1983). The logic and limits of trust. New Brunswick: Rutgers University Press.

Bargh, M. S., Choenni, S., & Meijer, R. (2016). On design and deployment of two privacy-preserving procedures for judicial-data dissemination. Government Information Quarterly, 33(3), 481-493.

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain–the gateway to trust-free cryptographic transactions.

Behn, R. D. (1998). The new public management paradigm and the search for democratic accountability. International Public Management Journal, 1(2), 131-164.

Bekkers, R. (2003). Trust, accreditation, and philanthropy in the Netherlands. Nonprofit and Voluntary Sector Quarterly, 32(4), 596-615.

Bhatnagar, S. (2008). Building trust through e-government: Leadership and Managerial Issues. United Nations Public Administration Network. http://unpan.un.org./intradoc/groups/public/documents/unpan/unpan025871. pdf.

Biermann, F. (2007). 'Earth system governance'as a crosscutting theme of global change research. Global environmental change, 17(3-4), 326-337.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., & Menkveld, A. J. (2020). Equilibrium bitcoin pricing. Available at SSRN 3261063.

Botchway, K. (2001). Paradox of empowerment: Reflections on a case study from Northern Ghana. World development, 29(1), 135-153.

Braithwaite, J. (2002). Restorative justice & responsive regulation. Oxford University press on demand.

Bühlmann, M., & Kunz, R. (2011). Confidence in the judiciary: Comparing the independence and legitimacy of judicial systems. West European Politics, 34(2), 317-345.

Chanley, V. A., Rudolph, T. J., & Rahn, W. M. (2000). The origins and consequences of public trust in government: A time series analysis. Public opinion quarterly, 64(3), 239-256.

Child, J., & Möllering, G. (2003). Contextual confidence and active trust development in the Chinese business environment. Organization Science, 14, 69–80.

Christensen, T., & Lægreid, P. (2002). New public management: Puzzles of democracy and the influence of citizens. Journal of Political Philosophy, 10(3), 267-295.

Coleman, J. S. (1990). The Foundations of Social Theory. Cambridge, Mass: Harvard University Press.

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. The Review of Financial Studies, 32(5), 1754-1797.

Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction - platforms and infrastructures in the digital age. Information Systems Research, 29(2), 381-400.

Creutzfeldt, N., & Bradford, B. (2016). Dispute resolution outside of courts: procedural justice and decision acceptance among users of Ombuds services in the UK. Law & Society Review, 50(4), 985-1016.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

Cukierman, A. (2000). Accountability, credibility, transparency and stabilization policy in the eurosystem.

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, 14(4), 639-658.

Davis, F. (1986). Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results, unpublished doctoral dissertation, MIT.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340.

De Blok, L., & Kumlin, S. (2021). Losers' Consent in Changing Welfare States: Output Dissatisfaction, Experienced Voice and Political Distrust. Political Studies.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, 101284.

De Filippi, P., & Mauro, R. (2014). Ethereum: the decentralised platform that might displace today's institutions. Internet Policy Review, 25.

Deutsch, M. (1958). Trust and suspicion. Journal of conflict resolution, 2(4), 265-279.

Dirks, K. T., & Ferrin, D. L. (2002). Trust in leadership: Meta-analytic findings and implications for research and practice. Journal of applied psychology, 87(4), 611.

DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In Bitcoin and beyond (pp. 157-177). Routledge.

Elster, J. (1989). Nuts and bolts for the social sciences. Cambridge University Press.

Ennew, C., & Sekhon, H. (2007). Measuring trust in financial services: The trust index. Consumer Policy Review, 17(2), 62.

Espinal, R., Hartlyn, J., & Kelly, J. M. (2006). Performance still matters: Explaining trust in government in the Dominican Republic. Comparative Political Studies, 39(2), 200-223.

Falagas, M. E., Pitsouni, E. I., Malietzis, G. A., & Pappas, G. (2008). Comparison of PubMed, Scopus, web of science, and Google scholar: strengths and weaknesses. The FASEB journal, 22(2), 338-342.

Fogg, B. J. (2003). Prominence-interpretation theory: Explaining how people assess credibility online. In CHI'03 extended abstracts on human factors in computing systems, (pp. 722-723).

Freitag, M., & Traunmüller, R. (2009). Spheres of trust: An empirical analysis of the foundations of particularised and generalised trust. European journal of political research, 48(6), 782-803.

Friedlmaier, M., Tumasjan, A., & Welpe, I. M. (2018). Disrupting industries with blockchain: The industry, venture capital funding, and regional distribution of blockchain ventures. In Venture capital funding, and regional distribution of blockchain ventures. Proceedings of the 51st annual Hawaii international conference on system sciences (HICSS).

Fukuyama, F. (1995). Social capital and the global economy. Foreign Aff., 74, 89.

Funk, E., Riddell, J., Ankel, F., & Cabrera, D. (2018). Blockchain technology: a data framework to improve validity, trust, and accountability of information exchange in health professions education. Academic Medicine, 93(12), 1791-1794.

Gambetta, D., & Hamill, H. (2005). Streetwise: How taxi drivers establish customer's trustworthiness. Russell Sage Foundation.

Garfinkel, H. (1963). A conception of and experiments with “trust” as a condition of concerted stable actions. The production of reality: Essays and readings on social interaction, 381-392.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough?. Future Internet, 10(2), 20.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. Omega, 28(6), 725-737.

Ghode, D., Yadav, V., Jain, R., & Soni, G. (2020). Adoption of blockchain in supply chain: an analysis of influencing factors. Journal of Enterprise Information Management.

Giddens, A. (1990). The consequences of modernity. Cambridge: Polity Press

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

Greenhalgh, T., & Peacock, R. (2005). Effectiveness and efficiency of search methods in systematic reviews of complex evidence: audit of primary sources. Bmj, 331(7524), 1064-1065.

Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. Hastings Science & Technology Law Journal, 4, 160.

Grittersová, J. (2020). Foreign banks and sovereign credit ratings: Reputational capital in sovereign debt markets. European Journal of International Relations, 26(1), 33-61.

Gulati, R., & Sytch, M. (2008). Does familiarity breed trust? Revisiting the antecedents of trust. Managerial and Decision Economics, 29(2-3), 165-190.

Hanseth, O., & K. Lyytinen (2010). Design theory for dynamic complexity in information infrastructures: the case of building internet. Journal of Information Technology, 25(1), 1-19.

Hardin, R., & Offe, C. (1999). Democracy and trust. Cambridge University Press.

Harré, R. (1999). Trust and its surrogates: psychological foundations of political process. Democracy and trust, 249-272.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic commerce research and applications, 29, 50-63.

Hayes, S. C., Barnes-Holmes, D., & Roche, B. (2001). Relational frame theory: A post Skinnerian account of human language and cognition. New York: Kluwer, Academic/Plenum Publishers.

Hayes, S. C., Zettle, R. D., & Rosenfarb, I. (1989). Rule-following. In Rule-governed behavior (pp. 191-220). Springer, Boston, MA.

Ho, P. (2014). The 'credibility thesis' and its application to property rights:(In) secure land tenure, conflict and social welfare in China. Land Use Policy, 40, 13-27.

Ho, P. (2018). Institutional function versus form: The evolutionary credibility of land, housing and natural resources. Land use policy, 75, 642-650.

Ho, P., & Spoor, M. (2006). Whose land? The political economy of land titling in transitional economies. Land use policy, 23(4), 580-587.

Hodgson, G. M. (2006). What are institutions?. Journal of economic issues, 40(1), 1-25.

Hood, C., & Peters, G. (2004). The middle aging of new public management: into the age of paradox?. Journal of public administration research and theory, 14(3), 267-282.

Horvath, R., & Katuscakova, D. (2016). Transparency and trust: the case of the European Central Bank. Applied Economics, 48(57), 5625-5638.

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). Communication and persuasion.

Hsieh, Y. Y., Vergne, J. P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. Journal of Organization Design, 7(1), 1-16.

Hsu, C. L., & Lu, H. P. (2004). Why do people play on-line games? An extended TAM with social influences and flow experience. Information & management, 41(7), 853-868.

Hurley, R. F. (2012). The trustworthy leader: the first step toward creating high-trust organizations. Leader to leader, 66, 33-39.

Hurley, R. F. (2006). The decision to trust. Harvard business review, 84(9), 55-62.

Husted, B.W. and Folger, R. 2005. Fairness and transaction costs: The contribution of organizational justice theory to an integrative model of economic organization. Organization Science, 15(6): 719–29.

Ibarra, H., & Obodaru, O. (2016). Betwixt and between identities: Liminal experience in contemporary careers. Research in Organizational Behavior, 36, 47-64.

Igbaria, M., Iivari, J., & Maragahh, H. (1995). Why do individuals use computer technology? A Finnish case study. Information & management, 29(5), 227-238.

Inkpen, A. C., & Currall, S. C. (2001). Joint-venture trust: Inter-personal, inter-group and inter-firm levels.

Jackson, J., Bradford, B., Stanko, B., & Hohl, K. (2012). Just authority?: Trust in the police in England and Wales. Willan.

Jentzsch, N. (2016). Blockchain: Revolution der Finanzwelt?. DIW Wochenbericht, 83(29), 656-656.

Johnson-George, C., & Swap, W. C. (1982). Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other. Journal of personality and Social Psychology, 43(6), 1306.

Kaboolian, L. (1998). The new public management: Challenging the boundaries of the management vs. administration debate. Public Administration Review, 58(3), 189-193.

Kagan, R. A., & Scholz, J. T. (1984). The criminology of the corporation and regulatory enforcement strategies. Enforcing regulation, 67, 69-74.

Kelly, R. M. (1998). An inclusive democratic polity, representative bureaucracies, and the new public management. Public administration review, 58(3), 201-208.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.

Kramer, R. M. (2006). Organizational trust: A reader. Oxford University Press on Demand.

Kramer, R. M., & Tyler, T. R. (1995). Trust in organizations: Frontiers of theory and research. Sage Publications.

Kumlin, S. (2004). The personal and the political. In The personal and the political: How personal welfare state experiences affect political trust and ideology (pp. 3-19). Palgrave Macmillan, New York.

La Porte, T. R. (1994). Large technical systems, institutional surprises, and challenges to political legitimacy. Technology in Society, 16(3), 269-288.

La Porte, T. R., & Metlay, D. S. (1996). Hazards and institutional trustworthiness: Facing a deficit of trust. Public administration review, 341-347.

Lane, C. (1998). Introduction: Theories and issues in the study of trust. Trust within and between organizations: Conceptual issues and empirical applications, 1-30.

Lane, C., & Bachmann, R. (1996). The social constitution of trust: Supplier relations in Britain and Germany. Organization Studies, 17, 365–395.

Lane, C., & Bachmann, R. (1997). Co-operation in inter-firm relations in Britain and Germany: the role of social institutions. British Journal of Sociology, 226-254.

Lankton, N., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into Expectation Disconfirmation Theory. The Journal of Strategic Information Systems, 23(2), 128-145.

Leonhard, R. (2017). Corporate Governance on Ethereum's Blockchain. Available at SSRN 2977522.

Lessig, L. (2003). Law regulating code regulating law. Loy. U. Chi. LJ, 35, 1.

Lessig, L. (2006). Code. Version 2.0. New York: Basic Books.

Levi, M. (2006). Why we need a new theory of government. Perspectives on Politics, 4(1), 5-19.

Levi, M., & Stoker, L. (2000). Political trust and trustworthiness. Annual review of political science, 3(1), 475-507.

Lewenberg, Y., Sompolinsky, Y., & Zohar, A. (2015). Inclusive block chain protocols. In International Conference on Financial Cryptography and Data Security (pp. 528-547). Springer, Berlin, Heidelberg.

Lewis, J. D., & Weigert, A. J. (1985). Social atomism, holism, and trust. The sociological quarterly, 26(4), 455-471.

Lind, E. A., & Tyler, T. R. (1988). The social psychology of procedural justice. Springer Science & Business Media.

Lippert, S. K. (2007). Investigating postadoption utilization: an examination into the role of interorganizational and technology trust. IEEE Transactions on Engineering Management, 54(3), 468-483.

Lippert, S. K., & Forman, H. (2006). A supply chain study of technology trust and antecedents to technology internalization consequences. International Journal of Physical Distribution & Logistics Management.

Luhmann, N. (1979). Trust and power. New York: John Wiley & Sons.

Luhmann, N. (1988). Law as a social system. Nw. UL Rev., 83, 136.

Lumineau, F., & Oliveira, N. (2018). A pluralistic perspective to overcome major blind spots in research on interorganizational relationships. Academy of Management Annals, 12(1), 440-465.

Lumineau, F., & Oliveira, N. (2020). Reinvigorating the study of opportunism in supply chain management. Journal of Supply Chain Management, 56(1), 73-87.

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain governance - A new way of organizing collaborations?. Organization Science, 32(2), 500-521.

Lustig, C., & Nardi, B. (2015). Algorithmic authority: The case of Bitcoin. In 2015 48th Hawaii International Conference on System Sciences (pp. 743-752). IEEE.

Majchrzak, A., Jarvenpaa, S. L., & Bagherzadeh, M. (2015). A review of interorganizational collaboration dynamics. Journal of Management, 41(5), 1338-1360.

Manski, S. (2017). Building the blockchain world: Technological commonwealth or just more of the same?. Strategic Change, 26(5), 511-522.

Marien, S., & Werner, H. (2019). Fair treatment, fair play? The relationship between fair treatment perceptions, political trust and compliant and cooperative attitudes cross-nationally. European Journal of Political Research, 58(1), 72-95.

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. Social semiotics, 23(2), 261-277.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 20(3), 709-734.

Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

McCroskey, J. C., & Young, T. J. (1981). Ethos and credibility: The construct and its measurement after three decades. Communication Studies, 32(1), 24-34.

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. ACM Transactions on management information systems (TMIS), 2(2), 1-25.

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. International journal of electronic commerce, 6(2), 35-59.

McKnight, D. H., & Chervany, N. L. (2005). What builds system troubleshooter trust the best: experiential or non-experiential factors?. Information Resources Management Journal (IRMJ), 18(3), 32-49.

McKnight, D. H., & Chervany, N. L. (2006). Reflections on an initial trust-building model. Handbook of trust research, 29.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. The journal of strategic information systems, 11(3-4), 297-323.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. Academy of Management review, 23(3), 473-490.

McKnight, D. H., & Kacmar, C. J. (2007). Factors and effects of information credibility. In Proceedings of the ninth international conference on Electronic commerce, 423-432.

Mena, S., & Palazzo, G. (2012). Input and output legitimacy of multi-stakeholder initiatives. Business Ethics Quarterly, 22(3), 527-556.

Mendling, J., Weber, I., Aalst, W. V. D., Brocke, J. V., Cabanillas, C., Daniel, F., ... & Zhu, L. (2018). Blockchains for business process management-challenges and opportunities. ACM Transactions on Management Information Systems (TMIS), 9(1), 1-16.

Mickiewicz, T., Rebmann, A., & Sauka, A. (2019). To pay or not to pay? Business owners’ tax morale: Testing a neo-institutional framework in a transition environment. Journal of Business Ethics, 157(1), 75-93.

Miller, H., & Griffy-Brown, C. (2018). Developing a Framework and Methodology for Assessing Cyber Risk for Business Leaders. Journal of Applied Business & Economics, 20(3).

Mishler, W., & Rose, R. (1997). Trust, distrust and skepticism: Popular evaluations of civil and political institutions in post-communist societies. The journal of politics, 59(2), 418-451.

Mishra, A. K., & Mishra, K. E. (2013). The research on trust in leadership: The need for context. Journal of Trust Research, 3(1), 59-69.

Möllering, G. (2001). The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. Sociology, 35(2), 403-420.

Möllering, G. (2006). Trust: Reason, routine, reflexivity. Oxford: Elsevier.

Murphy, C. N. (2004). Global institutions, marginalization and development. Routledge.

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, (ja).

Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin. URL: https://bitcoin. org/bitcoin. pdf, 4.

Nesbitt, E. The Scope of Cryptocurrency in the Information Age. Security and Society, 179.

Nooteboom, B. (2007). Social capital, institutions and trust. Review of social economy, 65(1), 29-53.

North, D. C. (1990). A transaction cost theory of politics. Journal of theoretical politics, 2(4), 355-367.

North, D. C. (1998). Economic performance through time. The new institutionalism in sociology, 247.

O'Hara, K. (2012). Transparency, open data and trust in government: shaping the infosphere. In Proceedings of the 4th annual ACM web science conference (pp. 223-232).

Offe, C. (1999). How can we trust our fellow citizens. Democracy and trust, 52, 42-87.

Okhuysen, G. A., & Bechky, B. A. (2009). 10 coordination in organizations: An integrative perspective. Academy of Management annals, 3(1), 463-502.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 34(3), 355-364.

Orren, G. (1997). Fall from Grace: The Public's Loss of Faith in Government, in: Nye, J. S., Zelikov, P. D., King, D. C. (eds.): Why People don't trust government. Cambridge, 77 – 107.

Parasuraman, A. (2000). Technology Readiness Index (TRI) a multiple-item scale to measure readiness to embrace new technologies. Journal of service research, 2(4), 307-320.

Pariser, E. (2011). The filter bubble: What the Internet is hiding from you. Penguin UK.

Parmigiani, A., & Rivera-Santos, M. (2011). Clearing a path through the forest: A meta-review of interorganizational relationships. Journal of Management, 37(4), 1108-1136.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. Information systems research, 15(1), 37-59.

Pero, L. V., & Smith, T. F. (2008). Institutional credibility and leadership: critical challenges for community-based natural resource governance in rural and remote Australia. Regional Environmental Change, 8(1), 15-29.

Poppo, L., Zhou, K. Z., & Zenger, T. R. (2008). Examining the conditional limits of relational governance: specialized assets, performance ambiguity, and long-standing ties. Journal of Management Studies, 45(7), 1195-1216.

Pozen, D. E. (2018). Transparency's Ideological Drift. Yale LJ, 128, 100.

Rikken, O., Janssen, M., & Kwee, Z. (2019). Governance challenges of blockchain and decentralized autonomous organizations. Information Polity, 24(4), 397-417.

Riley, J. G. (2001). Silver signals: Twenty-five years of screening and signaling. Journal of Economic literature, 39(2), 432-478.

Roeck, D., Sternberg, H., & Hofmann, E. (2020). Distributed ledger technology in supply chains: a transaction cost perspective. International Journal of Production Research, 58(7), 2124-2141.

Rogers, E. M. (1995). Lessons for guidelines from the diffusion of innovations. The Joint Commission journal on quality improvement, 21(7), 324-328.

Rothschild, M. D., & J. E. Stiglitz. 1976. Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information. Quarterly Journal of Economics 90: 629-649

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. American psychologist, 26(5), 443.

Rotter, J. B., Chance, J. E., & Phares, E. J. (1972). Applications of a social learning theory of personality.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. Academy of management review, 23(3), 393-404.

Sas, C., & Khairuddin, I. E. (2015). Exploring trust in Bitcoin technology: a framework for HCI research. In Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (pp. 338-342).

Sas, C., & Khairuddin, I. E. (2017). Design for trust: An exploration of the challenges and opportunities of bitcoin users. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 6499-6510).

Sato, K. (1988). Trust and group size in a social dilemma. Japanese Psychological Research, 30(2), 88-93.

Schillewaert, N., Ahearne, M. J., Frambach, R. T., & Moenaert, R. K. (2005). The adoption of information technology in the sales force. Industrial marketing management, 34(4), 323-336.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. Academy of Management review, 32(2), 344-354.

Schuette, L. A. (2021). Forging unity: European commission leadership in the Brexit negotiations. JCMS: Journal of Common Market Studies.

Schutz, W. P. (1964). Banks and Other Financial Institutions; Stock Exchanges; and Business Regulation in General.

Seidel, M. D. L. (2018). Questioning centralized organizations in a time of distributed trust. Journal of Management Inquiry, 27(1), 40-44.

Seidel, M. D. L., & Greve, H. R. (2017). Emergence: How novelty, growth, and formation shape organizations and their ecosystems. In Emergence. Emerald Publishing Limited.

Sekhon, H., Ennew, C., Kharouf, H., & Devlin, J. (2014). Trustworthiness and trust: influences and implications. Journal of marketing management, 30(3-4), 409-430.

Self, C. C. (1996), "Credibility," in Michael B. Salwen & Don W. Stacks (Hrsg.), An Integrated Approach to Communication Theory and Research, (S. 421-441), Mahwah, Ill: Lawrence Erlbaum.

Shapiro, S. P. (1987). The social control of impersonal trust. American Journal of Sociology, 93, 623–658.

Sheppard, B. H., & Sherman, D. M. (1998). The grammars of trust: A model and general implications. Academy of management Review, 23(3), 422-437.

Simonite, T. (2016). Web pioneer tries to incubate a second digital revoluion. MIT Technology Review.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. Academy of management review, 17(1), 9-38.

Skinner, B. F. (1984). An operant analysis of problem solving. Behavioral and brain sciences, 7(4), 583-591.

Smith, M. L. (2010). Building institutional trust through e-government trustworthiness cues. Information Technology & People.

Smith, M. L. (2011). Limitations to building institutional trustworthiness through e-government: a comparative study of two e-services in Chile. Journal of Information Technology, 26(1), 78-93.

Söderlund, J., & Borg, E. (2018). Liminality in management and organization studies: Process, position and place. International Journal of Management Reviews, 20(4), 880-902.

Spence, M. (1973). Job market signaling, Quarterly Journal of Economics, 87(3), 355-374.

Steiner, J. (2012). The foundations of deliberative democracy: Empirical research and normative implications. Cambridge University Press.

Sztompka, P. (1999). Trust: A sociological theory. Cambridge university press.

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research commentary - Digital infrastructures: The missing IS research agenda. Information systems research, 21(4), 748-759.

Törneke, N., Luciano, C., & Salas, S. V. (2008). Rule-governed behavior and psychological problems. International Journal of Psychology and Psychological Therapy, 8(2), 141-156.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British journal of management, 14(3), 207-222.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

Tseng, S., & Fogg, B. J. (1999). Credibility and computing technology. Communications of the ACM, 42(5), 39-44.

Tullberg, J. (2008). Trust—The importance of trustfulness versus trustworthiness. The journal of socio-economics, 37(5), 2059-2071.

Tyler, T. R. (1997). The psychology of legitimacy: A relational perspective on voluntary deference to authorities. Personality and social psychology review, 1(4), 323-345.

Tyler, T. R., & Degoey, P. (1996). Trust in organizational authorities. Trust in organizations: Frontiers of theory and research, 331-356.

Tyler, T. R., & Lind, E. A. (1992). A relational model of authority in groups. Advances in experimental social psychology, 25, 115-191.

Van der Heijden, H. (2004). User acceptance of hedonic information systems. MIS quarterly, 695-704.

Van Dyne, L., Vandewalle, D., Kostova, T., Latham, M. E., & Cummings, L. L. (2000). Collectivism, propensity to trust and self-esteem as predictors of organizational citizenship in a non-work setting. Journal of organizational behavior, 21(1), 3-23.

Van Esterik-Plasmeijer, P. W., & Van Raaij, W. F. (2017). Banking system trust, bank trust, and bank loyalty. International Journal of Bank Marketing.

Van Ryzin, G. G. (2011). Outcomes, process, and trust of civil servants. Journal of Public Administration Research and Theory, 21(4), 745-760.

Wang, J., Wu, P., Wang, X., & Shou, W. (2017). The outlook of blockchain technology for construction engineering management. Frontiers of engineering management, 67-75.

Werbach, K. D. (2016). Trustless Trust. University of Pennsylvania, The Wharton School. Legal Studies & Business Ethics Department.

Williamson, O. E. (1985). The economic institutions of capitalism. New York: The Free Press.

Williamson, O. E. (1991). Economic institutions: Spontaneous and intentional governance. Journal of Law, Economics, & Organization, 7, 159-187.

Williamson, O. E. (1993). Calculativeness, trust, and economic organization. The journal of law and economics, 36(1, Part 2), 453-486.

Wilson, D., & Ateniese, G. (2015). From pretty good to great: Enhancing PGP using bitcoin and the blockchain. In

International conference on network and system security, (pp. 368-375). Springer, Cham.

Wong, W., & Welch, E. (2004). Does e-government promote accountability? A comparative analysis of website openness and government accountability. Governance, 17(2), 275-297.

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664.

Yamagishi, T., Cook, K. S., & Watabe, M. (1998). Uncertainty, trust, and commitment formation in the United States and Japan. American Journal of Sociology, 104(1), 165-194.

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. Organization science, 9(2), 141-159.

Zettle, R. D., & Hayes, S. C. (1982). Rule-governed behavior: A potential theoretical framework for cognitive–behavioral therapy. In Advances in cognitive–behavioral research and therapy, (pp. 73-118). Academic Press.

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial innovation, 2(1), 1-7.

Zhou, K. Z., & Xu, D. (2012). How foreign firms curtail local supplier opportunism in China: Detailed contracts, centralized control, and relational governance. Journal of International Business Studies, 43(7), 677-692.

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops, (pp. 180-184). IEEE.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. In B. M. Staw & L. L. Cummings (Eds.), Research in organizational behaviour, 8 (pp. 53–111). Greenwich, CT: JAI Press.

APPENDIX A

Characteristics that lead to evaluating the credibility of institutions have been considered repeatedly in the literature of social science. I present the procedures used to review this literature and address the challenges concerning the conceptual dispersion across fields. Specifically, I build on the procedure used by Oliveira and Lumineau (2018) in a prior review of the concept of the dark side in inter-organizational relationships. As I proceed in such a way, I increase the transparency of the review process (Tranfield, Denyer, and Smart, 2003) and guarantee that inter-field contributions are included (Ibarra, and Obodaru, 2016).

Step 1: Marking the boundaries of institutional credibility. I first search for conceptual and empirical articles that use the term “institutional credibility” in the domain of trust (108 articles in total). Starting from that pool of articles, I establish a variety of keywords by comparing my list of words against major conceptual pieces (e.g., Ho, 2018; Ho, 2013;

Pero, & Smith, 2008). As I proceed in this way, I capture exactly what has been meant in the literature as institutional credibility. Institutional credibility refers to the trustworthy properties that individuals or groups perceive and interpret as important cues to evaluate the work of institutions (Ho, 2014; Gambetta, & Hamill, 2005; Bacharach, & Gambetta, 2011; Offe, 1999; Sztompka, 1999; Zucker, 1986). Using the keyword "institutional credibility" together with other relevant keywords (such as functionality, accountability, shared rules, transparency, clarity, fairness, and justice), my initial search of Scopus data set yielded over 2,600 results. Compared to other databases, like PubMed and Web, I use Scopus because it covers a wider range of journals in the fields of social science (Falagas, Pitsouni, Malietzis, & Pappas, 2008). This allows me to have a more inclusive and multidisciplinary overview of the concept of institutional credibility. Following that approach, I find a set of synonyms ranging from formality to privatization, security, and legitimacy. These characteristics reflect the multifaceted aspect of the concept under study.

Step 2: Specifying the review scope. I restrict my search to a list of journals across fields of research. First, I identify a list of top-tier journals that publish empirical, conceptual, or review articles. I specifically focus on top-tier journals in general management, business ethics, political science, sociology, and economics. I capture different treatments of institutional credibility across multiple fields of research. I place no date restriction on my search; my time window in 1979 (the first search result available in Scopus) and ends in 2021. Table 1 shows how I build the set of keywords to reach saturation in the number of search results. To avoid contributions discussing institutional credibility only marginally, I apply more restrictive criteria: (1) focus on institutional credibility in economic life and (2) study of its characteristics. I code each article for relevance based on these criteria. With this approach, I ensure that my search retrieves relevant definitions and multiple forms concerning institutional credibility across diverse fields over time (e.g., sociology vs economics). I identify 291 initial results. Starting from this pool of studies, I use a snowball approach to track contributions not included in Scopus (Greenhalgh & Peacock, 2005). In the end, I obtain a total of 326 articles potentially manifesting the characteristics of institutional credibility. Among those, I select studies being published in highly ranked journals with impact factors approximately equal to or greater than 3 (Soderlund, and Borg, 2017; Aguinis, and Glavas, 2012). The final pool includes 116 relevant studies.

Word set	Rational	Search words	Results
1	To identify words that appear in the abstract of core conceptual pieces about institutional credibility	"persistence" OR "order" OR "function" OR "social support" OR "functional" OR "stability" OR "structural functionalism" OR "conflict resolution" OR "conflict prevention and management" AND "institutional credibility"	432
2	To identify words that appear in the definition of institutional credibility	"functionality" OR "interest" OR "immutability" OR "independence" OR	318

		"unintended intentionality" OR "appropriateness" OR "coherence" AND "institutional credibility"	
3	To identify words that appear in the definition of institutional credibility synonyms in the domain of trust	"privatization" OR "formality" OR "security" OR "legitimacy" OR "power" OR "authority" OR "reputation" OR "accreditation" OR "truth" AND "trust" AND "institution"	422
4	To identify words that quote institutional credibility and appear in the abstract of documents on trust	"accountability" OR "accountable" OR "shared rules" OR "transparency" OR "transparent" OR "clarity" OR "fairness" "fair" OR "justice" OR "functionality" OR "impartiality" OR "responsive" OR "structural assurance" OR "situation normality" AND "trust" AND "institution"	915
5	To identify synonyms of words in the set	"neutrality" OR "correctness" OR "reliability" OR "accuracy" OR "performance" OR "effectiveness" OR "effective" OR "procedural fairness" OR "distributive justice" OR "respect" OR "equity" OR "rightness" OR "objectivity" OR "consistency" OR "threat of sanction" OR "monitoring" AND "institutional credibility"	554

Table 1 – Saturation of words of characteristics of institutional credibility

Step 3: Manifesting the characteristics of institutional credibility.

Table 2 summarizes the main manifestation of institutional credibility.

I explore whether the manifestations focus on a single dimension versus multiple dimensions of institutional credibility. Evidence from this cross-disciplinary collection suggests that these manifestations often evoke similar meanings. In dealing with such a richness, I leverage on conceptual similarity in the meaning Such an approach has been widely employed in prior studies of literature review to redirect different manifestations into group categories from the viewpoint of tractability and parsimony (Majchrzak, Jarvenpaa, & Bagherzadeh, 2015; Parmigiani, & Rivera-Santos, 2011). As I inspect aspects in common that make one manifestation like another, I identify three group categories: functionality, fairness, and responsiveness. Each of these three categories is described by some unique elements paralleling also items used in the theory of rule-governed behavior to describe rule credibility (Hayes et al., 2001; Hayes, Zettle & Rosenfard, 1989; Zettle & Hayes, 1982; Skinner, 1966).

Functionality. A few authors conceptualize institutional credibility as the performance of various types of formal and informal institutions to reduce uncertainty and make possible regular economic interaction (van Esterik-Plasmeijer & van Raaij, 2017; Sekhon et al., 2014; Hurley, 2006, 2012; Bühlmann & Kunz, 2011; Espinal et al., 2006; Ho, 2006; Chanley et al., 2000; Mishler, & Rose, 1997; La Porte, & Metlay,1996; La Porte, 1994; North, 1990; Giddens, 1990). For example, studies that draw on the economic tradition focus on the level of performance. The level of performance is dependent on the structure and effectiveness of rules and their enforcement to convey human behavior to a specific social order (Ghode, 2020; Ho, 2016; King et al., 2012; Smith, 2011; Pavlou, & Gefen, 2004; Warren, 2004; 1999; Child, & Möllering, 2003; Arrighetti, Bachmann, & Deakin, 1997; Lane, & Bachmann, 1996; 1997). This implies that differences in economic success concern the pattern of correlations between the kind of institutional constraint and their level of effectiveness in practices. Finally, characteristics such as constancy, accuracy, and speed of feedback communicate those institutions operating to meet some specific standards in serving a purpose well (van Esterik-Plasmeijer & van Raaij, 2017; Child and Möllering, 2003; Arrighetti, Bachmann, & Deakin, 1997; Lane, & Bachmann, 1996; 1997)

Fairness. Some studies include additional aspects dealing with individual perceptions of procedural fairness and distributive justice. Procedural fairness concerns the process by which decisions are made, while distributive justice refers to the mode of resource allocation including the punishment of wrongs (Kumlin, 2004; Murphy, 2004; Levi, & Stoker, 2000; Sztompka, 1999; Levi, 1998; Lind & Tyler, 1988; Mishler, & Rose, 1997; Orren, 1997). These concepts are linked to the growing application of New Public Management (Hood, & Peters, 2004; Christensen, & Lægreid, 2002; Behn, 1998; Kaboolian, 1998; Kelly, 1998). In the same vein, other concepts have been introduced. They include neutrality, equity, impartiality, and transparency (de Blok & Kumlin, 2021; Marien & Werner, 2019; Mickiewicz, 2019; Creutzfeldt & Bradford, 2016; Mena & Palazzo, 2012; van Ryzin; 2011; Freitag, 2009; O'Hara, 2004; Botchway, 2001;

Tyler, 1997; Tyler, & Degoey, 1996; Tyler, & Lind, 1992; Luhmann, 1988; 1979; Zucker, 1986), transparency and accountability (e.g., Baker, 2007; Biermann, 2007; Pavlou, & Gefen, 2004; Warren, 2004) and moral concern (e.g., Baker, 2007; Biermann, 2007; Ennew & Sekhon, 2007; Ho, 2006), and formality, clarity, and correctness (Child, & Möllering, 2003; Arrighetti, Bachmann, & Deakin, 1997; Lane, & Bachmann, 1996; 1997; Giddens, 1990). The latter arises from the recent financial crisis which is essentially a macro-level trust crisis (Bachmann & Inkpenn, 2011).

Responsiveness. Several manifestations are confined to research studies because specific historical events occurred providing an idea for reflection and investigation. This is the case of the recent global economic crisis. The global economic crisis has highlighted the need to have more qualitative and responsive institutions which are capable to sustain individual responsibility and cooperation support at a given time and space (Arvanitidis, 2020; Funk et al., 2018; Pozen, 2018; King et al., 2012; Mena & Palazzo, 2012; van Ryzin; 2011; Baker, 2007; Biermann, 2007; Ennew & Sekhon, 2007; Ho, 2006; Braithwaite, 2003; Pavlou, 2002). For example, according to Ho (2014), it is the ability to provide permanent social support upon a shared moral purpose that makes institutions credible. Further, most recent scholars have proposed additional characteristics of institutional credibility like the attachment to practical strategies of commonwealth (Schuette, 2021; Ghode, 2020; Bargh et al., 2016; Horvath & Katuscakova, 2016; Sekhon et al., 2014; Smith, 2011; Biermann, 2007; Chanley et al., 2000; Tyler, 1997; Tyler, & Degoey, 1996; Tyler, & Lind, 1992) and flexibility to act and react in the face of major environmental changes that may compromise the actual social order (Arrighetti, Bachmann, & Deakin, 1997; Lane, & Bachmann, 1996; 1997).

Characteristics of institution's credibility	**Characteristics of technology's credibility**
Performance of delivering on promises and consistency (van Esterik-Plasmeijer & van Raaij, 2017; Sekhon et al., 2014; Hurley, 2006, 2012; Bühlmann & Kunz, 2011; Espinal et al., 2006; Ho, 2006; Chanley et al., 2000; Mishler, & Rose, 1997; La Porte, & Metlay,1996; La Porte, 1994; North, 1990; Giddens, 1990) Effectiveness (Ghode, 2020; Ho, 2016; King et al., 2012; Smith, 2011; Pavlou, & Gefen, 2004; Warren, 2004; 1999; Child, & Möllering, 2003; Arrighetti, Bachmann, & Deakin, 1997; Lane, & Bachmann, 1996; 1997) Constancy, accuracy, and speed of feedback (van Esterik-Plasmeijer & van Raaij, 2017; Child and Möllering, 2003; Arrighetti, Bachmann, & Deakin, 1997; Lane, & Bachmann, 1996; 1997)	Functionality
Neutrality, equity, and impartiality (de Blok & Kumlin, 2021; Marien & Werner, 2019; Mickiewicz, 2019; Creutzfeldt & Bradford, 2016; Mena & Palazzo, 2012; van Ryzin; 2011; Freitag, 2009; O'Hara, 2004; Botchway, 2001; Tyler, 1997; Tyler, & Degoey, 1996; Tyler, & Lind, 1992; Luhmann, 1988; 1979; Zucker, 1986) Formality, clarity, and correctness (Child, & Möllering, 2003; Arrighetti, Bachmann, & Deakin, 1997; Lane, & Bachmann, 1996; 1997; Giddens, 1990) Transparency and accountability	Fairness

(Schuette, 2021; Ghode, 2020; O'Brien, 2019; Funk et al., 2018; Pozen, 2018; Shambaugh & Shen, 2018; Grittersova, 2017; Bargh et al., 2016; Horvath & Katuscakova, 2016; King et al., 2012; Hurley, 2006, 2012; Bühlmann & Kunz, 2011; Smith, 2011; Carman, 2010; Biermann, 2007; Ennew & Sekhon, 2007; Meijer, 2007; Gelders, 2005; Bhatnagar, 2004; Kumlin, 2004; Murphy, 2004; Wong, & Welch, 2004; Bekkers, 2003; Weare, 2002; Botchway, 2001; Cukierman; 2000; Warren, 1999) Procedural fairness and distributive justice (Jackson et al., 2012; Hurley, 2006, 2012; Bühlmann & Kunz, 2011; Freitag, 2009; Espinal et al., 2006; Kumlin, 2004; Murphy, 2004; Chanley et al., 2000; Levi, & Stoker, 2000; Sztompka, 1999; Levi, 1998; Mishler, & Rose, 1997; Orren, 1997)	
Acting in the interests and respect (Schuette, 2021; Ghode, 2020; Bargh et al., 2016; Horvath & Katuscakova, 2016; Sekhon et al., 2014; Smith, 2011; Biermann, 2007; Chanley et al., 2000; Tyler, 1997; Tyler, & Degoey, 1996; Tyler, & Lind, 1992) Providing support (Arvanitidis, 2020; Funk et al., 2018; Pozen, 2018; King et al., 2012; Mena & Palazzo, 2012; van Ryzin; 2011; Baker, 2007; Biermann, 2007; Ennew & Sekhon, 2007; Ho, 2006; Braithwaite, 2003; Pavlou, 2002) Flexibility (Arrighetti, Bachmann, & Deakin, 1997; Lane, & Bachmann, 1996; 1997)	Responsiveness

Table 2 – Characteristics of institution's credibility

MEASURING TRUST IN CODE-BASED SYSTEM: SCALE DEVELOPMENT AND INITIAL TEST

Trust is increasingly being recognized as an important subject for academic research of blockchain-like technologies. However, empirical research in this area suffers from the lack of a validated scale to measure the antecedents, effects, and interacting factors of a code-based trust model regarding blockchain-mediated transactions. In this paper, I present a final twenty-six-item trust scale that encompasses key dimensions of the code-based trust model. Scale development involves three basic steps: item generation based on theoretical analysis of literature and pre-existing scales, testing and refinement using an on-line field survey, and psychometric analysis to assess the levels of reliability and validity. Results from psychometric analysis demonstrate that the proposed scale exhibits adequate levels of reliability and (convergent, discriminant, and nomological) validity.

Keywords: trust metrics, blockchain, code-based trust, scale development

INTRODUCTION

The call for additional research to explore how digital technologies offer novel routes around social phenomena has been echoed by scholars in organization studies (Lumineau et al., 2021; Hawlitschek et al., 2018; Seidel, 2018; Seidel, & Greve, 2017; Lachance, 2016; Mayer-Schonberger, & Cukier, 2013). Such calls, perhaps, have inspired a few field studies aimed at uncovering the implication of blockchain-like technologies for trust deficits (De Filippi et al., 2020;

Davidson et al., 2018; Hawlitschek et al., 2018). One area that has attracted significant research concerns replacing trust in people with trust in the rules-of-code (De Filippi et al., 2020; Sas, & Khairuddin, 2017; Lustig, & Nardi, 2015; Antonopoulos, 2014; Maurer et al., 2013). Trust in the rules-of-code is an important concept to characterize blockchain-mediated transactions between unknown traders under conditions of uncertainty and potential opportunism. It helps assure that the rules-of-code can perform important actions that limit opportunistic behaviors, minimize the need for an intermediary, and encourage long-term relationships (De Filippi et al., 2020; Lumineau et al., 2021; Davidson et al., 2018). Hence, building trust in the rules-of-code is important for the success of most digital transactions. It helps adopt a code-based trust behavior in which skepticism about another trader is suspended because the rules-of-code provide good motives to securely expect things to go well (De Filippi et al., 2020; Sas, & Khairuddin, 2017; Antonopoulos, 2014; Maurer et al., 2013).

However, little attention has been paid to the development of theoretically and empirically rigorous instruments to measure the components of a code-based trust model in the event of blockchain-mediated transactions. Survey-based studies of the blockchain (Al Khalil et al., 2017; Sas, & Khairuddin, 2017; Lustig, & Nardi, 2015) are neither theoretically derived, nor rigorously validated. They are specifically designed to target a first empirical exploration of users' general opinions about blockchain without being a point of reference about measurement. Prior trusting scales in the field of information technology, on the other hand, are hard to accommodate. They are related to individual expectations about the performance of a specific technology without considerations of micro-level factors (such as perceived characteristics of technology's credibility) that may influence the trust-building processes in the rules-of-code. Research moves head more quickly when a measurement system is well defined and corresponds to conceptual definitions (Schwab 1980; Kaplan 1964). In this study, I address this challenge by building on Sciarra (2022) code-based trust model as a theoretical basis. The model presents a view of several facets of code-based trust relationships such as trusting attitudes, beliefs, intentions, and behaviors. Because its purpose is to develop a complete model of code-based trust, it helps develop and validate a richer and holistic scale of code-based trust.

For scale development, I follow the process guidelines recommended by De Vellis, & Thorps (2021) including item selection, pretest, item refinement, and scale validation. Regarding item selection, I first determine clearly what it is you want to measure, articulating each construct through a systematic review of the literature. By systematically sampling the literature, I generate an item pool and define the item format. Next, the item pool is reviewed by expert judges for improvement. Thus, an initial scale is validated via a field survey involving a sampled panel of subjects that I identify through the Prolific platform. Within the field survey, subjects are presented with a realistic situation of online ticket reselling and requested to evaluate their level of trust when a blockchain-like technology is used to disintermediate the transaction. Based on responses received, a series of statistical tests are performed (factor analysis, Cronbach's alpha) to assess which combination of items constitutes a reliable unidimensional measure of each model construct. The final twenty-six-item scale demonstrates adequate psychometric properties regarding reliability, convergent and discriminant validity. Finally, I complete scale validation by testing for nomological validity. Estimates reveal that my scale gives accurate predictions to support the expected relations from the code-based trust model.

This study presents two-fold arguments for academic research. The proposed scale indeed addresses the lack of an empirically validated scale to measure trust in the face of code-based systems. Overall, I show that my scale provides a combination of conceptual clarity, reliability, and validity. In my view, this is one important step in empirical research to provide meaningful and accurate instruments for advancing empirical studies of trust in blockchain-mediated transactions. I expected that authors interested in researching trust in blockchain-mediated transactions may find my scale useful for conducting empirical studies. Also, I think that my scale can be extended to other types of technologies (such as artificial intelligence and machine learning, robotic process automation, edge computing) with appropriate adaptations. Second, this scale is a first attempt to support researchers and practitioners in assessing and measuring the effect of blockchain-like technologies on trust-building in process and user behavior. Since I evaluate the correspondence between the theoretical specification of the code-based trust model and empirical data, I test the model goodness-of-fit. Path coefficients and their significance help better understand which trusting dimensions matter most. Finally, for practice, I not only give an instrument measurement to uncover how people decide to be dependent on the rules-of-code, but also demonstrate the role of trust in the rule-code in encouraging users to engage in blockchain-mediated transactions with strangers.

The study is organized into three sections. I first present and theoretically discuss a model of code-based trust. Next, I describe in detail the procedures and methods I employed for developing an initial code-based trust scale. Finally, I illustrate the complete results of exploratory and confirmatory factor analysis and discuss my contributions.

THEORETICAL FOUNDATION

Definition of trust in the rules-of-code

In the realm of blockchain technology, trust in the rules-of-code has emerged as a novel concept to express the individual willingness to transact with one another by eliminating the need for prior mutual learning of real motives (De Filippi et al., 2020; Sas, & Khairuddin, 2017; Lustig, & Nardi, 2015; Antonopoulos, 2014; Maurer et al., 2013). The argumentation is grounded on the idea that transactional security can be achieved (most effectively) via dependability on the deterministic computation of the rules-of-code. The premise of blockchain is that the rules-of-code enable the secure exchange of valued assets over a decentralized, immutable, and public platform without the intervention of an intermediary or any prior assumptions about the reputation of a counterpart. They help mitigate the risk of opportunism that characterizes humanly devised relationships. It does not mean that the risk of a negative outcome is completely resolved, but there is a shift from people to the rules-of-code as the primary source of dependability. Because the blockchain platform processes important transactional data for a transaction to take place automatically, users are vulnerable to the actions of the rules-of-code. Some vulnerabilities (such as system misconfiguration, hacking, and privacy issues) may undermine the success of the transaction and cause harm (Manski, 2017; Sas, & Khairuddin, 2017). Hence, the need to trust the rules-of-code. Trust in the rules-of-code can be viewed as the individual psychological state to voluntarily depend on the rules-of-code, in a situation in which unexpected problems are possible (Sciarra, 2022).

By its very definition, the concept of trust in the rules-of-code is different from what literature on e-commerce has approached: trust toward a company providing products or services through an ecommerce platform vis à vis trust about a company providing a platform itself. Trust in the rules-of-code requires a consideration of the specific dimensions, causal relations, and context under study that goes beyond a model of trust which is mediated by reputation for a company providing an ecommerce platform. Focusing on the specific context of blockchain as institutional technology, Sciarra (2022)[1] presents a model of code-based trust. In the presentation of the model, the author builds on institution-based trust literature with the integration of the psychological theory of ruled-governed behavior. In integrating these streams of literature one to another, perceived characteristics of technology's credibility appear as an important dimension to capture the origins of trust in the rules-of-code as a state of mind which is developed over time in the face of a code-based system. These are used to represent trusting beliefs and explicate the formation of trust in the rules-of-code over time. The following figure depicts how these characteristics relate to the other trusting dimensions with a specification of causal relations between trust in the rules-of-code and its antecedents and outcomes in the context of blockchain-mediated transactions. A distinction between trusting beliefs, attitudes, intentions, and behaviors follows Mayer et al. (1995). Such a distinction is also helpful for the future development of a scale measurement.

[1] In Blockchain-based trust systems: an integrative model of how rules of code can build trust in digital economic transactions.

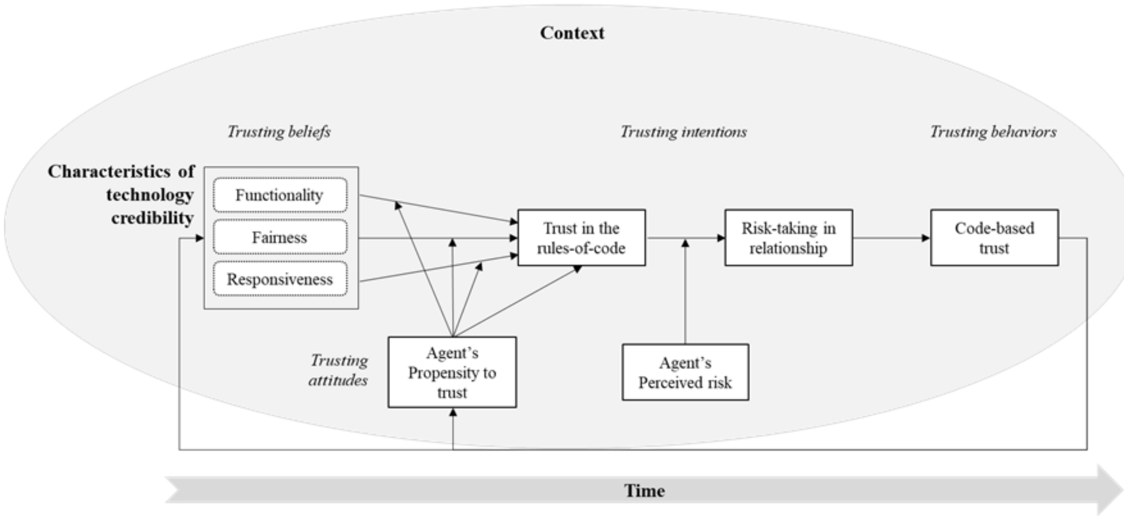

Figure 1 – Model of code-based trust

Dimensions of trust in the rules-of-code and causal relations

Trusting Beliefs. Trusting beliefs are perceptions about the credibility of a specific subject to provide important benefits to the trustor (McKnight, & Chervany, 2002, 2001; Mishra, 1996; Mayer et al., 1995). In the model of code-based trust, trusting beliefs indicate the extent to which one perceives, with feelings of relative security, that the rules-of-code possesses characteristics of technology credibility about being beneficial to the users. Three are the characteristics related to technology credibility in the domain of digital transactions. First, functionality means that the rules-of-code are suited to serve a purpose. The user would securely believe that the rules-of-code can provide proper and convenient safeguards in blockchain-mediated transactions. Second, fairness means that the rules-of-code apply an impartial and just treatment in computing blockchain-mediated transactions. This would reflect the belief that the rules-of-code operates in a customary situation of proper order. Third, responsiveness means that the rules-of-code can react positively to the need for achieving a successful exchange. This would mean that the rules-of-code are perceived to care about the individual and collective interests. High perceived functionality and responsiveness would be associated with a high level of structural assurance because the rules-of-code can protect one from frauds and losses, given other's harmful intentions (Manski, 2017; Sas, & Khairuddin, 2017). On the other hand, high perceived fairness would imply that the technology is appropriate, well ordered, and favorable for doing personal business in a normal situation. Thus, higher levels of perceived characteristics of technology credibility would encourage users to hold a secure willingness to depend on the rules-of-code of blockchain to execute safe and secure economic transactions within the digital environment.

Trusting Intentions. Trusting intentions are the expression of the willingness to depend on (Mcknight et al., 2002; 2001; 1998;). (Schoorman et al., 2007; McKnight, & Chervany, 2002, 2001; Rousseau et al., 1998; Mishra, 1996; Mayer et al., 1995; Davis et al. 1989). They correspond precisely to trust in the rules-of-code, as a volitional preparedness to engage in trust-related behaviors in a situation of risk (Coleman, 1990; Bierman, Bonini, & Hausman, 1969). In the context of digital transactions, such a willingness involves a subjective computation of probability that something could go wrong. The rules-of-code may disappoint the initial expectations because of some specific technology-related challenges. In the case of blockchain, these technology-related challenges concern the correct functioning and maintenance of the platform against system errors, data breaches, and hacking. Despite these tendencies to potentially cause loss or harm, the decision to trust the rules-of-code is influenced by the positive expectancy that the specific rules-of-code have enough safeguards. Thus, a user who trusts the rules-of-code is likely to believe that things will go well because the rules-of-code create guidelines that cannot be ignored.

Trusting Attitudes. People may hold different trust-building strategies about their propensity to trust (Van Dyne, Vandewalle, Kostova, Latham, & Cummings, 2000; Sato, 1988; Rotter, 1971). Propensity to trust is a personal attitude to display a general tendency to be willing to depend across a broad spectrum of situations (McKnight et al., 2001, 2002; Mayer et al., 1995). In the model of code-based trust, trusting attitudes define the users' natural inclination to believe that the rules-of-code are generally right, well-meaning, and dependable. They include two sub-constructs: personal innovativeness and experience with technology in general. Personal innovativeness is a trait depicting a general optimism regarding new ideas or technologies (Agarwal, & Prasad 1998). It is often observed characterizing individuals who are active information seekers and opinion leaders. Experience with technology in general, on the other hand, is the result of previous observation and direct training with other technological products, including evaluation in terms of usefulness and ease of use. A high level of satisfaction with these products also sustains a positive orientation toward the specific technology (Dutton, & Shepherd, 2006;

McKnight et al., 2002; Lewis et al., 2003; Agarwal, & Karahanna, 2000). For instance, some studies have shown that blockchain-mediated transactions are more welcomed by users with very advanced technological expertise (Manski, 2017; Sas, & Khairuddin, 2017; Lustig, & Nardi). In the end, a propensity to trust is expected to have a dual moderating effect, both on trusting beliefs and intentions directly.

Trusting Behaviors. Trusting behaviors are the outcome of individual intentions to trust. They go beyond the projection of an individual's future actions to capture a solid willingness to carry out specific actions that are important for the development of dependable interactions upon secure conditions (McKnight and Chervany, 2001, 2002). In the code-based trust model, trusting behaviors are defined as code-based trust, meaning that one feels secure about things because the rules-of-code mitigate the perceived risk of loss or harm involved in dealing with strangers. However, it is important to note that the transition from a trusting intention to behavior passes through evaluation of the residual risk which is context-specific. For example, all blockchain transactions are accompanied by the inherent risk of cyber security and privacy concerns, an unsettled regulatory environment, and decreased corporate accountability (Manski, 2017; Sas, & Khairuddin, 2017). This may encourage the counterpart to assume an opportunistic behavior, thus contravening the original objectives of blockchain to provide safeguards against malicious motives. If the level of trust in the rules-of-code surpasses perceived risk, then a blockchain user is prepared to pursue a not detrimental code-based conduct. And, if there exists a long-term good experience, that experience will sustain repeated code-based trusting behaviors over time (Sas, & Khairuddin, 2017; Lankton et al., 2014; McKnight et al., 2002). This just explains the backlink in Figure 1.

Other Trusting Enabling factors. The model presented above (Figure 1) includes other important trusting factors: time and context. Time is the dimension through which the way motion of trust in the rules-of-code is captured from one period to another. As time passes, changes in the level of each trusting dimension could be observed suggesting a dynamic nature of the code-based model. In the remainder of this study, I exclude time with no regard to the temporal frame. Since I am interested in describing a snapshot about initial trust in the rules-of-code, I focus on one period of time. Context, on the other hand, forms the setting for developing trust in the rules-of-code. It helps explain its formation in the light of some surrounding facts that include risk preference, technology acceptance, and societal factors. Risk preference reflects the individual disposition to engage in behaviors involving some potential for loss (Sitkin, & Pablo, 1992). This, in turn, influences the individual's willingness to take a risk. Next, technology acceptance models the intention to rely on a specific technology, based on a perception of usefulness and ease of use (Davis 1989). They are related to judgments about the quality of a specific technology to produce material results and be learned at low effort. Many studies (e.g., Manski, 2017; Sas, & Khairuddin, 2017) found that if the blockchain is perceived useful and easy to use in achieving a predetermined outcome, then trust in the rules-of-code is enhanced. Finally, factors like social trust are important to capture features of social life (Putnam, 1995). It is about the individual position towards the role of social institutions in reducing uncertainties and establishing stable social relations (Bachman & Inkpenn, 2011; Nooteboom, 2007). Optimistic evaluations of general institutions contribute to maintaining a trusted behavior even in face of any institutional arrangement like the rules-of-code, in the expectation that they can determine the rules of the game (Lessig, 2003; 2006).

Measurement of trust in the code-based system

While the code-based trust model depicted in Figure 1 is very informative, the measurement has not been addressed. Although many researchers in information technology have produced and validated diverse scale items for the study of trust within a technological environment, in my view they cannot be easily transferred to blockchain-mediated transactions. For example, some e-commerce researchers have measured trust in the online platform using a selection of human-like items (domain competence, fairness in the conduct, receptivity, and empathy to needs) as a representation of trusting beliefs (Venkatesh et al., 2011; Wang, & Benbasat, 2005; McKnight et al., 2002; Bhattacherjee, 2002). On this point, a few scholars observe that ascribing human-like traits as trusting beliefs is not appropriate to study trust in something that is naturally perceived as not human (Lankton et al., 2014; McKnight et al., 2011; McKnight et al., 2005). In this vein, Lippert (2001) has developed and validated a scale of 8 system-like items including question items of predictability, reliability, and utility. Yet, other scholars have proposed question items of usefulness and ease of use (Thatcher et al., 2011; McKnight, & Kacmar, 2007), functionality (Lankton et al. 2014; Thatcher et al., 2011), reliability (Lankton et al., 2014; Mcknight et al., 2011), transparency and accountability (Smith, 2011; 2010).

More recent explorative studies of blockchain have used a variety of sociotechnical items to measure the user's opinion. These items include impartiality, correctness, and increased control of information (Al Khail et al., 2017; Ahangama, & Poo, 2016; Lustig, & Nardi, 2015). Lusting, & Nardi (2015), for example, have found that question items about the evaluation of blockchain formal correctness help capture the users' willingness to rely on. Those studies, however, are in their infancy and do not always maintain rigor in developing a comprehensive measurement instrument. Specifically, they do not demonstrate adequate psychometric properties (including reliability, convergent and discriminant validity, and nomological validity), therefore limiting any effort to advance research. Given this lack of meaningful and accurate scale items, I develop and validate a scale survey of code-based trust which is derived from Sciarra (2022) model. I use Sciarra (2022) as a theoretical foundation for developing a revised scale within a context of code-based trust. The next section discusses the procedures for scale development and empirical results.

SCALE DEVELOPMENT

The section describes the methods I used to operationalize and validate psychometrically each model component of Figure 1 that I take as a theoretical reference. While different methods are available to measure trust (such as experiments, field interviews, surveys, analytical modeling, and approaches from cognitive neuroscience), a survey-based approach is the most frequently applied (Söllner et al., 2016; Schoorman et al., 2007; Cummings, & Bromiley, 1996; Rotter, 1967). Accordingly, I adopt a survey-based approach following the methodological guidelines provided by De Vellis, & Thorpe (2021) for scale development and initial test.

Item Selection

What we want to measure. The scale construction starts with narrowing the conceptual range of each construct. For each model component of Figure 1, I perform a content domain sampling of literature to select the best candidate items. Since I aim to have an inclusive and multidisciplinary overview on the topic, I largely survey the literature on the Scopus dataset to guarantee contributions from different domains. Following Söderlund, & Borg (2018), I search for documents, articles (and articles in press), reviews, books, and book chapters containing the words "institutional trust" and/or "technology trust" in the abstract, keywords, or title. I then filter by the area of research (Social Sciences, Business, Management and Accounting, and Psychology). To avoid marginal contributions, I then apply more restrictive criteria. I reduce the results only to documents containing words like "institutional technology", "computer-program procedure", “algorithm”, “rules-of-code”, “law code”, “technology and authority” “institutional trust”, “technology trust”, “technology credibility”, “technology perception”, “perceived technology”, “technology and functionality”, “technology and fairness” and “technology and responsiveness”. I collect a multitude of documents, which I analyze singularly to ensure their content is relevant for the present study. Starting from the remaining pool of articles, I deploy a snowball approach to track documents not included yet (Greenhalgh, & Peacock, 2005). My final sample contains a total of 30 documents (Table 1).

Studies	Focal items	Context
McKnight et al. (2002); Hsu et al. (2006) ; Kim et al. (2009)	Service level, performance	E-commerce
Bhattacherjee (2002)	Expertise, fairness, receptivity	E-commerce
Susarla et al. (2003); Suh et al. (1994); Szajna, & Scamell (2003)	Functional capability, technical service guarantees	Business application systems
Corritore et al. (2005)	Ease of use, reputation, honesty, predictability	E-commerce
Dutton, & Shepherd (2006)	Net-confidence, net-risk, proximity	Internet-based application
Lankton, & Wilson (2007)	Ease of use, usefulness, enjoyment, responsiveness, access	E-health
Lippert (2007; 2001); Lippert, & Forman (2006)	Predictability, functionality, reliability, utility	Collaborative visibility network in supply chain
McKnight, & Kacmar (2007)	Information credibility, usefulness,	Advice web site
Brown et al. (2008)	Ease of use, usefulness	Common banking system
Smith (2010; 2011)	Performance, aligned interests,	E-government

	transparency, accountability	
Venkatesh et al. (2011)	Usefulness, ease of use, facilitating conditions	E-government
Thatcher et al. (2011)	Ease of use, usefulness, functionality, predictability, helpfulness, self-efficacy	Knowledge management system
Lankton et al. (2014); McKnight et al. (2011)	Functionality, helpfulness, reliability	Strategic information system
Lustig, & Nardi (2015), Zarifis et al (2015), Ahangama, & Poo (2016); Craggs, & Rashid (2019)	Transparency, procedurality, reputation, self-imposed regulation	Blockchain-based payment systems
Al Khail et al. (2017)	Legal and formal correctness	Blockchain-based payment systems

Table 1 – Sample of trust measurement studies

An item pool. Based on evidence from the literature review, I identify an initial shortlist of 104 items that I group in four macro dimensions: trusting attitudes, trusting beliefs, trusting intentions, trusting behaviors and other trusting enabling factors. Table 2 illustrates that most items are adapted from existing scales. This includes items that are associated with constructs overlapping other studies. Items of personal innovativeness are adapted from Agarwal, & Prasad (1998), experience with technology from studies in information systems (Dutton, & Shepherd, 2006; McKnight et al., 2002; Lewis et al., 2003, Agarwal, & Karahanna, 2000), and code-based trust from studies in web-based applications (McKnight et al., 2007; McKnight et al., 2002; Jarvenpaa, & Tractinsky, 1999). Then, items of risk perceptions, technology acceptance, and societal trust are based on McKnight et al.

(2007; 2002), Davis (1989), World Values Survey, respectively. Original elaboration of items is created in lack of prior operational references. This specifically relates to trusting beliefs and intentions. Sciarra (2022) has introduced characteristics of technology credibility (functionality, fairness, and responsiveness) and trust in the rules-of-code as very novel concepts to academic research. Given, I characterize items following the exact definitions of Sciarra (2022).

Construct	**Scale Source**
Trusting attitudes	
Personal Innovativeness	Agarwal, & Prasad (1998)
Experience with technology	Dutton, & Shepherd (2006); McKnight et al. (2002); Lewis et al. (2003), and Agarwal, & Karahanna, (2000)
Trusting beliefs	
Functionality	Our original elaboration
Fairness	Our original elaboration
Responsiveness	Our original elaboration
Trusting intentions	
Trust in the rules-of-code	Our original elaboration
Trusting behaviors	
Code-based Trust	McKnight et al. (2007); McKnight et al. (2002); Jarvenpaa, & Tractinsky (1999)
Other trusting enabling factors	
Propensity to Risk	McKnight et al. (2007; 2002)
Technology Acceptance	Davis (1989)
Societal Trust	World Values Survey

Table 2 – Scale items of code-based trust system

The format for measurement. I present items as statements to evaluate in a questionnaire format. Because negative statements may reflect distrust, which is not the opposite of trust (Lewicki et al., 1998), I propose only positively worded statements. Among these, some statements are in fact attention checks to detect in advance respondents who pay insufficient attention (Meade & Craig, 2012; Kam & Meyer, 2015) or invest in low effort responding (Huang et al., 2012). Precisely the use of reverse-keyed statements helps mitigate the risk of accepting poorly meaningful measures at the validation stage. Responses to all statements are scaled using a typical five-level Likert format. They are built to vary in the degree of agreement or disagreement with each statement (i.e., “strongly disagree”, “disagree”, “neither agree nor disagree”, “agree” and “strongly agree”). As I am aware of potential distortions from several biases (for example, central tendency and social desirability bias), I avoid using extreme response categories and sentences having an institutionalized connotation.

Pretest and Item Refinement

Item pool reviewed by expert judges. The next goal is to refine the initial item pool and reduce items. Item refinement is done by involving experts (5 academicians and 4 IT practitioners to review the overall scale). I provide each expert with operational definitions of each model component and the initial scale items. Experts provided insightful comments for survey improvements regarding ambiguity in item wording, recommended changes, and item removal. Based on this feedback, I rephrase ten items for further clarity, and I drop several items to avoid redundancy. This leads to eighty scale items in total: 12- trusting attitudes items, 23- trusting beliefs items, 11- trusting intentions items, and 34- other trusting enabling factor items.

Scale Validation

The psychometric properties of scale are examined using Prolific (https://www.prolific.co/). Prolific is a flexible tool for online surveys which is an alternative to the MTurk platform. It helps recruit trusted participants for fair pay on voluntary participation. The pay is calculated automatically by the service provider, considering a minimum pay of £7.50/$9.60 per hour. Although this online mode is relatively new, it is increasingly being used for research purposes (Mellis, & Bickel, 2020; Hahl et al., 2018; Peer et al., 2017; Bucher et al., 2016; Lowry et al., 2016). Because respondents are generally comfortable with the internet in their everyday life and have general experience with an online survey, the risk of introducing any novelty bias on survey responses is low (Paolacci et al., 2010). Moreover, since the recent Covid-19 emergency, I have considered it appropriate to use.

Pilot test. The initial trust scale is administered to a random sample of thirty-one Prolific users. This group is 53 percent female, has a mean age of 25,4 years, subscribes to a wide range of professions (students, full-time job, part-time job, self-employed, unemployed, retired), and has a mean Prolific accuracy rate of 88,3. Information of accuracy rate is automatically calculated based on previous Prolific submissions, thus indicating respondents' reliability and honesty. To solicit participation in my survey, I enclose some useful information in the introductory message, such as the study objectives, the estimated time for completion (30 minutes), and the compensation rate (£3.75). The message also provides a hyperlink to my online survey form, including a declaration of compliance with General Data Protection Regulation (EU) 2016/679 about data processing.

First respondents are given a fictional scenario. I ask to imagine themselves being in a situation of ticket reselling, which is a typical scenario of risk of fraud. I propose Transtech as a blockchain-based application for secure ticket reselling which is not controlled by any company, unlike ecommerce platforms. A video tutorial of Transtech is made and tested with the purpose to provide an easy step-by-step guide to learn about Transtech and its features (i.e. immutability, decentralized technology, enhanced security, distributed ledgers, and faster settlement). Following a tour of Transtech, the survey form is presented. I add at the end of this survey an extra open-ended question for the purpose to collect general opinions about and suggestions of improvement. Subjects maintain a median duration of 24 minutes to complete the online survey. Responses to the open-ended question contain important indications to refine and streamline the initial survey form for the confirmatory study. They help resolve some residual ambiguity in item wording, revise the scale length, and confirm the adequacy of time for completion.

Confirmatory study. The subject sample consists of 300 randomly selected users from a stratified sample of U.S. participants (see Table 3). The respondent group is 51 percent female, has a mean age of 46 years, subscribes to a wide range of professions (students, full-time job, part-time job, self-employed, unemployed, retired), and has a mean Prolific accuracy rate of 611,3. Similar to the pilot study, a message introduces the confirmatory study, including information about the estimated time for completion (20 minutes) and the compensation rate (£2.50). I then proceed to present the same scenario of the pilot test before inviting respondents to complete the online survey form. As responses are returned, they are analyzed individually to reject those submissions that failed one or more attention checks. Failed submissions are then replaced with new submissions by other respondents until I target a total of 300 usable responses. In this confirmatory study, subjects maintain a median duration of 16,26 minutes.

Sex	**Female**			**Male**	
	153			147	
Age	**18-27**	**28- 37**	**38-47**	**48-57**	**58+**
	55	55	49	52	89
Ethnicity	**Asian**	**Black**	**Mixed**	**Other**	**White**
	25	45	15	10	205

Table 3 – Sample breakdown

DATA ANALYSIS AND RESULTS

Exploratory factor analysis

The first step in the evaluation of items is conducting an exploratory factor analysis to reduce the questionnaire into more manageable sub-themes which could explain the maximal amount of variance in responses. Those sub-themes identify the latent variables corresponding to abstract concepts of physical reality like behavioral or mental state. I employ the principal component analysis (PCA) with oblique rotation to infer those latent variables. I choose 0.40 (Mayers, 2013) and 1 (Kaiser, 1960) as the cut-off for loading factors and factor extraction, respectively. Factor reliability is measured using Cronbach's alpha. I consider values of 0.7 to 0.8 as being an acceptable level (Mayers, 2013). I use SPSS v.27 as a statistical software package for PCA and reliability tests.

To make sense of this exploratory analysis, I first test assumptions of correlation and multi-collinearity (Mayers, 2013). An examination of the correlation matrix demonstrates that I have a pretty good correlation; coefficients are mostly greater than 0.3 and none is above 0.80. The determinant table, on the other hand, shows that multi-collinearity is neither a concern because it exceeds 0.0001. Further, the main diagonal line of the anti-image correlation matrix confirms that correlation values are consistently above the threshold of 0.5. Finally, I obtain very good results (ranging between 0.8 and 0.9) for the Kaiser-Meyer-Olkin (KMO). I report in Appendix A evidence of these verification checks confirming that correlation and multi-collinearity are not a concern.

Table 4 illustrates some key results of this exploratory analysis. Items related to trusting attitudes are grouped into two factors: Personal Innovativeness (4 items, with 42.2% of explained variance) and Experience with technology (5 items, 18.9%). The two factors are tested for reliability, using Cronbach's alpha. Personal Innovativeness and Experience with technology show a Cronbach's alpha of .859 and .755, respectively. In the case of trusting beliefs, I obtain a total of 3 factors: Functionality (7 items, 58.7%), Fairness (6 items, 53.2%), and Responsiveness (7 items, 60.9%). The resulting three factors are tested for reliability. Functionality shows a very high internal consistency with an overall of .887. I observe that an increase of Cronbach's alpha to .905 is expected by removing one single item. The same is applied for Fairness (Cronbach's alpha = .85). I decide to remove two items from Fairness, resulting in a Cronbach's alpha of .886. Responsiveness has a Cronbach's alpha of .892 with no expected improvement from the removal of any items. For Trust in the rules-of-code and code-based Trust, I find one factor for each (5 items, 69.9%, and 4 items, 60.4% respectively). A reliability test shows a Cronbach's alpha of .503 and .813, respectively. Examination of Cronbach's alpha scores suggests that having five and four items, respectively, would enhance the internal consistency of Trust in the rules-of-code (Cronbach's alpha = .872) and code-based Trust (Cronbach's alpha = .834). Lastly, I treat the items about other trusting enabling factors in three separated groups. Risk propensity is composed of one factor (2 items, 64.5%) which is reliable at .816. Technology Acceptance counts of two initial factors: (2 items, 65.9%; Cronbach's alpha = .891), Ease of Use (2 items, 23.6%; Cronbach's alpha = .875). Societal Trust initially generates four factors. Evidence from the correlation matrix and Cronbach's alpha scores suggest that I would benefit from the removal of some items. After removing those poorly representative items, I end up with two factors: General Trust in others (11 items, 32,6%; Cronbach's alpha = .838) and General Trust in institutions (5 items, 18.4%; Cronbach's alpha = .905).

In conclusion, I obtain 10 factors for a total of 61 items representing the baseline to conduct Confirmatory Factor Analysis.

Construct	**Nr. Factor**	**Nr. Items**	**Tot. Variance explained**
Trusting attitudes			
Personal Innovativeness	1	4	
Experience with technology	1	5	
Trusting beliefs			
Functionality	1	7	58.735
Fairness	1	6	58.906
Responsiveness	1	6	60.887
Trusting intentions			
Trust in the rules-of-code	1	5	
Trusting behaviors			
Code-based Trust	1	4	60.431
Other trusting enabling factors			
Perceived Risk	1	4	
Technology Acceptance	2	2; 2	73.3; 75.104
Societal Trust	2	11; 5	

Table 4 – Final scale breakdown

Confirmatory factor analysis

Confirmatory factor analysis (CFA) is useful for scale validation in terms of convergent and discriminant validity. CFA uses structural equation modeling (SEM) to determine how well the anticipated model fits the real data according to some statistical criteria (Messick, 1998; Yang, 1998). It requires that some assumptions are met: i) a sufficient sample size (n >200), ii) data must come from a random sample, iii) data should have a multivariate normality distribution, and iv) the a priori model is correctly specified (χ^2 has $p \geq .05$). While my data meet assumptions i) and ii), I notice that the last two assumptions deserve much attention. Some items show skewness and kurtosis estimates slightly ranging outside the -2 to +2 interval, suggesting the potential departure of real data from the multivariate normality assumption. Because the multivariate assumption is not met, I obtain a default model which is incorrect (χ^2 = 3653.063; df = 1714; p = .000). I try to work around this problem by using bootstrap ML to resample the original dataset with normally distributed estimations (Tibshirani, & Efron,1993). This also produces benefits in terms of the correct a priori model specification. I configure the bootstrap on 2000 repetitions which is adequate to ensure meaningful statistics (Bollen, & Stine, 1993). The results of the Bollen-Stine bootstrapping method of χ^2 confirm that the model fits better in 2000 bootstrap samples (p = .000), meaning a good model.

We use AMOS as statistical software packages for CFA (Arbuckle, 2004; included in SPSS). Results are examined more in detail in the following sections.

Convergent validity. I evaluate convergent validity following Fornell and Larcker’s (1981) recommended criteria: i) factor loadings significantly exceeding 0.7, ii) construct reliabilities exceeding 0.8, and iii) average variance extracted (AVE) by each factor exceeding 0.5. In addition, I consider the Tucker–Lewis's index (TLI $\geq$ .95), the comparative fit index (CFI $\geq$ .95), and the root mean square error of approximation (RMSEA $\leq$ .05). As shown in Table 5, the initial estimates (χ^2 = 3795.873, df = 1774, Bollen-Stine bootstrap= 0.000) provide some poor results in terms of fit (TLI= 0.816, CFI= 0.828 and RMSEA= 0.062). This is due to the presence of items with factor loadings (λ) lower than 0.7, suggesting the removal of those items. As I remove those items, a twenty-six-item scale is obtained (see Appendix A). These items are explained more by their hypothesized reflective construct than by the error term (χ^2 = 405.42, df = 244, Bollen-Stine bootstrap= 0.004). As Table 6 illustrates, the criterion of factor loading (λ) is now met in all factors (the lowest λ value is 0.727, corresponding to items CBT4 and PT4). Cronbach's alphas range between 0.79 and 0.90. Next, the average variance extracted ranges between 0.58 and 0.78. Lastly, TLI, CFI, and RMSEA are 0.964, 0.975, and 0.044, respectively (see Table 5). I conclude all the scales sufficiently satisfy the norms for convergent validity.

Model tested	**$\chi 2$**	**df**	**B-S**	**TLI**	**CFI**	**RMSEA**
Initial model	3795.873	1774	0.000 (1)	0.816	0.828	0.062
Revised model	405.42	244	0.021 (2)	0.964	0.975	0.044
Goodness of fit	-	-	$\leq$ 0.05	$\geq$ 0.95	$\geq$ 0.95	$\leq$ 0.05

Table 5 – Goodness-of-fit statistics

(1) Bollen-Stine. The model fits better in 2000 bootstrap samples. It fits worse or fails to fit in 0 bootstrap samples. Testing the null hypothesis that the model is correct, p=0.000.

(2) Bollen-Stine. The model fits better in 1959 bootstrap samples. It fits worse or fails to fit in 41 bootstrap samples. Testing the null hypothesis that the model is correct, p=0.021.

Item		**Latent variable**	**λ**	**Prob. Level**	**Error variance**	**AVE**	**Root sq. AVE**
		Functionality				0.718	0.847
FU6	→		0.815	***	0.336		
FU5	→		0.879	***	0.227		
		Fairness				0.693	0.832
FA8	→		0.81	***	0.344		
FA6	→		0.855	***	0.269		
		Responsiveness				0.729	0.854
RE6	→		0.878	***	0.229		
RE5	→		0.829	***	0.312		
		Trust in the rules-of-code				0.65	0.806
TR6	→		0.87	***	0.243		
TR5	→		0.758	***	0.425		
TR1	→		0.786	***	0.382		
		Code-based trust				0.576	0.759
CBT5	→		0.803	***	0.355		
CBT4	→		0.727	***	0.471		
CBT1	→		0.745	***	0.445		
		Experience with technology				0.72	0.848
EXP6	→		0.849	***	0.279		
EXP7	→		0.848	***	0.28		
		Personal Innovativeness				0.679	0.824
INN4	→		0.727	***	0.471		
INN5	→		0.911	***	0.17		
		Technology Acceptance Model				0.78	0.882
TAM8	→		0.851	***	0.275		
TAM9	→		0.913	***	0.166		
		General trust in institutions				0.70	0.836
TRI14	→		0.816	***	0.334		
TRI12	→		0.809	***	0.345		
TRI13	→		0.883	***	0.22		
TRI15	→		0.834	***	0.304		

		General trust in others				0.755	0.87
TRO2	→		0.984	***	0.03		
TRO8	→		0.737	***	0.457		
		Risk Perception				0.729	0.854
RI3	→		0.848	***	0.281		
RI4	→		0.86	***	0.26		

Table 6 – Scalar estimates (Maximum Likelihood estimates)

Discriminant validity. I now come to assess discriminant validity. First, I compare the root square AVE and inter-factor correlations (Fornell, & Larcker, 1981) in conjunction with the heterotrait-monotrait ratio of correlations (HTMT) introduced by Henseler, Ringle, & Sarstedt (2015). The root square AVE ranges between 0.76 and 0.87, while inter-factor correlations are between 0.014 and 0.95 (see Table 6). The recommended approach is to verify that the lowest root square AVE (0.76) is greater than the largest correlation (0.95), meaning that the measures of constructs are statistically unrelated from one another (Fornell & Larcker, 1981). As shown in Table 7, I find that the criterion is violated in eight cases out of fifty-five pairs of latent variables.

Latent variable			**Corr.**		**Root sq. AVE**
FA	↔	RE	0.838	≥	**0.833 (FA)**
				≤	0.854 (RE)
FU	↔	FA	0.896	≥	**0.848 (FU)**
				≥	**0.833 (FA)**
FU	↔	RE	0.923	≥	**0.848 (FU)**
				≤	0.854 (RE)
TR	↔	RE	0.843	≥	**0.806 (TR)**
				≤	0.854 (RE)
TR	↔	FU	0.95	≥	**0.806 (TR)**

				≥	**0.848 (FU)**
TR	↔	CBT	0.922	≥	**0.806 (TR)**
				≥	**0.759 (CBT)**
CBT	↔	FU	0.87	≥	**0.759 (CBT)**
				≥	**0.848 (FU)**
CBT	↔	FA	0.808	≥	**0.759 (CBT)**
				≤	0.833 (FA)

Table 7 – Inter-factor correlation

Because such a comparison may suffer from sensitivity problems (Rönkkö, & Evermann, 2013), I run the supplementary HTMT test using the Adanco trial software (see http://www.henseler.com/htmt.html). The HTMT is a measure of similarity between latent variables, resulting from the computation of correlations of the observed variables. For each pair of latent variables, it requires values smaller than 0.85 to demonstrate that two latent variables represent different theoretical concepts. I observe that is true in each pair of latent variables, except for five pairs of latent variables (see Appendix B). In these pairs, the correlation coefficient tends to approach 1 leading to a potential upward bias in the measurement. For this reason, I look at HTMT2 (Henseler, 2021; Roemer, Schuberth, & Henseler, 2021). The latter test demonstrates that those five pairs are above the threshold again, thus reducing the overall level of discriminant validity. Finally, I use a χ^2 difference test by comparing the χ^2 statistic of the unconstrained model (all constructs are free to correlate; $\chi^2_{unconst}$ = 2014.29, df = 307) against the constrained model (χ^2_{const} = 405.42, df = 244). Since the difference in χ^2 between the unconstrained and constrained models ($\Delta\chi^2$ = 1608.87, Δdf = 63) is statistically significant (meaning the square-root value of AVE higher than inter-construct correlation at p = .000), I received confirmation of the presence of discriminant validity (see Table 8). All this together displays that discriminant validity is sufficiently adequate.

Model	**χ2**	**Df**	**Prob. level**
Constrained model	405,42	244	***
Unconstrained model	2014,29	307	***
Difference	1608,86	63	***

Table 8 – Chi-Square test

Nomological validity

We assess the nomological validity of the scale by testing the expected relations I discussed in the previous section. I test these relations collectively (see Figure 2), using structural equation modelling (SEM). Maximum likelihood estimates are provided.

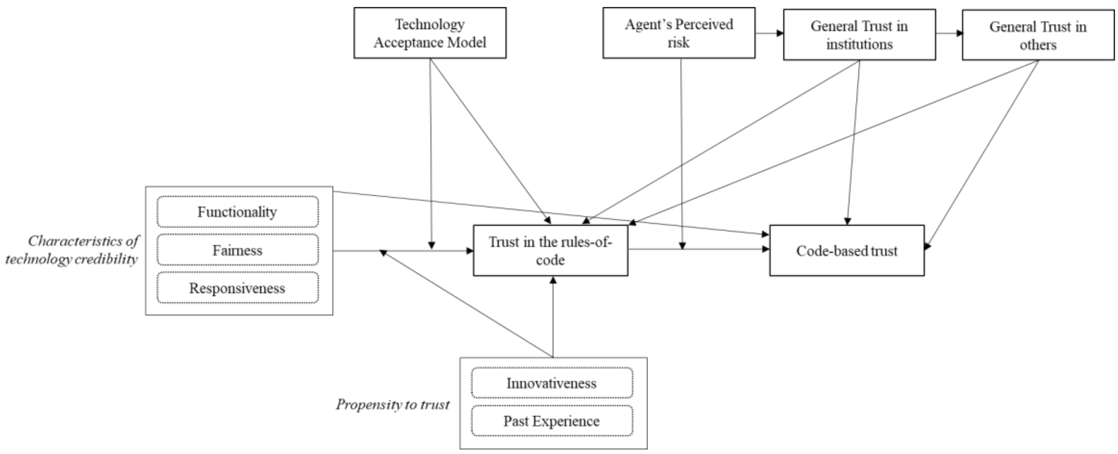

Figure 2 – Nomological model

We present the goodness of fit metrics, path coefficients, and path significance in Table 9.

			Estimate	S.E.	P-value
CR	←	FU	.446	.001	***
CR	←	FA	.423	.001	***
CR	←	RE	.44	.001	***
CR	←	INN	.001	.000	.097
CR	←	EXP	.000	.000	.303
CR	←	TAM	-.001	.000	.127
TR	←	CR	.628	.073	***
TR	←	INN	.07	.037	.092
TR	←	EXP	.169	.037	***
TR	←	TAM	.155	.044	.002
TR	←	RI	-.015	.034	.707
TR	←	TRI	.014	.034	.717
TR	←	TRO	.093	.032	.012
CBT	←	CR	.313	.061	***
CBT	←	TR	.448	.062	***
CBT	←	RI	.02	.042	.542
CBT	←	TRI	.052	.038	.21
CBT	←	TRO	.063	.042	.126
TRI	←	RI	-.117	.058	.042
TRO	←	TRI	.024	.057	***

Table 9 – Standardized regression weights

(1) Chi-square=520.896, df=43, p=0.000.
(2) Fit indices: NFI=0.888, CFI=0.896.

All the expected relations between items are supported at the 0.05 significance level. Functionality, fairness, and responsiveness are significant predictors of the characteristics of technology credibility (β = 0.446, 0.423, and 0.44, respectively). Characteristics of technology credibility are also a strong predictor of trust in the rules-of-code (β = 0.628). They indirectly affect (β = 0.313) the decision to develop code-based trust through the mediation of trust in the rules-of-code (β = 0.448). Regression weights appear to support the causal relations of the left side of the code-based trust model. Then, the agent's propensity to trust technology (experience with technology and personal innovativeness) (β = 0.169 and 0.07, respectively) is a positive moderating factor of the relationship between technology credibility and trust in the rules-of-code, even though the effect of personal innovativeness is marginally significant. This means, for example, that individuals who are more inclined to technology are more likely to allocate more trust in technology if technology is believed as credible. A similar inference is also true for technology acceptance, whereby high levels of perceived usefulness support beliefs of technology credibility and the willingness to trust. Technology acceptance has a significant positive effect on trust in the rules-of-code (β = 0.136). In the end, the other trusting enabling factors (risk perception, general trust in others, and trust in institutions) affect code-based trust through the following relation: risk perception → trust in institutions → general trust in others. I find that risk perception has a significant negative effect on trust in institutions (β = -0.117), while it is not statistically significant for general trust in others, trust in the rules-of-code, and code-based trust. Trust in general institutions mediates the relationship between risk perception and general trust in others (β = 0.024), but it does not have a significant direct effect on trust in the rules-of-code, and code-based trust. This means that individuals who are risk-takers value less the intervention of credible institutions as a guarantor, while they are more important for risk-averse individuals who are more suspicious in general and need structural assurance. Lastly, general trust in others affects the level of code-based trust (β = 0.057). From a conceptual point of view, those who show a high general trust in others are more engaged in trusting mechanisms.

DISCUSSIONS

In this study, I develop a final 26-item scale (see Appendix A) to operationalize trust in the context of blockchain-mediated transactions for potential use in future empirical studies. As discussed earlier, prior trust scales emphasize aspects that are not directly applicable to the blockchain setting. Based on Sciarra (2022), an initial 81-item trust scale in the context of blockchain-mediated ticket reselling is constructed. Field survey helps validate this scale by reducing it into a final scale demonstrating adequate properties and predictive ability. The development of this scale is part of a larger research question about the dynamics underlying the trust-building process within a digital environment. In view of these facts, this study offers important contributions for theory and practice.

First, I empirically test the expected relations of Sciarra's (2022) conceptual model of code-based trust. I show that characteristics of technology credibility are a significant predictor of trust in the rules-of-code as well as of the willingness to engage disintermediated transactions within a digital environment. This would suggest that the proposed scale is able to capture the relationship between the causes and outcome of trust in the rules-of-code. Second, I validate a measurement tool aimed to facilitate empirical research in the more general area of digital transactions. Although the proposed scale is designed in the context of blockchain-mediated transactions, it can be sufficiently generalized with reference to the property of external validity. The scale may be applied with adaptations to other situations and contexts where other institutional technologies are employed to reduce opportunistic behavior in economic transactions. Thus, I expect my trust scale may be used in future works aiming to evaluate how trust in the rules-of-code can impact the progress of digitally mediated transactions. Further, I think it may be also useful in comparative analysis between trust in the rules-of-code and trust in other people. Third, I support previous studies using crowdsourcing platforms (like Amazon Mechanical Turk and Prolific) to administer field surveys. I confirm that the utilization of these platforms is generally comfortable to respondents, without introducing bias or distorted measures.

Finally, from a practitioner standpoint, I find that trust in the rules-of-code appears to affect the willingness of users to make a disintermediated transaction. Thus, the development of practical strategies for introducing technology in mediating transactions should pass through the assessment of how users perceive technology itself. This suggests that some technology features deserve a greater attention during the design phase if the rules-of-code are to mediate important economic transactions. The benefits derived from early measurement of users' perceptions may help anticipate their future intentions for understanding issues, determining potential areas of low trust, and targeting special marketing campaigns or education initiatives to increase familiarity with technology.

This study presents a few limitations. First, the proposed scale yields a portion of unexplained variance. It suggests that the entire domain of trust in the rules-of-code might be not sufficiently represented in the proposed scale. Although I conduct extensive literature, other salient dimensions might be uncovered. I invite scholars to take on this challenge to carefully reconcile all dimensions of trust in the rules-of-code and examine their relevance also in different contexts through a larger population. In my view, a different context may represent potentially fruitful ways of identifying such additional dimensions. Authors may offer an empirical test of the model about people's attitudes and behaviors within a range of asset values. For example, people may develop different trusting levels depending on the value they assign to each specific asset under exchange (between over 800 euros of an international flight ticket and less than ten euros of a book). This may represent a step beyond thr initial test which is limited to one single asset value. I believe that authors may obtain nontrivial results when people are presented with different stakes. Second, I find that my scale performs not so well in discriminant validity. The analysis of psychometric properties shows that further item refinement is needed.

This especially concerns items of functionality and trust in the rules-of-code. I believe that future studies may provide alternative specifications of those items. One possible strategy is to adopt an inductive approach (Lin, & Hsieh, 2011; Kapuscinski, & Masters, 2010; Ladhari, 2010; Sharma, 2010; Sveinbjornsdottir, & Thorsteinsson, 2008) based on qualitative information obtained from interviews of the target population, expert panels, and forum (for example, BitcoinTalk.org, Reddit Forum, Ethereum.org). They may give more original and genuine information to distinguish one item from another compared to the most widely used deductive methods of literature review. Those additional items may, perhaps, consider any advantages and disadvantages of blockchain or more general institutional technology. Those items are expected to shed light on some nuances between different trusting levels.

REFERENCES

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. MIS quarterly, 665-694.

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. Information systems research, 9(2), 204-215.

Ahangama, S., & Poo, D. C. C. (2016). Credibility of Algorithm Based Decentralized Computer Networks Governing Personal Finances: The Case of Cryptocurrency. In International

Conference on HCI in Business, Government, and Organizations (pp. 165-176). Springer, Cham.

Al Khalil, F., Butler, T., O'Brien, L., & Ceci, M. (2017). Trust in smart contracts is a process, as well. In International Conference on Financial Cryptography and Data Security (pp. 510-519). Springer, Cham.

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.".

Arbuckle JL. Amos 5.0. SPSS; Chicago, IL: 2004.

Bachmann, R., & Inkpen, A. C. (2011). Understanding institutional-based trust building processes in inter-organizational relationships. Organization studies, 32(2), 281-301.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. Journal of management information systems, 19(1), 211-241.

Bierman, H., Jr., Bonini, C.P., & Hausman, W.H. (1969). Quantitative analysis for business decisions (3rd ed.). Homewood. IL; Irwin.

decisions (3rd ed.). Homewood. IL; Irwin.

Bollen, K. A., and Stine, R. A. (1993). "Bootstrapping Goodness-of-Fit Measures in Structural Equation Models," in Bollen, K. A., and Long, J. S. (Eds.) Testing Structural Equation Models, Newbury Park, CA: Sage, pp. 111--135.

Brown, S. A., Venkatesh, V., Kuruzovich, J., & Massey, A. P. (2008). Expectation confirmation: An examination of three competing models. Organizational Behavior and Human Decision Processes, 105(1), 52-66.

Bucher, E., Fieseler, C., & Lutz, C. (2019). Mattering in digital labor. Journal of Managerial Psychology.

Coleman, J. S. (1990). The Foundations of Social Theory. Cambridge, Mass: Harvard University Press.

Corritore, C. L., Marble, R. P., Wiedenbeck, S., Kracher, B., & Chandran, A. (2005). Measuring online trust of websites: Credibility, perceived ease of use, and risk.

Craggs, B., & Rashid, A. (2019, May). Trust beyond computation alone: Human aspects of trust in blockchain technologies. In 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS) (pp. 21-30). IEEE.

Cummings, L. L., & Bromiley, P. (1996). The organizational trust inventory (OTI). Trust in organizations: Frontiers of theory and research, 302(330), 39-52.

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, 14(4), 639-658.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, 101284.

DeVellis, R. F., & Thorpe, C. T. (2021). Scale development: Theory and applications. Sage publications.

Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology. Information, Communication & Society, 9(4), 433-451.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics.

Greenhalgh, T., & Peacock, R. (2005). Effectiveness and efficiency of search methods in systematic reviews of complex evidence: audit of primary sources. Bmj, 331(7524), 1064-1065.

Hahl, O., Kim, M., & Zuckerman Sivan, E. W. (2018). The authentic appeal of the lying demagogue: Proclaiming the deeper truth about political illegitimacy. American Sociological Review, 83(1), 1-33.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic commerce research and applications, 29, 50-63.

Henseler, J. (2021). Composite-based structural equation modeling: Analyzing latent and emer620 gent variables. Guilford Press.

Hsu, P. F., Kraemer, K. L., & Dunkle, D. (2006). Determinants of e-business use in US firms. International Journal of Electronic Commerce, 10(4), 9-45.

Huang, J. L., Curran, P. G., Keeney, J., Poposki, E. M., & DeShon, R. P. (2012). Detecting and deterring insufficient effort responding to surveys. Journal of Business and Psychology, 27(1), 99-114.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. Journal of Computer-Mediated Communication, 5(2), JCMC526.

Kam, C. C. S., & Meyer, J. P. (2015). How careless responding and acquiescence response bias can influence construct dimensionality: The case of job satisfaction. Organizational Research Methods, 18(3), 512-541.

Kaplan, A. The conduct of inquiry. San Francisco, Calif.:Chandler, 1964.

Kapuscinski, A. N., & Masters, K. S. (2010). The current status of measures of spirituality: A critical review of scale development. Psychology of Religion and Spirituality, 2(4), 191.

Kim, H. B., Kim, T. T., & Shin, S. W. (2009). Modeling roles of subjective norms and eTrust in customers' acceptance of airline B2C eCommerce websites. Tourism management, 30(2), 266-277.

Ladhari, R. (2010). Developing e-service quality scales: A literature review. Journal of retailing and consumer services, 17(6), 464-477.

Lankton, N., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into Expectation Disconfirmation Theory. The Journal of Strategic Information Systems, 23(2), 128-145.

Lankton, N. K., & Wilson, E. V. (2007). Factors influencing expectations of e-health services within a direct-effects model of user satisfaction. E-Service Journal, 5(2), 85-112.

Lessig, L. (2003). Law regulating code regulating law. Loy. U. Chi. LJ, 35, 1.

Lessig, L. (2006). Code. Version 2.0. New York: Basic Books.

Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998). Trust and distrust: New relationships and realities. Academy of management Review, 23(3), 438-458.

Lewis, W., Agarwal, R., & Sambamurthy, V. (2003). Sources of influence on beliefs about information technology use: An empirical study of knowledge workers. MIS quarterly, 657-678.

Lin, J. S. C., & Hsieh, P. L. (2011). Assessing the self-service technology encounters: development and validation of SSTQUAL scale. Journal of retailing, 87(2), 194-206.

Lippert, S. K. (2007). Investigating postadoption utilization: an examination into the role of interorganizational and technology trust. IEEE Transactions on Engineering Management, 54(3), 468-483.

Lippert, S. K. (2001). An exploratory study into the relevance of trust in the context of information systems technology. The George Washington University.

Lippert, S. K., & Forman, H. (2006). A supply chain study of technology trust and antecedents to technology internalization consequences. International Journal of Physical Distribution & Logistics Management.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. The Journal of Strategic Information Systems, 25(3), 232-240.

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain governance - A new way of organizing collaborations?. Organization Science, 32(2), 500-521.

Lustig, C., & Nardi, B. (2015). Algorithmic authority: The case of Bitcoin. In 2015 48th Hawaii International Conference on System Sciences (pp. 743-752). IEEE.

Manski, S. (2017). Building the blockchain world: Technological commonwealth or just more of the same?. Strategic Change, 26(5), 511-522.

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. Social semiotics, 23(2), 261-277.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 20(3), 709-734.

Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Mayers, A. (2013). Introduction to statistics and SPSS in psychology.

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. International journal of electronic commerce, 6(2), 35-59.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. The journal of strategic information systems, 11(3-4), 297-323.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. Academy of Management review, 23(3), 473-490.

McKnight, D. H., & Kacmar, C. J. (2007, August). Factors and effects of information credibility. In Proceedings of the ninth international conference on Electronic commerce (pp. 423-432).

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. ACM Transactions on management information systems (TMIS), 2(2), 1-25.

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. Psychological methods, 17(3), 437.

Mellis, A. M., & Bickel, W. K. (2020). Mechanical Turk data collection in addiction research: Utility, concerns and best practices. Addiction, 115(10), 1960-1968.

Messick, S. (1998). Test validity: A matter of consequence. Social Indicators Research, 45(1), 35-44.

Mishra, A. K. (1996). Organizational responses to crisis. Trust in organizations: Frontiers of theory and research, 261, 1996.

Nooteboom, B. (2007). Social capital, institutions and trust. Review of social economy, 65(1), 29-53.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on amazon mechanical turk. Judgment and Decision making, 5(5), 411-419.

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. Journal of Experimental Social Psychology, 70, 153-163.

Putnam, R. D. (1995). Tuning in, tuning out: The strange disappearance of social capital in America. PS: Political science & politics, 28(4), 664-683.

Roemer, E., Schuberth, F., & Henseler, J. (2021). HTMT2–an improved criterion for assessing discriminant validity in structural equation modeling. Industrial Management & Data Systems.

Rönkkö, M., & Evermann, J. (2013). A critical examination of common beliefs about partial least squares path modeling. Organizational Research Methods, 16(3), 425-448.

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. American Psychologist, 26(5), 443.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. Academy of Management Review, 23(3), 393-404.

Sato, K. (1988). Trust and group size in a social dilemma. Japanese Psychological Research, 30(2), 88-93.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. Academy of Management Review, 32(2), 344-354.

Sas, C., & Khairuddin, I. E. (2017). Design for trust: An exploration of the challenges and opportunities of bitcoin users. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 6499-6510).

Schwab, D. P. (1980). Construct validity in organizational behavior. Res Organ Behav, 2, 3-43.

Sciarra, M. (2022). Blockchain-based trust systems: an integrative model of how rules of code can build trust in digital economic transactions. In Sciarra, M., Doctoral Thesis: Trust who? And trust what? Reappraising central debates on trust in the era of digital economy.

Seidel, M. D. L. (2018). Questioning centralized organizations in a time of distributed trust. Journal of Management Inquiry, 27(1), 40-44.

Seidel, M. D. L., & Greve, H. R. (2017). Emergence: How novelty, growth, and formation shape organizations and their ecosystems. In Emergence. Emerald Publishing Limited.

Sharma, P. (2010). Measuring personal cultural orientations: Scale development and validation. Journal of the Academy of Marketing Science, 38(6), 787-806.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. Academy of management review, 17(1), 9-38.

Smith, M. L. (2011). Limitations to building institutional trustworthiness through e-government: a comparative study of two e-services in Chile. Journal of Information Technology, 26(1), 78-93.

Smith, M. L. (2010). Building institutional trust through e-government trustworthiness cues. Information Technology & People.

Söderlund, J., & Borg, E. (2018). Liminality in management and organization studies: Process, position and place. International Journal of Management Reviews, 20(4), 880-902.

Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. European Journal of Information Systems, 25(3), 274-287.

Sveinbjornsdottir, S., & Thorsteinsson, E. B. (2008). Adolescent coping scales: A critical psychometric review. Scandinavian journal of psychology, 49(6), 533-548.

Suh, K., Kim, S., & Lee, J. (1994). End-user's disconfirmed expectations and the success of information systems. Information Resources Management Journal (IRMJ), 7(4), 30-39.

Susarla, A., Barua, A., & Whinston, A. B. (2006). Understanding the 'service'component of application service provision: an empirical analysis of satisfaction with ASP services. Information systems outsourcing, 481-521.

Szajna, B., & Scamell, R. W. (1993). The effects of information system user expectations on their performance and perceptions. Mis Quarterly, 493-516.

Tibshirani, R. J., & Efron, B. (1993). An introduction to the bootstrap. Monographs on statistics and applied probability, 57, 1-436.

Van Dyne, L., Vandewalle, D., Kostova, T., Latham, M. E., & Cummings, L. L. (2000). Collectivism, propensity to trust and self-esteem as predictors of organizational citizenship in a non-work setting. Journal of organizational behavior, 21(1), 3-23.

Venkatesh, V., Thong, J. Y., Chan, F. K., Hu, P. J. H., & Brown, S. A. (2011). Extending the two-stage information systems continuance model: Incorporating UTAUT predictors and the role of context. Information Systems Journal, 21(6), 527-555.

Zarifis, A., Cheng, X., Dimitriou, S., & Efthymiou, L. (2015). Trust in Digital Currency Enabled Transactions Model. In MCIS (p. 3).

APPENDIX A

Scale Item Construct Measurement

Trusting Attitudes

1. On average, how many hours per week do you spend on each of the following activities? [None – > 10 hours]
   a. (INN3) - Reading blogs, magazines, and books about the latest tech news
   b. (INN4) - Following experts in the tech field
2. (EXP1) - If you heard about a new technology, how interested are you in experimenting with it?
   [Not interested at all – Very interested]
3. (EXP2) - Among your peers, how often are you the first to try out a new technological product?
   [Never – Always]

Trusting Beliefs

1. (FU5) - Transtech performs its role of giving appropriate safeguards to make secure trading.
   [Strongly disagree – Strongly disagree]
2. (FU6) - Transtech is a capable and proficient platform for ticket resale. [Strongly disagree – Strongly disagree]
3. (FA6) - I would characterize Transtech as truthful in dealing with trading facts. [Strongly disagree – Strongly disagree]

4. (FA8) - I would feel that meeting transparency requirements is at the foundation of Transtech.
   [Strongly disagree – Strongly disagree]
5. (RE5) - Transtech provides a valuable service within the secondary ticket market.
   [Strongly disagree – Strongly disagree]
6. (RE6) - If a user wants to avoid scams, Transtech can help meet this need. [Strongly disagree – Strongly disagree]

Trusting Intentions

1. (TR1) - I feel that I could count on Transtech to help with ticket trading. [Strongly disagree – Strongly disagree]
2. (TR5) - If it was possible, how likely it is that you might use Transtech also for other types of digital transactions?
   [Extremely unlikely – Extremely likely]
3. (TR6) - All in all, how would you place on this scale your willingness to rely on Transtech?
   [No willingness at all – A great deal of willingness]

Trusting Behaviors

1. (CBT1) - I would feel that most Transtech users act with the best intentions. [Strongly disagree – Strongly disagree]
2. (CBT4) - You would say that people using Transtech are:
   [Very untrustworthy – Very trustworthy]
3. (CBT5) - Taking all things together, how likely is it that Transtech may increase your trust in others during ticket resale?

[Extremely unlikely – Extremely likely]

Other Trusting Factors

1. (RI3) - Generally speaking, how would you place yourself on the following scale? (Risk Averse – Risk Propense)
2. (RI4) - Compared to the average person, I would say I take more risks (Strongly disagree – Strongly disagree)
3. (TAM7) - Transtech may enhance the effectiveness within the secondary ticket market. (Strongly disagree – Strongly disagree)
4. (TAM8) - Transtech may increase the success rate of ticket trading. (Strongly disagree – Strongly disagree)
5. (TRO2) - Generally speaking, how much do you trust people close to you?

   [Not trust at all – Trust completely]
6. (TRO8) - On average, how would you rate your relationship with close people?

   [Very bad – Very good]
7. If you had to give an opinion, how do you evaluate the actual commitment of government and public institutions in your country to: [Very negative – Very positive]
   a. (TRI1) - Maintain order and fight crime
   b. (TRI2) - Work for a more democratic society
   c. (TRI3) - Develop and promote the country wealth
   d. (TRI4) - Improve the quality of the health system

APPENDIX B

Exploratory Factorial Analysis

Trusting Attitudes

Personal Innovativeness

Correlation Matrix				
	INN1	INN2	INN3	INN4
INN1	1.000			
INN2	0.523	1.000		
INN3	0.582	0.668	1.000	
INN4	0.632	0.587	0.634	1.000
Kaiser-Meyer-Olkin Test				**0.81**
Bartlett Test	Chi-square			577.313
	df			6
	prob. Level			***
Covariance anti-image				
	INN1	INN2	INN3	INN4
INN1	0.538			
INN2	-0.062	0.502		
INN3	-0.107	-0.203	0.442	
INN4	-0.191	-0.105	-0.127	0.47
Correlation anti-image				
INN1	**0.83**			
INN2	-0.119	**0.812**		
INN3	-0.22	-0.432	**0.792**	
INN4	-0.38	-0.215	-0.279	**0.81**
Component Matrix				
INN1				**0.812**
INN2				**0.827**
INN3				**0.863**
INN4				**0.853**
	Initial Auto value			Total
Component	%Variance	%Cumulation		%Variance
1	70.375	**70.375**		70.375
2	12.688	83.063		
3	8.883	91.946		
4	8.054	100.000		
Cronbach’s alpha				**0.859**
Cronbach’s alpha if one item is quitted				
INN1				0.813
INN2				0.797
INN3				0.833
INN4				0.837

Personal Experience

Correlation Matrix						
	EXP1	EXP2	EXP3	EXP4	EXP5	EXP6
EXP1	1.000					
EXP2	0.696	1.000				
EXP3	0.346	0.3	1.000			
EXP4	0.361	0.276	0.473	1.000		
EXP5	0.283	0.249	0.377	0.447	1.000	
EXP6	0.231	0.249	0.164	0.112	0.177	1.000
Kaiser-Meyer-Olkin Test						**0.72**
Bartlett Test		Chi-square				471.012
		df				15
		prob. Level				***
Covariance anti-image						
	EXP1	EXP2	EXP3	EXP4	EXP5	EXP6
EXP1	0.476					
EXP2	-0.31	0.503				
EXP3	-0.055	-0.037	0.71			
EXP4	-0.09	0.006	-0.219	0.665		
EXP5	-0.024	-0.025	-0.126	-0.214	0.747	
EXP6	-0.04	-0.078	-0.048	0.028	-0.08	0.917
Correlation anti-image						
EXP1	0.663					
EXP2	-0.634	0.648				
EXP3	-0.095	-0.062	**0.803**			
EXP4	-0.16	0.01	-0.319	**0.745**		
EXP5	-0.04	-0.041	-0.173	-0.303	**0.793**	
EXP6	-0.061	-0.115	-0.059	0.035	-0.097	**0.857**
Component Matrix						
EXP1						**0.773**
EXP2						**0.729**
EXP3						**0.683**
EXP4						**0.691**
EXP5						**0.634**
EXP6						0.404

	Initial Auto value		Total
Component	%Variance	%Cumulation	%Variance
1	43.963	**43.963**	43.963
2	17.895	61.858	
3	14.507	76.365	
4	10.292	86.658	
5	8.399	95.057	
6	4.943	100.000	
Cronbach’s alpha			**0.729**

Cronbach's alpha if one item is quitted	
EXP1	0.638
EXP2	0.655
EXP3	0.690
EXP4	0.696
EXP5	0.704
EXP6	**0.755**

* Trusting Attitude items originally included two other items, for a total of twelve items. They were included to introduce respondents more easily to this block of questions. I decide therefore to remove those two from the statistical analysis.

Trusting Beliefs

Functionality

Correlation Matrix								
	FU1	FU2	FU3	FU4	FU5	FU6	FU7	FU8
FU1	1.000							
FU2	0.609	1.000						
FU3	0.525	0.599	1.000					
FU4	0.532	0.606	0.754	1.000				
FU5	0.593	0.602	0.673	0.714	1.000			
FU6	0.611	0.594	0.568	0.593	0.716	1.000		
FU7	0.457	0.448	0.475	0.475	0.614	0.563	1.000	
FU8	0.308	0.318	0.276	0.256	0.343	0.281	0.243	1.000
Kaiser-Meyer-Olkin Test							**0.91**	
Bartlett Test			Chi-square				1301.91	
			df				28	
			prob. Level				***	
Covariance anti-image								
	FU1	FU2	FU3	FU4	FU5	FU6	FU7	FU8
FU1	0.506							
FU2	-0.133	0.47						
FU3	-0.022	-0.065	0.375					
FU4	-0.013	-0.059	-0.168	0.34				
FU5	-0.036	-0.015	-0.052	-0.092	0.304			
FU6	-0.102	-0.066	-0.008	-0.016	-0.115	0.403		
FU7	-0.031	-0.011	-0.02	-0.003	-0.112	-0.084	0.586	
FU8	-0.057	-0.066	-0.018	0.027	-0.066	0.008	-0.013	0.853
Correlation anti-image								
FU1	**0.929**							
FU2	-0.273	**0.931**						
FU3	-0.051	-0.154	**0.893**					
FU4	-0.03	-0.149	-0.469	**0.879**				

FU5	-0.093	-0.04	-0.153	-0.286	**0.896**			
FU6	-0.226	-0.151	-0.021	-0.042	-0.33	**0.915**		
FU7	-0.056	-0.021	-0.042	-0.007	-0.265	-0.173	**0.939**	
FU8	-0.087	-0.104	-0.032	0.05	-0.129	0.013	-0.018	**0.938**
Component Matrix								
FU1								**0.765**
FU2								**0.792**
FU3								**0.815**
FU4								**0.83**
FU5								**0.877**
FU6								**0.822**
FU7								**0.703**
FU8								0.44
				Initial Auto value				Total
Component			%Variance		%Cumulation			%Variance
1			58.735		**58.735**			58.735
2			10.698		69.433			
3			7.948		77.381			
4			7.152		84.532			
5			4.911		89.443			
6			4.544		93.987			
7			3.219		97.206			
8			2.794		100.000			
Cronbach's alpha								**0.887**
Cronbach's alpha if one item is quitted								
FU1								0.872
FU2								0.868
FU3								0.866
FU4								0.864
FU5								0.859
FU6								0.866
FU7								0.88
FU8								**0.905**

Fairness (1)

Correlation Matrix								
	FA1	FA2	FA3	FA4	FA5	FA6	FA7	FA8
FA1	1.000							
FA2	0.569	1.000						
FA3	0.494	0.626	1.000					
FA4	0.467	0.572	0.61	1.000				
FA5	0.298	0.366	0.288	0.495	1.000			
FA6	0.552	0.603	0.555	0.603	0.446	1.000		

FA7	0.171	0.24	0.241	0.247	0.209	0.297	1.000	
FA8	0.5	0.559	0.555	0.533	0.419	0.693	0.312	1.000
Kaiser-Meyer-Olkin Test								**0.894**
Bartlett Test			Chi-square					1025.954
			df					28
			prob. Level					***
Covariance anti-image								
	FA1	FA2	FA3	FA4	FA5	FA6	FA7	FA8
FA1	0.588							
FA2	-0.129	0.457						
FA3	-0.05	-0.136	0.474					
FA4	-0.026	-0.057	-0.147	0.46				
FA5	0.002	-0.031	0.075	-0.17	0.697			
FA6	-0.088	-0.064	-0.021	-0.08	-0.06	0.394		
FA7	0.032	-0.016	-0.025	-0.015	-0.042	-0.044	0.881	
FA8	-0.05	-0.038	-0.078	-0.01	-0.069	-0.166	-0.077	0.448
Correlation anti-image								
FA1	**0.925**							
FA2	-0.249	**0.907**						
FA3	-0.095	-0.292	**0.879**					
FA4	-0.051	-0.125	-0.316	**0.885**				
FA5	0.003	-0.054	0.131	-0.3	**0.873**			
FA6	-0.183	-0.152	-0.049	-0.187	-0.115	**0.887**		
FA7	0.045	-0.025	-0.038	-0.023	-0.053	-0.075	**0.939**	
FA8	-0.097	-0.085	-0.169	-0.021	-0.124	-0.395	-0.122	**0.892**
Component Matrix								
FA1								**0.714**
FA2								**0.804**
FA3								**0.775**
FA4								**0.797**
FA5								0.59
FA6								**0.839**
FA7								0.406
FA8								**0.804**
				Initial Auto value				Total
Component			%Variance		%Cumulation			%Variance
1			53.182		**53.182**			53.182
2			11.282		64.464			
3			9.761		74.225			
4			6.974		81.199			
5			6.195		87.394			
6			4.815		92.209			
7			4.295		96.504			
8			3.496		100.000			

Cronbach's alpha	**0.85**
Cronbach's alpha if one item is quitted	
FA1	0.833
FA2	0.821
FA3	0.825
FA4	0.82
FA5	0.845
FA6	0.816
FA7	**0.88**
FU8	0.818

Fairness (2)

Correlation Matrix							
	FA1	FA2	FA3	FA4	FA5	FA6	FA8
FA1	1.000						
FA2	0.569	1.000					
FA3	0.494	0.626	1.000				
FA4	0.467	0.572	0.61	1.000			
FA5	0.298	0.366	0.288	0.495	1.000		
FA6	0.552	0.603	0.555	0.603	0.446	1.000	
FA8	0.5	0.559	0.555	0.533	0.419	0.693	1.000
Kaiser-Meyer-Olkin Test						**0.888**	
Bartlett Test		Chi-square				989.842	
		df				21	
		prob. Level				***	
Covariance anti-image							
	FA1	FA2	FA3	FA4	FA5	FA6	FA8
FA1	0.59						
FA2	-0.129	0.457					
FA3	-0.05	-0.137	0.475				
FA4	-0.026	-0.057	-0.148	0.46			
FA5	0.003	-0.032	0.074	-0.171	0.699		
FA6	-0.087	-0.066	-0.023	-0.081	-0.063	0.396	
FA8	-0.048	-0.04	-0.081	-0.011	-0.074	-0.173	0.454
Correlation anti-image							
FA1	**0.926**						
FA2	-0.248	**0.903**					
FA3	-0.094	-0.293	**0.874**				
FA4	-0.05	-0.125	-0.317	**0.88**			
FA5	0.005	-0.056	-0.129	-0.301	**0.867**		
FA6	-0.18	0.154	-0.052	-0.189	-0.119	**0.88**	
FA8	-0.092	-0.089	-0.175	-0.024	-0.131	-0.408	**0.886**
Component Matrix							

FA1			**0.724**
FA2			**0.81**
FA3			**0.779**
FA4			**0.801**
FA5			0.59
FA6			**0.839**
FA8			**0.801**
	Initial Auto value		Total
Component	%Variance	%Cumulation	%Variance
1	58.906	**58.906**	58.906
2	11.391	70.297	
3	7.971	78.268	
4	7.321	85.589	
5	5.506	91.095	
6	4.909	96.004	
7	3.996	100.000	
Cronbach's alpha			**0.88**
Cronbach's alpha if one item is quitted			
FA1			0.869
FA2			0.856
FA3			0.861
FA4			0.856
FA5			**0.886**
FA6			0.851
FA8			0.857

Responsiveness

Correlation Matrix							
	RE1	RE2	RE3	RE4	RE5	RE6	RE7
RE1	1.000						
RE2	0.6	1.000					
RE3	0.642	0.626	1.000				
RE4	0.545	0.451	0.63	1.000			
RE5	0.501	0.343	0.463	0.509	1.000		
RE6	0.532	0.401	0.526	0.615	0.728	1.000	
RE7	0.51	0.445	0.509	0.482	0.67	0.677	1.000
Kaiser-Meyer-Olkin Test						**0.877**	
Bartlett Test		Chi-square				1143.888	
		df				21	
		prob. Level				***	
Covariance anti-image							
	RE1	RE2	RE3	RE4	RE5	RE6	RE7
RE1	0.461						

RE2	-0.157	0.544					
RE3	-0.116	-0.142	0.42				
RE4	-0.049	-0.017	-0.149	0.482			
RE5	0.052	0.038	-0.003	-0.022	0.403		
RE6	-0.027	0.007	-0.012	-0.12	-0.158	0.348	
RE7	-0.023	-0.07	-0.039	-0.016	-0.137	-0.113	0.44
Correlation anti-image							
RE1	**0.903**						
RE2	-0.312	**0.868**					
RE3	-0.263	-0.298	**0.875**				
RE4	-0.104	-0.033	-0.331	**0.894**			
RE5	-0.121	-0.08	-0.006	-0.051	**0.856**		
RE6	-0.069	0.15	-0.03	-0.292	-0.421	**0.856**	
RE7	-0.051	-0.143	-0.09	0.035	-0.324	-0.288	**0.894**
Component Matrix							
RE1							**0.792**
RE2							**0.693**
RE3							**0.801**
RE4							**0.777**
RE5							**0.776**
RE6							**0.827**
RE7							**0.789**
			Initial Auto value				Total
Component			%Variance	%Cumulation			%Variance
1			60.887	**60.887**			60.887
2			13.192	74.08			
3			7.807	81.887			
4			5.523	87.41			
5			4.767	92.177			
6			4.242	96.419			
7			3.581	100.000			
Cronbach's alpha							**0.892**
Cronbach's alpha if one item is quitted							
RE1							0.873
RE2							0.887
RE3							0.872
RE4							0.876
RE5							0.878
RE6							0.87
RE7							0.875

Trusting Intentions

Trust in the rules-of-code

Correlation Matrix						
	TR1	TR2	TR3	TR4	TR5	TR6
TR1	1.000					
TR2	0.52	1.000				
TR3	0.692	0.611	1.000			
TR4	-0.482	-0.509	-0.742	1.000		
TR5	0.461	0.388	0.551	-0.472	1.000	
TR6	0.569	0.494	0.655	-0.528	0.732	1.000
Kaiser-Meyer-Olkin Test						**0.835**
Bartlett Test		Chi-square				1079.57
		df				15
		prob. Level				***
Covariance anti-image						
	TR1	TR2	TR3	TR4	TR5	TR6
TR1	0.483					
TR2	-0.08	0.592				
TR3	-0.148	-0.086	0.263			
TR4	-0.046	0.055	0.182	0.435		
TR5	-0.009	0.015	-0.017	0.037	0.451	
TR6	-0.062	-0.051	-0.057	0.08	-0.23	0.357
Correlation anti-image						
TR1	**0.87**					
TR2	-0.151	**0.932**				
TR3	-0.414	-0.217	**0.797**			
TR4	-0.1	0.109	0.537	**0.829**		
TR5	-0.02	0.029	-0.05	0.084	**0.807**	
TR6	-0.15	-0.111	-0.187	0.021	-0.574	**0.819**
Component Matrix						
TR1						**0.78**
TR2						**0.729**
TR3						**0.897**
TR4						-0.783
TR5						**0.751**
TR6						**0.835**
			Initial Auto value			Total
Component			%Variance	%Cumulation		%Variance
1			63.661	**63.661**		63.661
2			12.232	75.893		
3			8.826	84.719		
4			7.945	92.665		
5			4.179	96.844		
6			3.156	100.000		
Cronbach’s alpha						**0.54**

Cronbach's alpha if one item is quitted	
TR1	0.348
TR2	0.359
TR3	0.312
TR4	**0.862**
TR5	0.332
TR6	0.281

Trusting Behaviors

Code-based Trust

Correlation Matrix					
	CBT1	CBT2	CBT3	CBT4	CBT5
CBT1	1.000				
CBT2	0.438	1.000			
CBT3	0.608	0.365	1.000		
CBT4	0.636	0.399	0.495	1.000	
CBT5	0.578	0.409	0.543	0.535	1.000
Kaiser-Meyer-Olkin Test					**0.845**
Bartlett Test		Chi-square			544,202
		df			10
		prob. Level			***
Covariance anti-image					
	CBT1	CBT2	CBT3	CBT4	CBT5
CBT1	0.444				
CBT2	-0.089	0.756			
CBT3	-0.166	-0.044	0.566		
CBT4	-0.185	-0.075	-0.055	0.54	
CBT5	-0.105	-0.099	-0.14	-0.113	-0.211
Correlation anti-image					
CBT1	**0.802**				
CBT2	-0.154	**0.909**			
CBT3	-0.331	-0.068	**0.849**		
CBT4	-0.379	-0.117	-0.099	**0.84**	
CBT5	-0.211	-0.151	-0.248	-0.205	**0.864**
Component Matrix					
CBT1					**0.853**
CBT2					0.644
CBT3					**0.782**
CBT4					**0.798**
CBT5					**0.795**
		Initial Auto value			Total
Component		%Variance	%Cumulation		%Variance

1	60.431	**60.431**	60.431
2	13.655	74.086	
3	10.128	84.214	
4	9.153	93.367	
5	6.633	100.000	
Cronbach's alpha			**0.813**
Cronbach's alpha if one item is quitted			
CBT1			0.745
CBT2			**0.834**
CBT3			0.770
CBT4			0.774
CBT5			0.763

Other Trusting Factors

Technology Acceptance Model

Correlation Matrix								
	TAM1	TAM2	TAM3	TAM4	TAM5	TAM6	TAM7	TAM8
TAM1	1.000							
TAM2	0.804	1.000						
TAM3	0.553	0.578	1.000					
TAM4	0.689	0.688	0.581	1.000				
TAM5	0.391	0.416	0.425	0.475	1.000			
TAM6	0.432	0.502	0.428	0.49	0.563	1.000		
TAM7	0.411	0.427	0.41	0.518	0.65	0.682	1.000	
TAM8	0.417	0.437	0.417	0.492	0.627	0.625	0.777	1.000
Kaiser-Meyer-Olkin Test								**0.883**
Bartlett Test			Chi-square					1491.819
			df					28
			prob. Level					***
Covariance anti-image								
	TAM1	TAM2	TAM3	TAM4	TAM5	TAM6	TAM7	TAM8
TAM1	0.314							
TAM2	-0.18	0.295						
TAM3	-0.04	-0.063	0.575					
TAM4	-0.093	-0.071	-0.099	0.402				
TAM5	0.001	-0.004	-0.057	-0.17	0.506			
TAM6	0.018	-0.07	-0.027	-0.08	-0.06	0.458		
TAM7	-0.003	0.021	0.006	-0.015	-0.09	-0.12	0.306	
TAM8	-0.009	-0.006	-0.02	-0.01	-0.082	-0.05	-0.168	0.355
Correlation anti-image								
TAM1	**0.83**							
TAM2	-0.592	**0.831**						

TAM3	-0.093	-0.153	**0.949**					
TAM4	-0.262	-0.207	-0.206	**0.927**				
TAM5	0.003	-0.011	-0.106	-0.071	**0.939**			
TAM6	0.048	-0.189	-0.052	-0.01	-0.125	**0.921**		
TAM7	-0.011	0.07	0.013	-0.136	-0.229	-0.321	**0.838**	
TAM8	-0.027	-0.019	-0.045	-0.023	-0.193	-0.125	-0.511	**0.872**
Model Matrix								
TAM1		1						**0.957**
TAM2		1						**0.931**
TAM3		1						**0.772**
TAM4		1						**0.719**
TAM5		2						**0.939**
TAM6		2						**0.901**
TAM7		2						**0.811**
TAM8		2						**0.759**
				Initial Auto value				Total
Component			%Variance		%Cumulation			%Variance
1			59.16		59.16			59.16
2			15.145		**74.305**			15.145
3			6.442		80.748			
4			5.408		86.155			
5			4.787		90.943			
6			4.076		95.018			
7			2.66		97.679			
8			2.321		100.000			
Cronbach’s alpha								**0.9**
Cronbach’s alpha if one item is quitted								
TAM1								0.887
TAM2								0.884
TAM3								0.894
TAM4								0.883
TAM5								0.891
TAM6								0.887
TAM7								0.885
TAM8								0.886

Risk Perceptions (1)

Correlation Matrix							
	RI1	RI2	RI3	RI4	RI5	RI6	RI7
RI1	1.000						
RI2	0.433	1.000					
RI3	0.04	-0.026	1.000				
RI4	0.035	-0.046	0.729	1.000			

RI5	0.001	0.033	0.379	0.402	1.000		
RI6	-0.061	-0.009	0.518	0.471	0.248	1.000	
RI7	-0.065	-0.032	0.44	0.35	0.226	0.645	1.000
Kaiser-Meyer-Olkin Test							**0.704**
Bartlett Test		Chi-square					618.164
		df					21
		prob. Level					***
Covariance anti-image							
	RI1	RI2	RI3	RI4	RI5	RI6	RI7
RI1	0.796						
RI2	-0.351	0.801					
RI3	-0.034	0.012	0.413				
RI4	-0.031	0.042	-0.254	0.437			
RI5	0.033	-0.056	-0.067	-0.118	0.815		
RI6	0.049	-0.038	-0.072	-0.075	-0.003	0.499	
RI7	0.023	0.011	-0.072	0.028	-0.036	-0.286	0.564
Correlation anti-image							
RI1	0.488						
RI2	-0.439	0.482					
RI3	-0.06	0.022	**0.73**				
RI4	-0.053	0.071	-0.597	**0.706**			
RI5	-0.041	-0.07	-0.115	-0.197	**0.872**		
RI6	0.077	-0.059	-0.159	-0.161	0.005	**0.735**	
RI7	0.034	0.017	-0.149	0.056	-0.053	-0.538	**0.712**
Component Matrix							
RI1		1					0.848
RI2		1					0.834
RI3		2					0.846
RI4		2					0.811
RI5		2					0.783
RI6		2					0.71
RI7		2					0.558
			Initial Auto value				Total
Component			%Variance	%Cumulation			%Variance
1			40.062	40.062			40.062
2			20.611	**60.673**			20.611
3			13.159	73.832			
4			10.041	83.873			
5			7.525	91.399			
6			4.871	96.27			
7			3.73	100.000			
Cronbach’s alpha							**0.688**
Cronbach’s alpha if one item is quitted							
RI1							**0.735**

RI2	**0.716**
RI3	0.577
RI4	0.59
RI5	0.661
RI6	0.612
RI7	0.636

Risk Perceptions (2)

Correlation Matrix					
	RI3	RI4	RI5	RI6	RI7
RI3	1.000				
RI4	0.711	1.000			
RI5	0.371	0.409	1.000		
RI6	0.479	0.452	0.234	1.000	
RI7	0.409	0.364	0.239	0.623	1.000
Kaiser-Meyer-Olkin Test					**0.736**
Bartlett Test		Chi-square			548.267
		df			10
		prob. Level			***
Covariance anti-image					
	RI3	RI4	RI5	RI6	RI7
RI3	0.452				
RI4	-0.266	0.456			
RI5	-0.064	-0.13	0.814		
RI6	-0.077	-0.07	0.009	0.541	
RI7	-0.054	-0.002	-0.052	-0.296	0.593
Correlation anti-image					
RI3	**0.728**				
RI4	-0.585	**0.712**			
RI5	-0.105	-0.213	**0.87**		
RI6	-0.155	-0.142	0.014	**0.734**	
RI7	-0.104	-0.004	-0.075	-0.524	**0.719**
Component Matrix					
RI3					**0.826**
RI4					**0.812**
RI5					0.564
RI6					**0.764**
RI7					**0.711**
		Initial Auto value			Total
Component		%Variance	%Cumulation		%Variance
1		54.994	**54.994**		54.994
2		18.554	73.547		
3		13.42	86.968		

4	7.337	94.304	
5	5.696	100.000	
Cronbach's alpha			**0.797**
Cronbach's alpha if one item is quitted			
RI3			0.716
RI4			0.732
RI5			**0.816**
RI6			0.746
RI7			0.772

General Trust in Others

Correlation Matrix

	TRO1	TRO2	TRO3	TRO4	TRO5	TRO6	TRO7	TRO8	TRO9	TRO10	TRO11
TRO1	1.000										
TRO2	0.269	1.000									
TRO3	0.297	0.525	1.000								
TRO4	0.235	0.409	0.552	1.000							
TRO5	0.355	0.359	0.386	0.444	1.000						
TRO6	0.301	0.345	0.354	0.29	0.515	1.000					
TRO7	0.163	0.712	0.36	0.269	0.253	0.248	1.000				
TRO8	0.29	0.374	0.457	0.491	0.318	0.304	0.388	1.000			
TRO9	0.234	0.23	0.296	0.221	0.347	0.358	0.175	0.46	1.000		
TRO10	0.17	0.364	0.206	0.164	0.216	0.143	0.441	0.334	0.254	1.000	
TRO11	0.112	0.283	0.215	0.203	0.208	0.136	0.382	0.406	0.297	0.706	1.000

Kaiser-Meyer-Olkin Test		**0.798**
Bartlett Test	Chi-square	1305.322
	df	55
	prob. Level	***

Covariance anti-image

	TRO1	TRO2	TRO3	TRO4	TRO5	TRO6	TRO7	TRO8	TRO9	TRO10	TRO11
TRO1	0.803										
TRO2	-0.05	0.383									
TRO3	-0.05	-0.12	0.547								
TRO4	0.024	-0.06	-0.17	0.559							
TRO5	-0.12	-0.2	-0.02	-0.15	0.59						
TRO6	-0.06	-0.04	-0.05	0.02	-0.22	0.66					
TRO7	0.43	-0.25	0.014	0.044	-0.00	-0.12	0.43				
TRO8	-0.08	0.033	-0.07	-0.17	0.043	-0.02	-0.08	0.531			
TRO9	-0.02	-0.01	-0.04	0.071	-0.09	-0.11	0.055	-0.19	0.692		
TRO10	-0.05	-0.04	0.02	0.027	-0.02	0.02	-0.06	0.004	-0.02	0.457	
TRO11	0.047	0.032	-0.00	-0.01	-0.01	0.02	-0.04	-0.09	-0.05	-0.29	0.458

Correlation anti-image

TRO1	**0.878**		
TRO2	-0.08	**0.77**	
TRO3	-0.08	-0.27	**0.867**

TRO4	0.036	-0.13	-0.31	**0.801**							
TRO5	-0.18	-0.04	-0.03	-0.26	**0.831**						
TRO6	-0.09	-0.09	-0.08	0.033	-0.35	**0.85**					
TRO7	0.073	-0.61	0.029	0.089	-0.004	-0.023	**0.75**				
TRO8	-0.13	0.07	-0.13	-0.31	0.077	-0.039	-0.178	**0.832**			
TRO9	-0.03	-0.02	-0.06	0.114	-0.14	-0.17	0.1	-0.314	**0.828**		
TRO10	-0.08	-0.09	0.035	0.053	-0.037	0.037	-0.139	0.007	-0.035	**0.729**	
TRO11	0.078	0.077	-0.007	-0.02	-0.03	0.033	-0.088	-0.175	-0.092	-0.725	**0.716**
Component Matrix											
TRO1											**0.474**
TRO2											**0.733**
TRO3											**0.698**
TRO4											**0.64**
TRO5											**0.64**
TRO6											**0.575**
TRO7											**0.659**
TRO8											**0.714**
TRO9											**0.55**
TRO10											**0.572**
TRO11											**0.565**

	Initial Auto value		Total
Component	%Variance	%Cumulation	%Variance
1	39.019	39.019	39.019
2	13.549	52.569	
3	9.876	62.445	
4	7.938	70.382	
5	6.868	77.251	
6	6.264	83.515	
7	4.37	87.887	
8	4.324	92.208	
9	3.164	95.373	
10	2.5	97.873	
11	2.127	100.000	
Cronbach’s alpha			**0.838**
Cronbach’s alpha if one item is quitted			
TRO1			0.818
TRO2			0.815
TRO3			0.824
TRO4			0.817
TRO5			0.823
TRO6			0.822
TRO7			0.829
TRO8			0.831
TRO9			0.826
TRO10			0.834

TRO11	0.827

General Trust in Institutions

Correlation Matrix					
	TRI1	TRI2	TRI3	TRI4	TRI5
TRI1	1.000				
TRI2	0.729	1.000			
TRI3	0.645	0.709	1.000		
TRI4	0.678	0.726	0.689	1.000	
TRI5	0.587	0.607	0.574	0.592	1.000
Kaiser-Meyer-Olkin Test					**0.891**
Bartlett Test		Chi-square			081.125
		df			10
		prob. Level			***
Covariance anti-image					
	TRI1	TRI2	TRI3	TRI4	TRI5
TRI1	0.397				
TRI2	-0.125	0.324			
TRI3	-0.057	-0.105	0.411		
TRI4	-0.082	-0.101	-0.107	0.377	
TRI5	-0.079	-0.065	-0.069	-0.074	0.549
Correlation anti-image					
TRI1	**0.891**				
TRI2	-0.348	**0.862**			
TRI3	-0.142	-0.286	**0.898**		
TRI4	-0.211	-0.288	-0.271	**0.889**	
TRI5	-0.17	-0.154	-0.146	-0.162	**0.933**
Component Matrix					
TRI1					**0.858**
TRI2					**0.891**
TRI3					**0.852**
TRI4					**0.869**
TRI5					**0.781**
		Initial Auto value			Total
Component		%Variance	%Cumulation		%Variance
1		72.419	**72.419**		72.419
2		9.375	81.794		
3		7.148	88.943		
4		6.056	94.998		
5		5.002	100.000		
Cronbach's alpha					**0.905**
Cronbach's alpha if one item is quitted					
TRI1					0.882

TRI2	0.879
TRI3	0.872
TRI4	0.883
TRI5	0.901

* General trust-related items originally included three more items, for a total of nineteen items. They were included to introduce respondents more easily to this block of questions. I decide therefore to remove those three from the statistical analysis.

Confirmatory Factorial Analysis

Discriminant validity

Correlation			**Estimate**
FU	↔	FA	0.896
FA	↔	RE	0.838
FU	↔	RE	0.923
EXP	↔	INN	0.532
FU	↔	EXP	0.241
FU	↔	INN	0.167
EXP	↔	TAM	0.297
INN	↔	TAM	0.165

HTMT			
FU			
FA	**0.894**		
RE	**0.926**	0.841	
TR	**0.965**	0.8	0.85

CBT	**0.882**	0.806	0.739	**0.913**							
EXP	0.239	0.236	0.213	0.433	0.388						
INN	0.14	0.167	0.233	0.296	0.298	0.528					
TAM	0.73	0.683	0.744	0.743	0.673	0.296	0.164				
RI	0.047	0.017	0.063	0.082	0.027	0.272	0.428	0.023			
TRI	0.212	0.232	0.085	0.23	0.24	0.289	0.224	0.085	0.134		
TRO	0.134	0.173	0.066	0.23	0.237	0.138	0.108	0.124	0.046	0.241	
	FU	FA	RE	TR	CBT	EXP	INN	TAM	RI	TRI	TRO

HTMT 2											
FU											
FA	**0.891**										
RE	**0.925**	0.839									
TR	**0.965**	0.797	0.85								
CBT	**0.875**	0.803	0.733	**0.911**							
EXP	0.23	0.228	0.192	0.422	0.384						
INN	0.119	0.145	0.233	0.285	0.296	0.522					
TAM	0.728	0.683	0.744	0.741	0.672	0.294	0.153				
RI	0.047	0.017	0.063	0.082	0.027	0.272	0.428	0.023			
TRI	0.198	0.22	0.068	0.22	0.213	0.284	0.218	0.085	0.134		
TRO	0.12	0.148	0.047	0.219	0.226	0.135	0.099	0.115	0.046	0.225	
	FU	FA	RE	TR	CBT	EXP	INN	TAM	RI	TRI	TRO

BUILDING TRUST THROUGH TECHNOLOGY IN AUTOMOBILE INSURANCE: AN EXAMINATION OF THE ROLE OF BLACK BOX

Insurance firms are exposed to the problem of asymmetric information. Adopting the black box is a rational choice that portrays the policyholder’s trustworthiness as a willingness to share complete private information. This study draws from the literature on information asymmetry in the car insurance market to test if, and if so how, the adoption of the black box is a credible signal to believe in the policyholder's claim of trustworthiness and support the trust-building process from the perspective of an insurance company. Estimates show that black box adoption has a positive effect after controlling for the level of accidentality in a specific area. However, contrasting results are obtained for women and more experienced drivers. I find that, for these groups of policyholders, the choice to adopt the black box can lead to a distortion in the signal to the insurance firm.

Keywords: digital trust, information asymmetry, car insurance market, black box

INTRODUCTION

Information is a strategic resource in most economic transactions. The ability to control more information has been recognized as hugely valuable because it can produce an important advantage (Chiappori, & Salanie, 2000). For many years, researchers in economics have studied this problem of information asymmetry (Wilson, 1977; Rothschild and Stiglitz, 1976; Akerlof, 1970). Information asymmetry deals with situations where one party in a transaction possesses more information to take advantage of another. Akerlof (1970), for example, uses the 'lemons' market to explain how information asymmetry can lead to inefficiencies. Because many important variables are not easily accessible for inspection in the 'lemons' market, adverse selection is one fraudulent consequence. The effect of adverse selection is also at the heart of several economic transactions within the car insurance market (Abbring, Chiappori, Heckman, & Pinquet, 2003; Dionne, Gourieroux, & Vanasse, 2001; Chiappori, & Salanié, 1997; Dionne, &

Gourieroux, 1996; Crocker, & Snow, 1986). In the car insurance market, adverse selection occurs because a policyholder uses their private information to gain an insurance policy at a cost that is below the true level of risk. Under conditions of limited access to information, things concerning the policyholders' trustworthiness (including fulfilling moral obligations, exhibiting fairness, and sharing information) are questioned. In the absence of credible cues, there is no placement for trust as a state of mind that only develops in the face of positive expectations about the behavior of someone (Rousseau, Sitkin, Burt, & Camerer, 1998; Mayer, Davis, & Schoorman, 1995).

In recent years, the black box has been introduced as telematic equipment to collect private information on driving behaviors. It uses a motion sensor to record several driving metrics that are given back to the insurance firm for monitoring if the car is driven safely. As the driving behavior is correctly monitored, the decision to adopt a black box is equivalent to voluntarily disclosing private information from a proof source. Because black box can combine the benefits of signa ling and screening strategies (Geyer, Kremslehner, & Muermann, 2020; Muermann, & Straka, 2011), it emerges as a potential solution to sustain an insurance company's trust-building process through continuous verification of driving behavior against initial claims of trustworthiness of good behavior. It means that policyholders are subject to the authority of technology that they confidently believe is effective to disseminate private information. So far, the academic discussion is relatively little (Geyer et al., 2022; Fan, & Wang, 2017;

Muermann, & Straka, 2011). I believe that a deeper understanding of the effects of black box devices is needed. To fill this gap, this study asks the following question: if, and if so, how, if, the adoption of the black box is a credible signal to believe in the policyholder’s claim of trustworthiness and support the trust-building process from the perspective of an insurance company.

The research question is examined using a dataset from an insurance car firm containing records of black box adoption in the Italian market. I integrate this dataset with other data from public repositories of societal trust, local accidentability, and Google trends. In this study, my identification strategy follows a two-tiered approach. First, a series of logit models is developed to test the correlation between black box adoption and the likelihood of an accident. Estimates show that the positive effect of black box adoption comes out after controlling for the level of accidentality in a specific area. For a ‘good driver’, adopting the black box is ideally not a problem. In high traffic areas, policyholders can prove their true quality because the black box provides an informational ground for real-time verification of prior claims of trustworthiness. Findings who subscribe to the insurance policy online, thus with no persuasion by the seller. I find, however, counterintuitive results. The trustworthiness signal is distorted when considering the effect of are confirmed even after controlling for black-box adopters gender and the amount of experience. Although women and more experienced drivers are generally believed to take fewer risks at driving (Lonczak et al., 2007; Yagil, 1998; Berger, 1986; Veevers, 1982), they manifest a tendency to overestimate their driving abilities. Second, I conduct a wide range of robustness tests against the self-selection bias and endogeneity issue.

The second part of the empirical analysis is dedicated to robustness checks to investigate whether there is the possibility of self-selection bias and endogeneity issues. I find strong evidence that the effect of the black box is separated from the decision to adopt when conducting Heckman's self-selection model in a quasi-natural experiment using data on corporate car policies. This result is also found in all the endogeneity tests. The adoption of the black box might be irrelevant for safer drivers. Using a variety of instrumental variables (societal trust, local accidentability, and general interest in the black box device) for the principal component analysis, I demonstrate that endogeneity is not an issue. Further, differences between the groups of black box adopters and non-adopters are studied through propensity score matching. I obtain a significant average treatment effect of black box devices on the likelihood of an accident. This demonstrates that black box adopters (treated group) are less likely to cause an accident compared to non-adopters.

The present study has twofold major contributions to the literature of behavioral economics. First, I introduce the black box as a new phenomenon and elaborate on its potential effects for the trust-building process under the problem of adverse selection. I find that the black box helps distinguish the real 'good' policyholders from those who claim to be, especially in those areas where accidents are more frequent. It is an effective means in the domain of signaling and screening. Therefore, I provide a categorization for the black box to spur new research at the intersection between technology and information asymmetry to shed light on how the insurance firm may find good reasons to trust. Second, in comparing the behavior of black box adopters and non-adopters, women and more experienced drivers make important mistakes in signaling their true type. Thus, I direct attention to an important challenge of how technology like the black box is not apart from the action of cognitive bias – most importantly, the overconfidence bias. Researchers interested in studying the choice of some subject categories should interpret results with some caution. Lastly, I recognize that this study has practical managerial implications. It provides very useful insight into the performance of the black box (and technology more in general) within the general risk management framework. Thus, managers should support the black box initiatives for the achievement of the full effect.

The study is organized as follows. Section 2 presents the literature review with a detailed discussion of information asymmetry and trust. Emphasis is given to the implications of the black box for the trust-building process within the car insurance market. Section 3 describes the data and defines the variables. In Section 4, I illustrate the statistical model and results of empirical analysis regarding the effect of the black box on trust. Next, results are validated through robustness checks that I document carefully. Finally, Section 5 provides concluding remarks for academic research and limitations that might be addressed in future studies.

TRUST AND THE PROBLEM OF INFORMATION ASYMMETRY IN THE CAR INSURANCE MARKET

Adverse selection and moral hazard

In an ideal world, a buyer pays a price that reflects the willingness to pay, the seller sells at the price which reflects the quality of goods and services. In reality, that's not the situation. Holding greater material knowledge allows maximizing self-utility (Williamson, 1991; Smitka, 1975). For example, in the market of used car sellers typically know more than buyers. Sellers have full knowledge of the quality of a car that buyers generally don't have, leaving only 'lemons' in the market (Williamson, 2002; Akerlof, 1970). This information failure is known as information asymmetry (Akerlof, 1970; Rothschild, & Spence, 1976). Adverse selection and moral hazard are just two consequences of information asymmetry. Adverse selection refers to a lack of equal information between the buyer and the seller about the quality of goods traded in the market. Since the seller typically knows more about the quality of goods, there is an opportunity for the seller in the marketplace to sell low-quality goods (the lemons) to unaware buyers. Moral hazard, on the other hand, describes the risk that a party is not entering into an economic transaction in good faith. There is a risk that one may change in the behavior after an agreement is reached for the obtainment of a superior gain. This is common in situations where consequences for fraudulent behavior cannot be perfectly observed because of a separation between ownership and control.

The car insurance market is an ideal archetype where those consequences of information asymmetry can take place (Rothschild, 1978; Smitka, 1975). The risk of an accident is an unobservable characteristic of policyholders. Policyholders (the buyer) have private information about their driving behavior which is unknown to the insurance firm (the seller) at the time of contracting. Because the former can benefit from this informational advantage for near fraudulent outcomes, a policy is one tactic to force the counterpart to reveal that private information. A policy is a contract that defines what the insurance firm should pay for loss when a car accident is caused. Under adverse selection, a policy involves ex-ante problem-solving. Theoretical studies of automobile insurance have discussed the importance of deductibles in a policy (Crocker, & Snow, 1986; Rothschild, 1978; Rothschild, & Stiglitz, 1976). The amount of deductible is one piece of information of the actual policyholder's driving behavior. It is a type of signaling and screening to determine the policyholder's risk profile based on an ex-ante self-assessment of driving behavior. This is reflected in the positive correlation between the policyholder's accident probability and the level of coverage in a single period (Dionne et al., 2013). In the case of moral hazard, driving aggressively can be an expression of a moral hazard problem due to the unobservability of efforts to prevent accidents. A policy includes the formalization of civil liability by law. It specifies the claims that the insurance firm is legally required to pay as compensation in case of accidents. For that reason, it is one control mechanism reducing the kind of ex-post risk behavior in a way that effective transactions are stimulated in the car insurance market (Wollner, 1999; Macaulay, 1963; Mowbray, 1961). High coverage, however, may decrease the incentives for safety, leading to more accidents because the full cost of that risk is not fully paid (Shavell, 1979).

While insurance policies can ease the way to protect against problems of information asymmetry through the attainment of common acknowledgment (Bachmann, & Inkpen, 2011; Nooteboom, 2007; Fukuyama, 1995; Gulati, 1995; Ring, & Van de Ven, 1992; Sitkin, & Weingart, 1992; Zucker, 1986), they are designed upon standard forms of legal enforcement which literature has described as weak legalistic remedies (Sitkin, & Roth, 1993; Donaldson, & Davis, 1991; Granovetter, 1985). Because it may be the case that an insurance policy is complex and costly to write, it is not feasible to specify every possible contingency (Chiappori, & Salanié, 1997). Moreover, a typical subscription of an insurance policy spans a short period, with the option to renew after one year. Given the finite repetition, policyholders have incentives to lie (Lyons, & Mehta, 1997). An insurance firm might be reluctant to believe in the trustworthiness of any claims about proper driving behavior. Whether or not an insurance firm offers a policy depends on the level of trust. This includes expectations that the policyholder will fulfill agreements and obligations, exhibit fairness, and share information (Zaheer, McEvily,

& Perrone, 1998; Noordewier, John, & Nevin, 1990). If the level of trust on the side of the insurance firm surpasses the threshold of perceived risk for fraudulent outcomes, then a transaction occurs even without a complete contract for controlling each possible behavior (Carson, 2006; Rousseau, Sitkin, Burt, & Camerer, 1998; Macaulay, 1963).

Trust and different forms of trust

In the insurance market, trust behavior is manifested in the willingness of an insurance firm to offer a policy on fair terms. It means that a policy is issued today in exchange for the policyholder's promises to not cheat in the future. Trust is a meaningful concept forming the basis for relationships because it helps reduce transaction costs (Guiso, Sapienza, & Zingales, 2008; Nooteboom, 2007; Carson, 2006; Fukuyama, 1995; Gambetta, 1988; Arrow, 1972). Several studies argue that trust originates from a complex building process, involving multiple components (Nooteboom, 2007; Schoorman, Mayer, & Davis, 2007; Möllering, 2006; Rousseau, Sitkin, Burt, & Camerer, 1998). In Mayer et al. (1995) the act of trust is differentiated between trusting attitudes, beliefs, intentions, and behaviors.

Trusting attitudes are highly related to a propensity to trust as an individual tendency to be willing to generally depend on. Trusting attitudes are derived from personal experiences, personality types, and cultural backgrounds (Rotter, 1971; Rotter, 1967). They contribute to coloring the intensity of trusting beliefs towards specific others (McKnight, Cummings, & Chervany, 1998). Trusting beliefs are a central aspect of the trust-building process and are related to the initial evaluation of a specific party. They originate from perceptions of the other's ability, integrity, and benevolence to perform something of importance for the trustor (Mayer, Davis, & Schoorman, 1995; Coleman, 2000). For instance, in the conventional wisdom, women display more empathy and sociability in relationships with others (Aggarwal, Goodell, & Selleck, 2015; Croson, & Buchan, 1999; Anderson, & Blanchard, 1982). Because they are likely to reciprocate and provide utility without self-interest (Wright, & Sharp, 1979), women appear more credible in the area of integrity and benevolence than men across high-risk situations (Kar, & Swain, 2014; Rosenberg, Gonzalez, & Narain, 2009). Thus, trusting someone is a manifestation of a reasoned intention which is guided by the belief that the risk of being betrayed is low (Cook, & Cooper, 2003; McKnight, Cummings, & Chervany, 1998; Mayer, Davis, & Schoorman, 1995). In other words, trusting intention is a matter of willingness to trust others with a feeling of relative security, despite the possibility of negative consequences. Such a volition gives a fiduciary obligation of risk acceptance which may come in many actions of proper conduct. Those actions are what Barber (1983) defines a trusting behavior, a concept that later studies clarify to vary along with a bandwidth from a calculated weighing of cost and benefits to a relational response based on the societal configuration (Rousseau, Sitkin, Burt, & Camerer, 1998).

From an economic perspective, trust is not a leap of faith but an instrumentally rational behavior (Williamson, 1991). It is calculated based on the evaluation of costs and benefits within the boundaries of the economic transaction, whether that transaction is an isolated transaction or any type of recurrence. Much of the economic literature assumes that the range of calculus-based trust is limited to situations where verifiable information can be obtained in the short term. A formal certification, perhaps, may provide an enforcement mechanism to calculus-based trust wherein incentives to trust are intentionally under a priori guidelines and good practices (Bachmann, & Inkpen, 2011; Rousseau, Sitkin, Burt, & Camerer, 1998; Lyons, & Mehta, 1997; Williamson, 1991; Barber, 1983). This makes future behavior more predictable. Thus, for an insurance firm, a calculus-based trust reflects confidence in the policyholder's reliability as a positive expectation that being trustworthy is more attractive compared to the gains obtained from breaching a policy. The rise of trust, however, is not apart from the social arena. It is also the result of a relation-oriented behavior to commit some moral and ethical principles for sharing, solidarity, collective action and cooperation, information sharing, and social cohesion and inclusion among people of the same social group (Grootaert, 2003; Helliwell, & Putnam, 1995). Putnam (1993) has discussed that in high-socially embedded areas the effect of relation-based trust is stronger than calculus-based trust for the proper functioning of these social groups. In this vein, some scholars (Guiso et al., 2016; 2011; Tabellini, 2008; Putnam, 1993) have correlated this finding to some measures of civic capital. Civic capital is a concept to describe the civic dimension of social capital regarding compliance with moral and ethical principles. This includes education and cultural background (Tabellini, 2008), donating blood and organs (Guiso et al., 2016; 2004), length of justice trials, and frequency of voting in political elections (Guiso et al., 2011; 2008; Putnam, 1993). This is a key issue also in insurance transactions. In car insurance transactions, parties tend to adhere to collectively shared values of good behavior, thereby developing effective information exchanges which help overcome the risk of self-seeking deviations (Muermann, & Straka, 2011).

TECHNOLOGY-BASED SYSTEM FOR THE TRUST-BUILDING PROCESS IN THE INSURANCE MARKET

The case for integrating trust in car insurance transactions requires calculus more than social relationships. The volition to trust is a rational choice deriving not only from the existence of improved contractual governance structures (Smitka, 1994; 1975) but also from the recognition of credible cues of trustworthiness in the immediate setting (Barber, 1983). Cues are an effective means to believe in the policyholder's claim to behave properly across a broad range of situations. They can improve the risk classification since new information is added to correct the problems involved with information asymmetry. The cues available to the insurance firm usually concern observable policyholder's characteristics (sex, age, income, region, driving experience), vehicle characteristics, past accidents, and choices of insurance contract and coverage (Dionne et al., 2013). Without these cues, an insurance company is unlikely to trade securely because there is skepticism and suspicion about the policyholder's reliability. The relevance of cues has been first discussed in Spence's (1973) job-market signaling model. The employees acquire education credentials to signal their ability level to the employer. Because the informational value of such a cue is public, it enables the employer to distinguish between low- and high-ability employees since the educational credential is positively correlated with having a greater ability. Affiliation to some recognized group traits is meant to signal that one deserves to be more or less trusted (Doney, 1998; Rousseau et al., 1998; Lyons, & Mehta, 1997; Mayer et al., 1995).

In the last few years, the black box device has been introduced in the Italian market of liability insurance as a proof source that the policyholder's claims of trustworthiness are true. The black box is a piece of telematic equipment that is installed on the insured car to collect and stored unobservable information of driving habits (such as vehicle speed, location, distance traveled, driving frequency, and time of day the car is in motion) in ledger tables which are resistant to data manipulation. This gives the insurance firm a more accurate basis to adjust policy premiums on how risky a car driver is, rather than relying on general statistics as that may penalize, for example, inexperienced drivers or be conducive to inappropriate policies (Cohen, 2005; Pinquet, 2005; 2000; Dionne, & Vanasse, 1992; Cooper, & Hayes, 1987; Dionne, & Lasserre, 1985; Crocker, & Snow, 1985; Hoy, 1982; Wilson, 1977; Rothschild, & Stiglitz, 1976). As a result, the insurance firm deals with transactions that are highly bounded through continuous data gathering, with no chance for the policyholder to exploit a potential informational advantage in the future. As Muermann and Straka (2011) have shown in their seminal work on the effect of private information in car insurance, telematic data are beneficial on two sides. Most importantly, telematic data provide the insurance firm with detailed information of risk preferences for more accurate screening of policyholders. The informational value of the black box would facilitate the achievement of the recommendation "trust but verify first" (Lewicki, McAllister, & Bies, 1998) which is also echoed by the recent introduction of blockchain (De Filippi et al., 2020). On the other hand, policyholders who drive responsibly may benefit from a lower premium because the actual 'high risk' car drivers (the 'lemons') can be easily detected. According to the Italian insurance act (n. 124/2017), the adoption of the black box is voluntary and does not require policyholders to pay the price of black box and installation. It is the policyholder who decides whether or not to adopt the black box.

Adopting the black box for handing over control of a piece of private information to the insurance firm is not a concern for policyholders who are really (or perceive themselves) trustworthy. In these circumstances, the black box can act as broad support to sustain the critical mass of trust of an insurance company toward the policyholder. In this study, I take a view of an insurance company and seek to deepen the understanding of the black box as a credible cue of the policyholder's trustworthiness. My focus is if, and if so how, the adoption of the black box matters about overcoming the problem of information asymmetry. Concerning the problem of information asymmetry, I refine my research question to the problem of adverse selection only.

EMPIRICAL MODEL

Following my research goal from the perspective of an insurance company, I specify a logit model that captures the effect of the choice to adopt the black box on the likelihood of an accident. All the components in this model vary across the policyholders, so I can examine how the effect differs between black box adopters and non-adopters.

$$Acc = a_0 + b_1BB_i + b_2BB + b_3\Sigma\ Contrs^k{}_i + e$$

In the model, *i* refers to policyholders. The likelihood of an accident (Acc) is the dependent variable. It is a dummy taking value 1 if a policyholder has experienced at least one accident in a given year (0, otherwise). As I am interested in evaluating if, and if so how, the decision to adopt the black box is a credible signal to believe in the policyholder's claim of trustworthiness when (s)he makes a self-declaration of driving abilities, I assume the accident is being explained by the black box adoption (BB). This is my independent variable taking value 1 in case of a black box adopter (0, otherwise). In this study, that variable is time-invariant because the black box device cannot be uninstalled before the policy is closed. The rest of the data available are used as control variables (Contrs). Their selection follows previous studies in the car insurance market focusing on the problem of information asymmetry (Dionne, Michaud, & Dahchour, 2013). I report the description of variables used for the model estimation in Appendix A.

DATA

We use data from multiple sources that contain information on various measures spanning policyholder's characteristics, decision to adopt the black box, rate of accidentability, and control variables. In what follows, I present each of these datasets and define the variables of my empirical analysis.

Data sample of insurance policyholders

My main dataset is from an insurance firm operating in the Italian market of car liability (i.e., Responsabilità Civile Auto). I use policyholders as an observational unit with a total of 1,301,886 Italian policyholders. Among those, corporate cars are about 5% of the entire population of policyholders. I exclude those observations from my analysis because the information available is limited to the company (no data is available about car drivers). That dataset is a five-year panel covering a period of observation from 2015 to 2019. A policyholder is not present each year. On average, a policyholder remains in the panel about 1.47 years from a minimum of 1 year (minimum duration) to a maximum of 5 years.

The panel is composed of three types of information. The first type concerns the policyholder's characteristics (gender, age, region, driving experience, history of accidents, etc). The second covers vehicle characteristics (year, fuel, car model, etc.). The third element regards policy characteristics (bonus-malus coefficient, level of coverage, black box adoption, premium, etc.). In Italy, the bonus-malus coefficient (classe di rischio universale) defines for a policyholder the risk classification to cause an accident. It ranges from 1 (low-risk driver) to 18 (high-risk driver). After each year of no-caused accident, the policyholder receives an improvement in the bonus-malus coefficient; otherwise, a downgrading will apply if a policyholder is responsible for a severe accident. Two types of insurance coverage are offered to Italian policyholders: all-risk insurance (assicurazione kasko) and third-party liability (assicurazione mini-kasko). The former protects against losses incurred by both the policyholder and third parties, whereas the latter protects against third-party losses only. Third-party liability is required at a minimum by Italian law. In both cases, the amount of premium varies with changes in observable characteristics, given the bonus-malus coefficient. According to the Italian insurance act (n. 124/2017), the choice to adopt the black box device must be separated from the choice of the level of coverage. If the black box is adopted, the policyholder receives some additional services (such as cheaper future premium, theft deterrent, 24/7 customer service). This should be understood as compensation for adopting a trusting behavior in a way that the willingness to share private information through the black box is compared to the willingness to cooperate with the insurance firm.

Table 1 gives the summary of descriptive statistics (see Appendix C). Nearly one-third (37%) of policyholders are women (Gender). In that panel, women are 478,093 in total. An interesting finding is that almost all women have a bonus-malus coefficient which is one. This may suggest that women are typically good drivers. For women, the mean value of accidents is close to zero. They are presumably causing a few accidents because they take less risk given their attitude to risk-aversion (Cohen, 2007). The typical policyholder is 54 years old. The mean age (Age) of policyholders provides an important indication of driving experience. More than half of the entire population is over the age of 50, corresponding to 30 years of driving experience. For the insurance firm, more experience is associated with fewer accidents. The mean value of accidents (PrevAcc) is less than one, meaning that policyholders tend to have no accidents in the previous 5 years. Thus, they are associated with the class of good drivers (low risk). Figure 1 illustrates the geographical distribution of this measure across the Italian provinces (see Appendix C). The measure is related to accidents (dependent variable) that I assume are time-invariant. The mean value shows that the unconditional likelihood of an accident is 7%. That percentage is more or less stable across the five years ranging from 6.46% in 2018 (lower-value) to 7.56% in 2015 (upper-value). This means that policyholders having a previous history of accidents continue to have more accidents also in the future years. However, as I will discuss later, it is possible that this data does not consider the totality of accidents, but only accidents that have been claimed to the insurance firm (Dionne et al., 2013).

Next, I observe that policyholders choose a third-parties liability (mini-kasko). This tells me that policyholders generally refuse moral hazard. Dionne et al. (2013) has demonstrated that an all-risks coverage is selected by individuals who are more likely to change their accident probability after a policy is issued. This is exactly the definition of moral hazard. As I have already discussed, the premium is not a fixed value, but it varies across policyholders every year. The mean premium paid by policyholders is € 330.00 per year. In the rest of the study, I convert premium in a logarithm measure; perhaps, the mean value of premium corresponds to 5.80 (Premium). Surprisingly, the mean value of black box adopters is very low. Only 2% have decided to install the black box device on the car (independent variable). This decision might be influenced by several factors that I will discuss in the next section. At this stage, I can only comment that the black box is more widespread in the area where the level of general trust is below the mean value (see Figure 1). This would confirm that the black box device is used for signaling and screening.

Finally, I comment on summary statistics of vehicle characteristics. The mean value of car age is 9 years old (CarAge). Fuel type is quite diversified: 44% is petrol cars, 49% diesel cars, less than 1% electric cars, 4% LPG cars, and 2% methane cars. Statistics indicate that petrol and diesel are the most preferred fuel types of insured cars.

Data sample of societal trust

A second dataset is used to measure the level of societal trust within Italian provinces. This is used as a control variable. I rely on Calcagnini and Perugini's (2019) contribution who have identified four elements to evaluate the level of well-being: i) blood donation, ii) bike lanes, iii) length of first-instance ordinary court proceedings, and iv) car theft. First, blood donation (GeoBlood) represents the individual propensity to reciprocate and cooperate. It is measured as blood donation per million inhabitants. The same variable is also present in Cartocci (2007) and Guiso et al. (2004). Table 1 reports 36.91 as the mean value. The geographical pattern of blood donation, however, is varied among Italian provinces (see Figure 1). Blood donation is higher in North Italy, weaker in the Centre, and very weak in the South (Guiso et al., 2009; 2000). Second, bike lanes (GeoBikeLanes) capture social inclusion and networks. It measures the length of bike lanes per 100 Km^2. More bike lanes are expected to enhance mobility for active commuting among people. Active commuting, indeed, can promote the circulation of resources through participation in several social networks or other social structures (Dominguez, 2003). The mean value of bike lanes is 15.99 kilometres per 100 Km^2. Again, I observe that North Italy performs better. The remaining variables measure generalized trust in institutions and society. The measures of length of first-instance ordinary court proceedings and car thefts work in the opposite direction compared to blood donation and bike lanes. The higher the value of the former, the lower the total amount of involvement in social affairs in that province (Guiso et al., 2011; 2008). First-instance ordinary court proceedings (GeoLenghtCourt) measures the length of first-instance ordinary court proceedings to take place, while car theft

(GeoCarThefts) counts for the number of car thefts per 100,000 inhabitants. The former takes on average three years, and the latter is 336 per 100,000 inhabitants. Figure 1 shows that overall, North Italy is more socially oriented. Such a greater stock of societal trust is rooted in historical events (Guiso et al., 2011; 2008; Acemoglu, 2005; Helliwell, & Putnam, 1995). North and South Italy have experienced different political treatments over time. Originally, North Italy was characterized by a lack of government. This lack was conducive to the formation of small communities that agreed with some social norms of mutual help and collaboration which is traceable in all the four elements of societal trust. On the contrary, such a political configuration was hardly developed in the South, where an autocratic monarchy was established (North, 1990).

Data sample of geographic accidentability

A third dataset is released by ISTAT (https://www.istat.it/) and concerns the distribution of car accidents across the Italian provinces. That data is used to correlate the likelihood of an accident to the characteristics of accidentability of a specific province which is referred to as the control variable. I identify four elements: local accidents, injured accidents, fatalities, and accidents by vehicle. Local accidents (IGeoAccidents) measure the number of accidents per 100,000 inhabitants in a specific province. As Table 1 illustrates, the average number of total accidents is 294 accidents per 100,000 inhabitants. Injured accidents (IGeoInjured) and fatalities (IGeoFatalities) measure precisely the number of injury and fatal accidents, respectively. Every year the mean value of injury accidents is 414 per 100,000 inhabitants. The mean value of fatal accidents is badly lower compared to injury accidents. There are five fatal accidents per 100,000 inhabitants. Lastly, accidents by vehicle (IGeoAccidentsByV) represents the number of total accidents per 10,000 vehicles. The geographical distribution of each element (see Figure 1) reveals that the North area is characterized by a greater number of accidents. One possible explanation is the tendency to claim an accident as a manifestation of civic behavior (Guiso et al., 2009). This is done despite changes in the premium being linked to past accidents (Dionne et al., 2013). More accidents lead to higher risk classification, resulting in a higher premium.

Data sample of trends in black box web searches

The last dataset provides insights into the general interest in the black box device by the Italian policyholders over the period from 2015 to 2019. Data is collected from Google Trends by entering the "black box" as a key term for search within the domain of the insurance industry. Because web searches are aggregated to form a monthly standardized score, a monthly time series of scores for each Italian region is available. The score ranges from 0 to 100. It equals the maximum value when a term, for instance "black box", is most frequently searched compared to previous months. As Figure 2 illustrates, the term "black box" was most frequently searched in November 2017, while April 2017 reports the minimum number of searches. This data, however, is not completely sufficient. I need that this data is meaningful per Italy region. For that reason, I release yearly Google search data. By joining this data with Google Trends, I obtain a better cross-section comparison among Italian regions that I capture through the BBGoogleT variable (control variable). Regions get the maximum score (100) when they correspond to the highest number of web searches of “black box”. Then, this is used as a reference metric to calculate the scores of other regions. It means that the score is not calculated as an absolute value but in relative terms.

RESULTS AND ESTIMATES

The adoption of the black box across policyholders

We start presenting descriptive statistics. I use the BB variable to generate two subsamples: black box adopters and non-adopters. Differences between black box adopters and non-adopters are statistically examined using a parametric t-test and a non-parametric χ 2 -test. I present complete results in Table 2.

We observe an interesting result. Black box adopters have more likelihood to cause an accident than non-adopters (9% versus 7%). This is statistically significant in both t-test and χ^2 -test. Friday is the time of the week when accidents are most frequent; they are dramatically reduced on Sunday. This is due to Italian habits. On Friday people tend to travel more because of personal affairs and job trips, while Sunday is traditionally devoted to spending time at home. hest frequency of accidents. This is associated with very bad weather conditions. Although black-box adopters have more chances to cause an accident, the severity is lower. IGeoInjured is lower for black-box adopters

(3Among months, January and February report the hig98 per 100,000 inhabitants) compared to non-adopters (414 per 100,000 inhabitants). Similarly, (IGeoAccidentsByV) is equal to 33.18 for black-box adopters compared to 34.64 accidents per 10,000 vehicles for non-adopters. As it appears from Figure 3, PrevAcc plays a big part in the decision to adopt the black box device. Policyholders who have experienced a greater number of accidents in the last few years are less attracted to the black box.

The black box, indeed, may give to the insurance firm better evidence of the actual driving abilities which may result in a more expensive premium for the policyholder because of worse risk classification. On the contrary, women and less experienced drivers adopt more black box devices. Women are around 40% of black-box adopters, while they do not exceed the 37% in the group of non-adopters. Further, the mean age value is lower for black-box adopters (49 versus 54 years old). A tendency to adopt the black box device is also displayed among policyholders holding a diesel, lpg, or methane car. Insurance firms generally assume that cars running on petrol are more expensive to maintain, therefore a policyholder may use less of the car to keep the private fuel cost minimum. This is expected to have a positive impact on the likelihood of accidents because car circulation is reduced (Richaudeau, 1999). Thus, black-box adopters driving cars running on more convenient fuel are those who are willing to communicate their trustworthiness for the obtainment of a better risk profile.

Other results seem to be consistent with studies of societal trust in economics (for example, Nooteboom, 2007; Guiso, Sapienza, & Zingales, 2004; Fukuyama, 1995; Coleman, 2000). Black box adopters live in areas where the level of societal trust is low (see Figure 1). The mean value of GeoBlood (34.65 versus 36.97 per 100,000 inhabitants), GeoBikeLanes (13.99 versus 16.04 per 100 Km^2), GeoLenghtCourt (1,106 versus 1,032 days), and (399.56 versus 334.19 per 100,000 inhabitants) would indicate that societal trust does matter. Where claims of trustworthiness are continuously questioned, the black box device appears as an important cue to communicate the intention of policyholders to behave properly. I suppose the black box device acting as a societal control to anticipate positive motives and sustain the critical mass of trust of the insurance firm to the policyholder (Bachmann, & Inkpen, 2011; Nooteboom, 2007; Rousseau, Sitkin, Burt, & Camerer, 1998).

The effect of black box adoption on the likelihood of an accident

We test for the effect of black box adoption on the likelihood of an accident with multivariate analysis. I study this relationship through a series of logit within correlation clustering (Thompson, 2011; Petersen, 2008), wherein correlations among policies in the same year and among years for the same policy are examined. Table 3 reports the estimates for the proposed model (see Appendix C).

In Model (1) the likelihood of an accident is significantly affected by the adoption of the black box (BB=0.19, p=***). The estimate suggests that black box adopters are more likely to cause an accident, ceteris paribus. The positive sign may seem counterintuitive in a way that the black box would leave the ‘lemons’ behind (bad drivers, i.e. drivers tending to be less careful about driving). With previous findings (Dionne et al., 2013), the likelihood of an accident is also significantly affected by previous accidents (PrevAcc=0.21, p=***) and the amount of premium (Premium=0.46, p=***).

The likelihood of an accident is also increased when I control for some observable characteristics. In model (2), women (gender=0.05, p=***) are associated with a greater likelihood of accidents than men. The same effect is observed for policyholders having caused at least one accident in the last five years (PrevAcc=0.22, p=***), paying a high premium (Premium=0.49, p=***), and driving very recent cars (CarAge=-0.02, p=***). The latter, indeed, are indicative of a high-risk driving profile to cause an accident (Dionne et al., 2013).

Model (3) includes additional control variables that I obtain by combining gender and age to interact with each other (BBxGender, BBxAge, and BBxGenderxAge). I observe a change in the estimated sign of the black box variable. The effect of black box adoption on the likelihood of an accident is negative, but not statistically significant (BB=-0.03, p=0.11). My main thesis is still not supported. However, the estimates of interaction variables add some important pieces of information. For women, the effect of the black box remains positive and statistically significant on the likelihood of accident (BBxGender=0.23, p=**). This would say that the choice to adopt the black box is self-defeating for women. Similarly, adopting the black box does not seem to add more value for more experienced drivers (BBxAge=0.00, p=***).

We now include a control variable capturing the level of accidentality in a specific area (IGeoAcc). In Model (4), I eventually find that the effect of the black box on the likelihood of an accident is negative (BB= -0.18, p=**). This would mean that previous models suffer from omitted variables. In this case, the level of accidentability would capture a certain amount of variance and explain that in high-traffic areas the likelihood of an accident is greater because of more vehicles on the road. Such a fact is exogenous to the choice to adopt the black box. Thus, my thesis is confirmed. Model (4) offers another interesting result. The effect of BBxPrevAcc on the likelihood of an accident is not statistically significant (BBxPrevAcc= -0.18, p=0.64). It means that the accidentability is not significantly different for black-box adopters and non-adopters, suggesting the absence of moral hazard in the behavior of black-box adopters. Additionally, I observe that gender is still helpful. Women adopting the black box are more likely to cause an accident (BBxGender= 0.23, p=**). The same thing is not with age which seems to have a null effect (BBxAge= 0.00, p=**). These findings would appear not consistent with the theory assuming women are more trustworthy than men. If the theory is true, BBxGender should have a negative sign. I hypothesize that one interpretation of such a contrasting effect would imply that the overconfidence bias is present among certain groups of black box adopters and is conducive to adverse selection to develop.

Finally, I propose Model (5). The model is restricted to those policyholders having subscribed to a car insurance policy online. Such a group of policyholders is assumed not to be influenced by the salesforce pressure. For example, I don't exclude that a policyholder has been persuaded by a broker to flag the black box option into the policy. Thus, for online policyholders, the choice to adopt the black box is a more reliable representation of their true level of trustworthiness. As I look at the estimates, all previous findings are confirmed about their sign and statistical significance. Once again, what is shown for women deserves further investigation since there might be important consequences for the problem of adverse selection. Under pure adverse selection, bad drivers behave as myopic agents who experience more accidents, obtain bad bonus-malus scores and continue to be like this over time (Dionne, & Doherty, 1994). This creates conditions for a bad screening between low and high-risk drivers, resulting in an average policy premium which is disadvantageous to the insurance firm's risk management (Dionne et al., 2013).

The existence of the overidentification bias

From previous findings, I recognize that the correct interpretation of all the estimates linked to gender might be distorted by the overconfidence bias. Overconfidence bias is a tendency for a person to hold an overestimation of their abilities. In the specific context of car driving, overplacement is the most prominent sub-section of overconfidence bias which is conducive to inaccurate calibration of beliefs (Moore, 2008). Perhaps, Svenson (1981) has found that American drivers celebrate themselves better than average. The literature agrees that women are believed to take fewer risks at driving because they are generally risk averse (Lonczak, 2007; Yagil, 1998; Berger, 1986; Veevers, 1982). However, such a self-identification with these positive beliefs can subsequently stimulate a false and misleading self-assessment of personal driving performance as higher than it is (Lackner et al., 2020; Necki et al. 2007). Experimental studies in social psychology have shown that women are judged more credible than men in the domain of trustworthiness (Van Den Akker, 2020; Rau, 2011; Croson, & Gneezy, 2009). Women are expected to act in good faith, develop more connections with others, and lie less (Weisberg, DeYoung, & Hirsh, 2011; Buchan, Croson, & Solnick, 2008; Schmitt, Realo, Voracek, & Allik, 2008). Although these characteristics of non-agentic behavior are not trust per se, they are important if the insurance firm is to understand how some policyholders are more trusted than others. Although women may be trusted to not lie, they aren't sometimes who they claim to be. This would imply that women may lose a full acknowledgement of their driving capabilities. Women are known to have little attitude and experience in driving (Lawrence, & Richardson, 2005) which is ideally at odds with the decision to adopt the black box device. Indeed, for bad drivers, the adoption of the black box would imply some drawbacks (such as higher premium) since the insurance firm can build a more accurate risk profile of the car driver.

We extend the same explanation to more experienced drivers who are likely to hold the illusion of better knowledge and control over a situation based on a longstanding driving experience. Several studies have shown that experience has a significant impact on the overconfidence bias (Kirchler, 2002; Heath, 1991). This may lead to underestimating the risk of a crash, thus taking a less safe driving behavior. In the short run, policyholders who perceive themselves to possess a better driving ability have the illusion of more control over their environment than they have. As a result, they don't have the incentive to be particularly cautious, nearly overlooking the actual traffic accident risk (Abbring, 2003).

What follows is that, under cognitive bias, the choice to adopt the black box does not provide a supporting cue to distinguish between low- and high-risk drivers from the group of women. It generates incorrect information accidentally presented as a fact. This argument is robust to alternative explanations. A possible alternative explanation concerns attraction for novelties. The effect of novelty is particularly prominent when a new technology is instituted (Seidel, & Greve, 2017; Agarwal, & Prasad 1998). In this vein, I compute again all models for a sub-sample of policyholders. I focus on policyholders who were acquired from 2015. This matches the launch date of the black box device by the insurance firm in 2015. At that time, policyholders might have been persuaded to adopt the black box following a massive marketing campaign or broker advice. In 2015, earlier black box adopters were 1.96% only. In later years, the total number increases to 2.97%. As

Table 3 illustrates, regression estimates are substantially the same for this sub-sample. This would mean that the overconfidence bias is a convincing explanation.

ROBUSTNESS CHECKS

In this section, I present some robustness checks for some key assumptions. First, I investigate whether the relationship between black box adoption and the likelihood of accidents is distorted by self-selection. Then, I model endogeneity in a couple of ways (instrumental variable and propensity score matching) to study the potential correlation with the error term.

Self-selection bias: A quasi-experimental control experiment

In the main data set, a sub-sample of 61,787 insurance policies is issued to corporate cars. For corporate cars, the choice to adopt the black box device is left to the employer, without involving employees. In my view, this sub-sample represents a quasi-natural experiment to investigate the issue of self-selection bias. Self-selection bias is common in any situation when the individual characteristics influence the choice of whether or not to enter into a group, causing undesirable conditions in the group itself (Heckman, 1976). Table 4 reports the estimates of Heckman's two-step model using a full-information maximum likelihood (Heckman, 1976). First, I compute a probit regression using car power (nKW) as an endogenous regressor representing driving over long distances which is presumably true for corporate cars. I find that corporate cars are relatively new (CarAge= -0.03, p=***), pay a higher insurance premium (Premium=0.88, p=***), commit more accidents in the last five years (PrevAcc= 0.08, p=***) and circulate more in high-traffic areas (IGeoAcc=0.00, p=***). Next, introducing the black box variable at the second-step model doesn't appear to have an impact on the likelihood of an accident (BB=0.04, p=0.03). The same result is found for the interaction terms (BBxPrevAcc, BBxIGeoAcc, and BBxPrevAccxIGeoAcc). Finally, the statistical significance of Heckman's coefficient (λ=0.01, p=***) informs that the sample of corporate cars behaves differently from individual policyholders. Overall, findings confirm that the adoption of the black box is not affected by the self-selection bias. I conclude that some unobserved factors are influencing the choice to adopt the black box. For example, it is the type of job that forces a greater usage of corporate cars which, in turn, may lead to a greater likelihood of an accident.

Endogeneity issue

Instrumental variables. For safer drivers, the adoption of black box devices is not expected to influence their driving behavior regarding a change in the likelihood of an accident. Therefore, given all the possible negative consequences, the black box nay be adopted by safer drivers only. I explicitly attempt to address this issue using an instrumental variable approach (Reiersøl, 1945; Sargan, 1958; Wright, 1928). This approach involves finding some variables that are sufficiently correlated with the black box adoption (BB is the endogenous regressor) but uncorrelated with the error term (Bascle, 2008; Nelson, & Startz, 1990). The Principal Component Analysis

(PCA) is used to reduce the dimensionality of instrumental variables (Kapetanios, & Marcellino, 2010; Amemiya, 1966; Kloek, & Menners, 1960). The instrumental variables are derived from three different domains: societal trust, accidentability, and general interest in the black box device (see Table 5 in Appendix C).

For the societal trust, the instrumental variables are represented by GeoBlood, GeoBikeLanes, GeoLenghtCourt, and GeoCarThefts. Panel (I) shows that there is no principal component with a proportion score less than 41% in explaining data. Because each principal component has an explanatory power that is not captured by the others, all social trust-related variables can be used as instrumental variables. I repeat the same computation for Italy accidentability in local areas. I find that two components (PC1 and PC2) explain more than 97% of the total variance. The first component (PCIGeoAcc) is positively related to all four accident variables (IGeoAcc, IGeoFatalities, IGeoInjured, and IGeoAccbyV). It captures the willingness of policyholders to report any accidents to the insurance firm, despite the accident severity. The second component (PCigeoclaim) behaves oppositely with a negative effect. Although low-severity accidents are not always claimed to the insurance firm, the same is not applied to fatalities as the actual damage cannot be hidden. Thus, that second component captures the willingness to report a severe claim. Finally, data from Google trends are used as an instrumental variable (BBGoogleT) to capture the geographical distribution of interest in the black box device among Italian policyholders. For all these instrumental variables, I suppose they affect both the choice to adopt the black box and the likelihood of an accident. Results are reported in Table 6 (see Appendix C).

In Model (1), the adoption of the black box is the dependent variable. I find that all the instrumental variables of societal trust are statistically significant with a negative effect. It means that the black box tends to be adopted in those geographical areas where the level of societal trust is low. This is also consistent with earlier findings in the economic literature (Coleman, 2000; Fukuyama, 1995; Nooteboom, 2007; Guiso et al., 2004). Also, PCIGoAcc and PCIGgeoClaim are statistically significant. The former shows that there is no incentive for adopting the black box in low-accidentability areas. The latter, on the other hand, has an opposite effect on the choice to adopt the black box. Finally, interest in the black box device is not surprisingly positive and statistically significant. In the Italian regions where the "black box" keyword is searched more on the web, the device is more likely to be adopted. Once controlling for BB as an endogenous variable, Model (2) illustrates that the adoption of the black box does not modify previous results, while negatively affecting the likelihood of accident (BB=0.41, p=***).

Propensity Score Matching. I employ a propensity score matching to estimate the impact of black box adoption on the likelihood of an accident. Using this matching, I adjust for the pre-treatment observable differences between the treated and untreated group (Caliendo, & Kopeinig, 2008). The black-box adopters are the treated group. For those, I measure the unconditional mean of accident likelihood which is equal to 8.88%. For black box non-adopters (untreated group) the unconditional mean of accident likelihood is 6.78%. Difference between means is highly significant using both a parametric (t-test = 14.72) and a non-parametric test (χ^2 -test = 41.26). These tests, however, might be distorted by the self-selection bias. As I have already discussed (see Table 5), the possibility of self-selection bias is not supported.

Starting from earlier logit regressions (see Model (2) in Table 6), I estimate the propensity score for the black box adopters by computing the Average Treatment Effect on the Treated estimation (ATT) using the Nearest Neighbor Matching method. Treated observations (nr. bb adopters =29,615) are matched with those similar observations from the control group (nr. bb non-adopters=61,862). The Average Treatment Effect on the Treated estimation (ATT) is -0.019 and statistically significant. The result remains statistically significant when computing analytical (t-test= -9.246) and bootstrapping standard errors test (t-test= -10.041). By comparing the average likelihood of accidents between black-box adopters and the matched control group, I find that the likelihood is lower for black-box adopters (1.9%). To sum up, results from Table 7 confirm the initial findings.

DISCUSSIONS

Adopting a black box is a rational choice to signal and screen themselves credibly. With black box, original claims of trustworthiness are continuously verified against real-time data on driving behavior. The informational value of the black box device comes from the fact that the insurance firm believes the black box device is positively correlated with having greater driving abilities. ‘Bad drivers’ would have no incentive to select the black box option. The latter is aware that the actual bad driving behavior will be publicly disclosed.

To confirm such an initial intuition, I employ data from multiple datasets. I propose a series of logit regressions aiming at examining the effect of black box adoption on the likelihood of accidents. Once controlling for several control variables, estimates are generally supportive. First, I find that the adoption of the black box is influential in areas of high accidentability. In those areas, the negative sign would imply that a black box is adopted to send a signal of trustworthiness because driving behavior is continuously verified. Thus, potential liars can be easily identified. Further analysis on a sub-sample of online policyholders corroborates these findings and demonstrates that the choice to adopt the black box is not caused by a persuasive action, but it is a real manifestation of trustworthiness. But, for women and more experienced drivers, the interpretation of the estimate is not so clear. i find that black box adopters from the group of women and experienced drivers are more likely to commit an accident. This seems to contrast existing literature on insurance (Lonczak, 2007; Yagil, 1998; Berger, 1986; Veevers, 1982). However, I discuss that one possible explanation is the possibility that the overconfidence bias exists. Thus, I perform some robustness tests which reject alternative confounding effects about the self-selection bias and endogeneity issue.

I recognize that my study contributes by modelling the black box in the theoretical framework of the economic literature on information asymmetry. Precisely, I discuss that the black box is effective in signaling and screening. By adopting the black box, ’good drivers’ are willing to share some private information with the insurance firm in return for a better premium. The premium is better because the risk classification is improved through the collection of unobservable data. It means that the sharing of private information is a beneficial action that may sustain the development of trust from the insurance firm to the policyholder. This suggests that economic transactions which may benefit more from technology are those affected by the problem of information asymmetry. In this vein, the present study is intended to provide the first contribution to this very recent research topic on digital technology. As an additional contribution, the findings reveal that such a kind of study may suffer from distortions in their estimates. This is due to some cognitive bias at work. Specifically, I discuss that the overconfidence bias may compromise the actual explanation of estimates, leading to unconsciously wrong signals. It means that the problem of adverse selection is not surpassed as the risk of overidentification continues to exist. Lastly, I see implications for managers operating in the automobile insurance industry. As demonstrated in this study, the black box may represent a significant predictor of policyholders’ trustworthiness in what they claim to be. Insurance firms interested in improving their risk framework should care for the black box for early identification of adverse selection following information asymmetry.

The study indicates several avenues for future research. As future research, I first invite scholars to replicate this empirical analysis in other settings being affected by the problem of information asymmetry. This would provide novel insights confirming the role of technology in the trust-building process. A suggestive scenario is testing my main thesis in the context of blockchain. With blockchain, economic transactions with unknown traders are completely disintermediated by the technology itself. The level of trust in the blockchain's correct functioning is a precondition for a transaction to occur under reciprocal beliefs of verified trustworthiness. Further, since the data set does not contain data before the introduction of black box, I believe that a longer panel may help to examine changes in the driving behavior over time. This would mean to account for the effect of learning in situations of severe information asymmetry. Also, authors should think about including the black box data on the actual driving performance (driving speed, braking system, covered distance, etc.). This would add a richer informational background for a more accurate analysis of the driver's behaviors, especially when the insurance company decides to share this data with policyholders to help them to drive more safely. Lastly, I bring attention to two additional avenues for future research. The first is about testing more in depth the overconfidence bias. Authors, for example, may replicate the present study introducing primary data of individual overconfidence bias to confirm my intuition about the unexpected results in statistical ways. Next, authors may extend this test beyond the Italy market and propose a comparative study about different policyholders' behavioral response to black box. This would provide some informative results about the role of cultural background.

REFERENCES

Abbring, J. H., Chiappori P. A., & Pinquet J. (2003). Moral hazard and dynamic insurance data. Journal of the European Economic Association, 1, 767-820.

Acemoglu, D., & Johnson S. (2005). Unbundling Institutions. Journal of Political Economy, 113, 949-995.

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. Information systems research, 9(2), 204-215.

Aggarwal, R., Goodell J. W., & Selleck L. J. (2015). Lending to women in microfinance: Role of social trust. International Business Review, 24, 55-65.

Akerlof, G. A. (1970). The market for" lemons": Quality uncertainty and the market mechanism. The Quarterly Journal of Economics, 84, 488-500.

Amemiya, T. (1966). On the use of principal components of independent variables in two-stage least-squares estimation. International Economic Review, 7, 283-303.

Anderson, L. R., & Blanchard P. N. (1982). Sex differences in task and social emotional behavior. Basic and Applied Social Psychology, 3, 109-139.

Arrow, K. J. (1972). Gifts and Exchanges. Philosophy and Public Affairs, 1, 343-362.

Bachmann, R., & Inkpen A. C. (2011). Understanding institutional-based trust building processes in inter-organizational relationships. Organization studies, 32, 281–30.

Bascle. G. (2008). Controlling for endogeneity with instrumental variables in strategic management research. Strategic Organization, 6(3), 285-327.

Barber, W. R. (1983). Toward understanding the role of auditing in the public sector. Journal of Accounting and Economics, 5, 213-227.

Berger, M. L. (1986). Women drivers!: The emergence of folklore and stereotypic opinions concerning feminine automotive behavior. Women's Studies International Forum, 9, 257-263.

Buchan, N. R., Croson R. T. A., & Solnick S. (2008). Trust and gender: An

examination of behavior and beliefs in the investment game. Journal of Economic Behavior & Organization, 68, 466-476.

Calcagnini, G., & Perugini F. (2019) Social capital and well-being in the italian provinces. Socio-Economic Planning Sciences, 68, 100668.

Caliendo M., & Kopeinig, S. (2008). Some practical guidance for the implementation of propensity score matching. Journal of Economic Surveys, 22(1), 31-72.

Carson, S. J., Madhok A., & Wu T. (2006). Uncertainty, opportunism, and governance: The effects of volatility and ambiguity on formal and relational contracting. Academy of Management Journal, 49, 1058-1077.

Cartocci, R. (2007), Mappe del tesoro. Atlante del capitale sociale in Italia, Bologna, il Mulino.

Chiappori, P. A., & Salanié, B. (1997). Empirical contract theory: The case of insurance data. European Economic Review, 41(3-5), 943-950.

Chiappori, P. A., & Salanié, B. (2000). Testing for asymmetric information in insurance markets. Journal of political Economy, 108(1), 56-78.

Cohen, A. (2005). Asymmetric information and learning: Evidence from the automobile insurance market. Review of Economics and Statistics, 87, 197-207.

Coleman, J. S. (2000). Foundations of Social Theory, Cambridge: Harvard University Press.

Cook, K. S., & Cooper, R. M. (2003). Experimental studies of cooperation, trust, and so cial exchange, In E. Ostrom J. Walker (Eds.), Trust and reciprocity: Interdisciplinary lessons from experimental research. Russell Sage Foundation, 209-244.

Croson, R., & Buchan, N. (1999). Gender and culture: International experimental evidence from trust games. American Economic Review, 89, 386-391.

Croson, R., & Gneezy U. (2009). Gender differences in preferences. Journal of Economic Literature, 47, 448-74.

Cooper, R., & Hayes B. (1987). Multi-period insurance contracts. International Journal of Industrial Organization, 5, 211–231.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, 101284.

Crocker, K. J., & Snow A. (1985). The efficiency of competitive equilibria in insurance markets with asymmetric information. Journal of Public Economics 26, 207-219.

Dionne, G., & Lasserre P. (1985). Adverse selection, repeated insurance contracts and announcement strategy. Review of Economic Studies, 52, 719-723.

Dionne, G., & Vanasse C. (1992). Automobile insurance ratemaking in the presence of asymmetrical information. Journal of Applied Econometrics, 7, 149-165.

Dionne, G., & Doherty N. A. (1994). Adverse selection, commitment, and renegotiation: Extension to and evidence from insurance markets. Journal of Political Economy, 102, 209–235.

Dionne, G., Gouriéroux, C., & Vanasse, C. (1996). Evidence of Adverse SelectioninAutomobileInsuranceMarkets. MimeO.(CREST Paris).

Dionne, G., Gouriéroux, C., & Vanasse, C. (2001). Testing for evidence of adverse selection in the automobile insurance market: A comment. Journal of Political Economy, 109(2), 444-453.

Dionne, G., Michaud, P. C., & Dahchour, M. (2013). Separating moral hazard from adverse selection and learning in automobile insurance: longitudinal evidence from France. Journal of the European Economic Association, 11(4), 897-917.

Dominguez, S., & Watkins C. (2003). Creating networks for survival and mobility: Social capital among African-American and Latin-American low-income mothers. Social Problems 50, 111-135.

Donaldson, L., & Davis J. H. (1991). Stewardship theory or agency theory: CEO governance and shareholder returns. Australian Journal of management, 16, 49-64.

Doney, P. M., Cannon J. P., & Mullen M. R. (1998). Understanding the influence of national culture on the development of trust. Academy of Management Review, 23, 601—620.

Fukuyama, F. (1995). Trust: The Social Virtues and the Creation of Prosperity, New York: Free Press.

Gambetta, D. (1988). Can We Trust?, In: Trust: Making and Breaking Cooperative Relations, edited by Gambetta, D., Oxford: Basil Blackwell.

Geyer, A., Kremslehner, D., & Muermann, A. (2020). Asymmetric information in automobile insurance: Evidence from driving behavior. Journal of Risk and Insurance, 87(4), 969-995.

Granovetter, M. (1985). Economic action and social structure: The problem of embedded ness. American journal of sociology, 91, 481-510.

Grootaert, C. (2003). Measuring social capital: An integrated questionnaire. World Bank Publications, 18.

Guiso, L., Sapienza P., & Zingales L. (2004). The role of social capital in financial development. American Economic Review, 94, 526-556.

Guiso, L., Sapienza P., & Zingales L. (2008). Trusting the Stock Market. The Journal of Finance, 63, 2557-2600.

Guiso, L., Sapienza, P., & Zingales, L. (2009). Cultural biases in economic exchange?. The quarterly journal of economics, 124(3), 1095-1131.

Guiso, L., Sapienza P., & Zingales L. (2011). Civic capital as the missing link. Handbook of Social Economics, 1, 417-480.

Guiso L. (2016). Long-term persistence. Journal of the European Economic Association, 14, 1401-1436.

Gulati, R. (1995). Social structure and alliance formation patterns: A longitudinal analysis. Administrative Science Quarterly, 619-652.

Heath, C., & Tversky A. (1991). Preference and belief: Ambiguity and competence in choice under uncertainty. Journal of risk and uncertainty, 4, 5-28.

Heckman, J. (1976). The common structure of statistical models of truncation, sample selection and limited dependent variables and a simple estimator for such models, In Annals of Economic and Social Measurement, 5(4), 475–492 (National Bureau of Economic Research, Inc).

Helliwell, J. F., & Putnam R. D. (1995). Economic growth and social capital in Italy. Eastern Economic Journal, 21, 295-307.

Hoy, M. (1982). Categorizing risks in the insurance industry. The Quarterly Journal of Economics 97, 321-33.

Kar, A. K., & Bali Swain R. B. (2014). Interest rates and financial performance of microfinance institutions: Recent global evidence. The European Journal of Development Research, 26, 87-106.

Kapetanios, G., & Marcellino, M. (2010). Factor-GMM estimation with large sets of possibly weak instruments manuscript. Computational Statistics and data Analysis, 54, 2655-2675.

Kirchler, E., & Maciejovsky B. (2002). Simultaneous over-and underconfidence: Evidence from experimental asset markets. Journal of risk and uncertainty, 25, 65-85.

Kloek, T., & Mennse, L. B. M. (1960). Simultaneous equations estimation based on principal components of predetermined variables. Econometrica, 28, 45-61.

Lawrence, C., & Richardson J. (2005). Gender-Based Judgments of Traffic Violations: The Moderating Influence of Car Type. Journal of Applied Social Psychology, 35, 1755-1773.

Lewicki, R. J., McAllister D. J., & J Bies R. J. (1998). Trust and distrust: New relationships and realities. Academy of Management Review, 23, 438-458.

Lyons, B., & J. Mehta (1997). Contracts, opportunism and trust: self-interest and social orientation. Cambridge journal of economics, 21, 239-257.

Lonczak, H. S., Neighbors C., & Donovan D. M. (2007). Predicting risky and angry driving as a function of gender. Accident Analysis Prevention 39, 536-545.

Macaulay, S. (1963). Non-contractual relations in business: A preliminary study, In Stew art Macaulay: Selected Works. Springer, Cham. 361-377.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709-734.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. Academy of Management Review, 23(3), 473-490.

Mollering, G. (2006). Trust: Reason, routine, reflexivity. Emerald Group Publishing.

Moore, D. A., & Healy P. J. (2008). The trouble with overconfidence. Psychological Review, 115, 502-517.

Mowbray, A. H, & Blanchard R. H. (1961). Insurance: Its Theory and Practice in the United States (5th ed.), New York: McGraw-Hill.

Muermann, A., & Straka, D. (2011). Asymmetric information in automobile insurance: new evidence from telematic data. Working paper, Vienna University of Economics and Business.

Nelson, C.R., & Startz, R. (1990). Some further results on the exact small sample properties of the instrumental variable estimator. Econometrica, 58(4), 967-76.

Noordewier, T. G., John, G., & Nevin J. R. (1990). Performance outcomes of purchasing arrangements in industrial buyer-vendor relationships. Journal of Marketing, 54, 80-93.

Nooteboom, B. (2007). Social capital, institutions and trust. Review of Social Economy, 65, 29–53.

Petersen, M. A. (2008). Estimating Standard Errors in Finance Panel Data Sets: Comparing Approaches. The Review of Financial Studies, 22, 435-480.

Pinquet, J. (2000). Experience Rating through Heterogeneous Models, In Handbook of Insurance, G. Dionne (ed.), Kluwer Academic Publishers, Boston.

Pinquet, J. (2005). Une Analyse des Syst`emes bonus-malus en Assurance Automobile. Assurances, 67, 241—249.

Putnam, R. D. (1993). What makes democracy work?. National Civic Review, 82, 101–107.

ReiersØl, O. (1945). Confluence analysis by means of instrumental sets of variables. Arkiv for Mathematik Astronomi och Fysik, 32a(4), 1-119.

Richaudeau, D. (1999). Automobile insurance contracts and risk of accident: An empirical test using French individual data. The Geneva Papers on Risk and Insurance Theory, 24, 97-114.

Ring, P. S., & Van de Ven A. H. (1992). Structuring cooperative relationships between organizations. Strategic Management Journal, 13, 483-498.

Rothschild, M. (1978). Searching for the lowest price when the distribution of prices is unknown. In Uncertainty in Economics (pp. 425-454). Academic Press.

Rothschild, M., & Stiglitz J. (1976). Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information. The Quarterly Journal of Economics, 90, 629-649.

Rothschild, M., & Stiglitz, J. (1978). Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. In Uncertainty in economics (pp. 257-280). Academic Press.

Rosenberg, R., Gonzalez A., & Narain S. (2009). The new moneylenders: Are the poor being exploited by high microcredit interest rates?, In Moving beyond storytelling: Emerging research in microfinance. Emerald Group Publishing Limited.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. Journal of Personality.

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. American Psychologist, 26, 443.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. Academy of Management Review, 23(3), 393-404.

Sargan, J. D. (1958). The estimation of economic relationships using instrumental variables. Econometrica, 26(3), 393-415.

Schmitt, D. P, Realo A., Voracek M., & Allik J. (2008). Why can't a man be more like a woman? sex differences in big five personality traits across cultures. Journal of Personality and Social Psychology, 94, 168.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. Academy of Management Review, 32(2), 344-354.

Seidel, M. D. L., & Greve, H. R. (2017). Emergence: How novelty, growth, and formation shape organizations and their ecosystems, In Emergence. Emerald Publishing Limited.

Shavell, S. (1979). On moral hazard and insurance, In Foundations of insurance economics. Springer, Dordrecht, 280-301.

Sitkin, S. B., Weingart L. R. (1992). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. Academy of Management Journal, 38, 1573—1592.

Sitkin, S. B, & Roth N. L. (1993). Explaining the limited effectiveness of legalistic “remedies” for trust/distrust. Organization science, 4, 367-392.

Smitka, M. (1975). Markets and hierarchies, In O. E. Williamson (Eds.), Markets and hierarchies. New York: Free Press.

Smitka, M. 1994. Contracting without contracts: How the Japanese manage organizational transactions. In S. B. Sitkin & R. J. Bies (Eds.), The legalistic organization: 91-108. Thousand Oaks, CA: Sage.

Spence, M. (1973). Job Market Signaling. Quarterly Journal of Economics, 87, 355-374.

Svenson, O. (1981). Are e all less risky and more skilful than our fellow drivers?. Acta Psychologica, 47, 143-148.

Tabellini, G. (2008). Institutions and Culture. Journal of the European Economic Association, 6, 255–294.

Thompson, S. B. (2011). Simple formulas for standard errors that cluster by both firm and time. Journal of Financial Economics, 99, 1–10.

Van Den Akker, O. R., van Assen M. A., Van Vugt M., & Wicherts J. M. (2020) Sex differences in trust and trustworthiness: A meta-analysis of the trust game and the gift-exchange game. Journal of Economic Psychology, 81.

Veevers, J. (1982). Women in the driver’s seat: Trends in sex differences in driving and death. Population Research and Policy Review, 1, 171-182.

Weisberg, Y. J., DeYoung C. G., & Hirsh J. B. (2011). Gender differences in personality across the ten aspects of the big five. Frontiers in Psychology 2, 178.

Wright, P. G. (1928). The tariff on animal and vegetable oil. New York, Macmillan.

Wright, T. L., & Sharp E. G. (1979). Content and grammatical sex bias on the interpersonal trust scale and differential trust toward women and men. Journal of Consulting and Clinical Psychology, 47, 72.

Williamson, O. E. (1991). Comparative economic organization: The analysis of discrete structural alternatives. Administrative Science Quarterly, 269-296.

Yagil, D. (1998). Gender and age-related differences in attitudes toward traffic laws and traffic violations. Transportation Research Part F: Traffic Psychology and Behaviour, 1, 123-135.

Wilson, C. (1977). A model of insurance markets with incomplete information. Journal of Economic theory, 16(2), 167-207.

Wollner, K. S. (1999). How to Draft and Interpret Insurance Policies Casualty Risk. Publishing LLC.

Zaheer, A., McEvily B., & Perrone, V. (1998). The strategic value of buyer supplier relationships. International Journal of Purchasing and Materials Management, 34, 20–26.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure. Research in organizational behavior, 1840-1920.

APPENDIX A

Variable name

Accidents	Number of accidents
Gender	Female
Age	Age 18 - 65+
CarAge	Age 0 - 9+
PrevAcc	Number of accidents
Premium	Amount of money for an insurance policy
Petrol	Petrol car powered
Diesel	Diesel car powered
Electric	Electric car powered
LPG	LPG car powered
Methane	Methane car powered
Online	Online policy subscription
Corporate	Corporate car
GeoTrust	
GeoBlood	Nr. Blood donation per mln inhabitants
GeoBikeLanes	Km bike lanes per 100 Km^2
GeoLenghtCourt	Nr. days before a first-instance ordinary court proceedings
GeoCarThefts	Nr. CarThefts per mln inhabitants
GeoAccidents (ISTAT)	
IGeoAcc	Accidents per 100,000 inhabitants in a specific area
IGeoFatalities	Fatal accidents per 100,000 inhabitants in a specific area
IGeoInjured	Injured accidents per 100,000 inhabitants in a specific area
IGeoAccidentsByV	Accidents per 10,000 vehicles in a specific area

GeoBBAttention (GTrends)	
BBGoogleT	Google trends for “black box” web searches

APPENDIX B

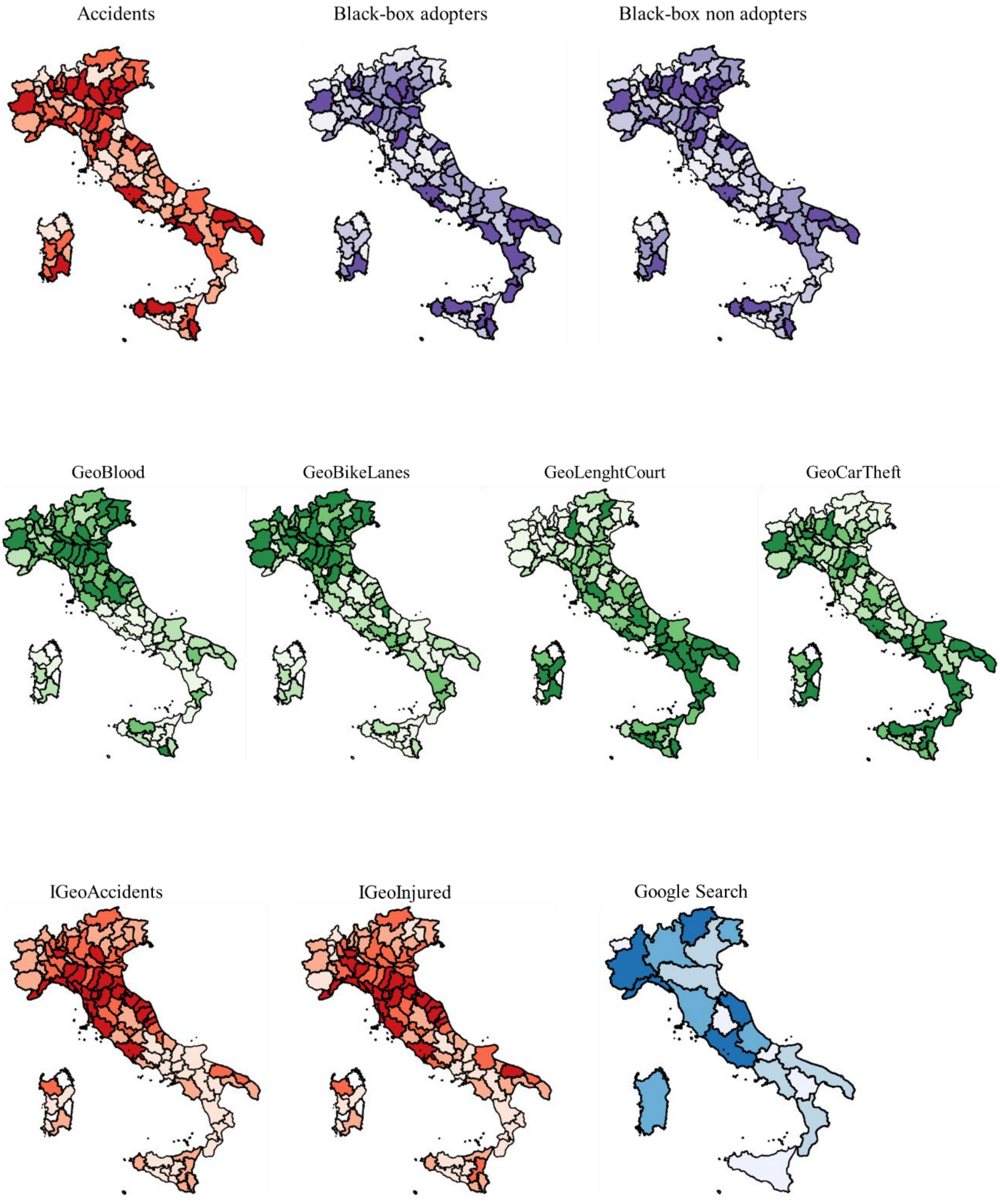

Figure 1: Geographical distribution of accidents, black-box adoption, societal trust, and black-box interest

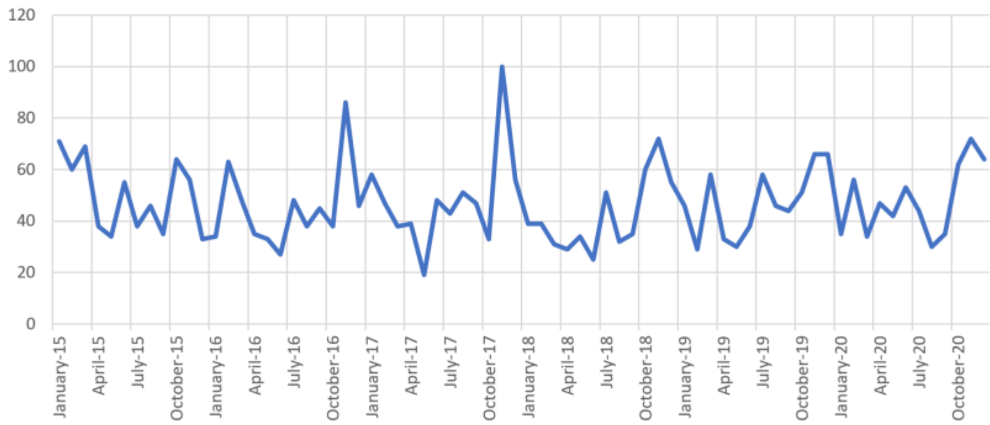

Figure 2: Monthly trends in people's search of the "black box" keyword within Google Search from 2015 to 2020.

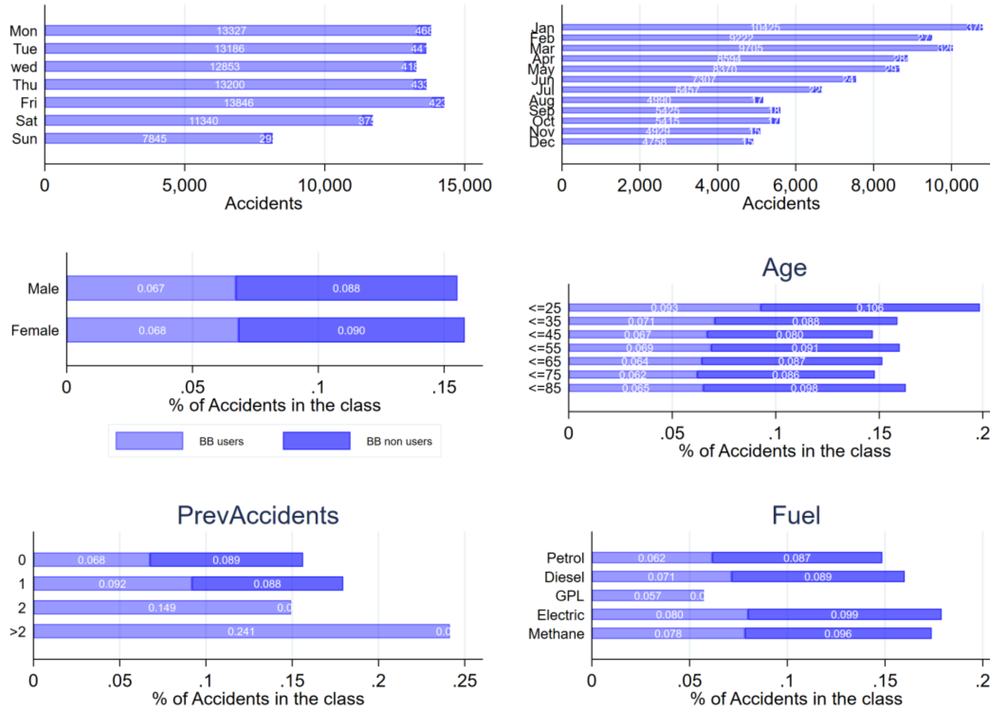

Figure 3: Observable characteristics within black box adopters. Distribution of accidents by time (per day and month), gender, age, and car fuel.

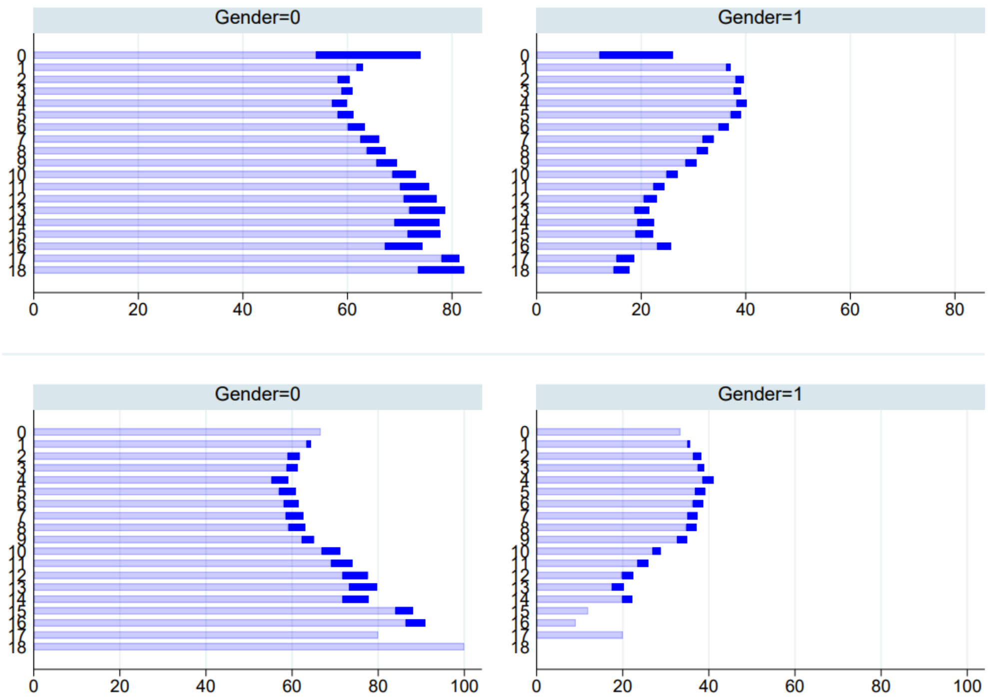

Figure 4: Distribution of policyholders' risk class (0 low-risk; 18 high-risk), distinguishing per gender (1 female; 0 male) and black box adoption (light blue bb non-adopter; blue bb adopters). The upper figures refer to the full sample while the bottom figures refer to online subscribers.

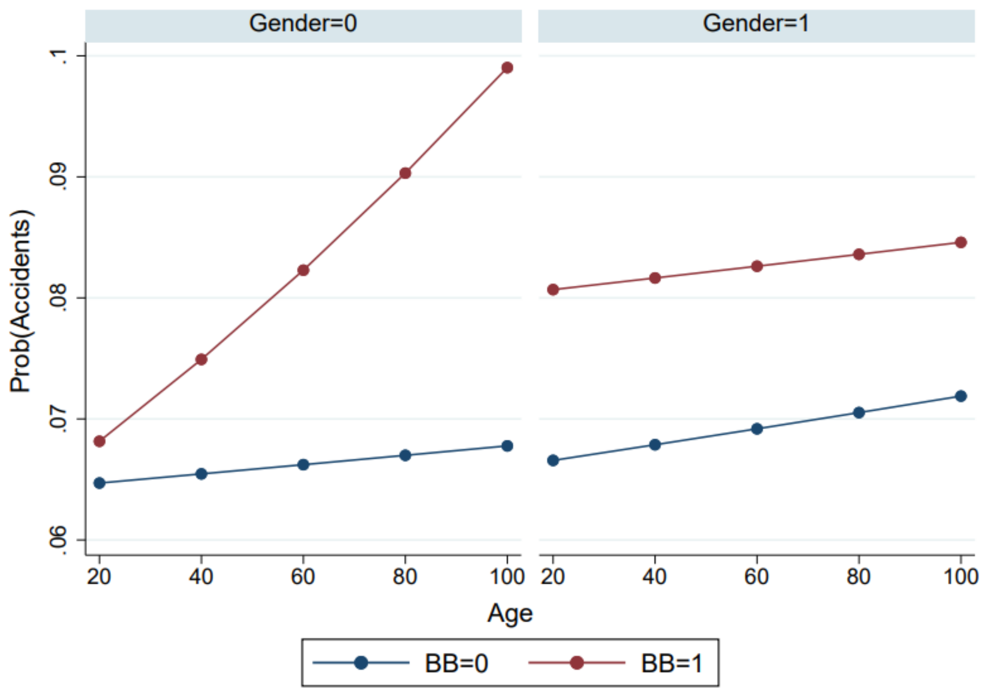

Figure 5: Predicted margins of accidents based on black-box adoption, gender, and driving experience (age).

APPENDIX C

	μ	med	σ	min	max
Acc	0.07	0.00	0.25	0.00	1.00
BB	0.02	0.00	0.16	0.00	1.00
Gender	0.36	0.00	0.48	0.00	1.00
Age	54.36	54.00	14.98	16.00	114.00
CarAge	8.89	9.00	5.95	0.00	82.00
PrevAcc	0.00	0.00	0.06	0.00	6.00
Premium	5.80	5.76	0.40	0.06	8.14
Petrol	0.44	0.00	0.50	0.00	1.00
Diesel	0.49	0.00	0.50	0.00	1.00
Electric	0.00	0.00	0.02	0.00	1.00
LPG	0.04	0.00	0.20	0.00	1.00
Methane	0.02	0.00	0.15	0.00	1.00
Online	0.18	0.00	0.30	0.00	1.00
Corporate	0.05	0.00	0.21	0.00	1.00
GeoTrust:					
GeoBlood	36.91	0.00	13.91	0.00	84.80
GeoBikeLanes	15.99	0.00	18.97	0.00	76.57
GeoLenghtCourt	1033.25	0.00	342.19	0.00	1947.83
GeoCarTheft	336.09	0.00	268.86	0.00	1061.80
GeoAcc:					
IGeoAcc	294.04	264.83	102.44	105.61	584.02
IGeoFatalities	5.28	4.74	1.63	2.57	10.89
IGeoInjured	414.07	370.77	112.46	162.95	709.84
IGeoAccByV	34.62	31.03	12.65	10.68	69.98
GeoBBAttention:					
BBGoogleT	50.62	47.00	22.39	0.00	100.00

Table 1: Summary statistics: means (μ), median (med), standard deviation (σ), minimum (min), and maximum value (max).

	BB=1		BB=0					
	μ	med	μ	med	t-test		X^2-test	
Acc	0.09	0.00	0.07	0.00	-14.72	***	41.26	***
Gender	0.37	0.00	0.36	0.00	-3.32	***	7.45	***
Age	49.32	49.00	54.44	54.00	54.38	***	-0.09	***
CarAge	7.75	7.00	8.91	9.00	34.68	***	1109.00	***
PrevAcc	0.00	0.00	0.00	0.00	0.52		6807.27	***
Premium	5.99	6.00	5.80	5.76	-82.76	***	-82.76	***
Petrol	0.35	0.00	0.45	0.00	33.83	***	846.97	***

Diesel	0.57	1.00	0.49	0.00	-29.28	***	642.14	***
Electric	0.00	0.00	0.00	0.00	1.09		-0.33	
LPG	0.05	0.00	0.04	0.00	-8.00	***	7.69	***
Methane	0.03	0.00	0.02	0.00	-3.65	***	0.88	
Online	0.16	0.00	0.18	0.00	10.55	***	50.49	***
Corporate	0.07	0.00	0.05	0.00	-3.22	***	68.78	***
GeoTrust:								
GeoBlood	34.65	30.30	36.97	37.90	29.44	***	1509.15	***
GeoBikeLanes	13.99	4.77	16.04	5.43	19.07	***	251.14	***
GeoLenghtCourt	1105.84	1054.75	1031.58	997.67	-38.34	***	1089.57	***
GeoCarTheft	399.56	350.17	334.19	268.83	-42.99	***	2177.34	***
GeoAcc:								
IGeoAcc	275.44	248.12	294.40	264.83	32.72	***	969.15	***
IGeoFatalities	5.04	4.70	5.29	4.87	27.37	***	823.94	***
IGeoInjured	398.18	369.23	414.35	374.16	25.41	***	450.67	***
IGeoAccByV	33.18	29.13	34.64	31.03	20.41	***	387.83	***
GeoBBAttent:								
BBGoogleT	47.93	46.00	50.68	47.00	21.68	***	360.84	***

Table 2: Black box subsamples: summary statistics between black box adopters (32,136) and non-adopters (1,269,750). Difference tested by t-test and χ-test wih significance code at: * p<0.10, ** p<0.05, *** p<0.01.

	(1)	(2)	(3)	(4)	(5)
	All	All	All	All	Online
BB	0.19***	0.19***	-0.03	-0.18**	-0.58*
	(0.03)	(0.02)	(0.11)	(0.08)	(0.15)
Gender		0.04***	0.04***	0.04***	0.06**
		(0.01)	(0.01)	(0.01)	(0.02)
Age		0.00***	0.00***	0.00***	0.00
		(0.00)	(0.00)	(0.00)	(0.00)
BBxGender			0.23**	0.23**	0.55*
			(0.11)	(0.11)	(0.31)
BBxAge			0.00*	0.00*	0.01*
			(0.00)	(0.00)	(0.01)
BBxGenderxAge			-0.00*	-0.00*	-0.01
			(0.00)	(0.00)	(0.01)
BBxPrevAcc				-0.18	
				(0.64)	
BBxIGeoAcc				0.00***	0.00***
				(0.00)	(0.00)

BBxPrevAccxIGeoAcc				-0.01 (0.01)	
RiskClass	0.00* (0.00)	0.00* (0.00)	0.00* (0.00)	0.00* (0.00)	-0.00 (0.001)
PrevAcc	0.21*** (0.05)	0.22*** (0.07)	0.22*** (0.07)	0.23*** (0.07)	
IGeoAcc	0.00*** (0.00)	0.00*** (0.00)	0.00*** (0.00)	0.00*** (0.00)	0.00*** (0.00)
CarAge	-0.02*** (0.00)	-0.02*** (0.00)	-0.02*** (0.00)	-0.02*** (0.00)	-0.02*** (0.00)
Premium	0.46*** (0.02)	0.49*** (0.02)	0.49*** (0.02)	0.49*** (0.02)	0.55** (0.08)
Constant	-5.22*** (0.14)	-5.40*** (0.17)	-5.40*** (0.17)	-5.39*** (0.17)	-6.10 (0.55)
GeoBBAttention:	1,234,89	1,234,89	1,234,89	1,234,89	227,532
Dummy fuel	YES	YES	YES	YES	YES
Dummy year	YES	YES	YES	YES	YES

Table 3: Logit model estimates on the likelihood of an accident. Each model accounts for within-cluster correlations.

	(1)	(2)
	Corporate	Accident
KW	0.01*** (0.00)	
BB		0.04 (0.03)
BBxPrevAcc		-0.11 (0.62)
BBxIGeoAcc		-0.00 (0.00)
BBxPrevAccxIGeoAcc		-0.00 (0.00)
CarAge	-0.03*** (0.00)	-0.00*** (0.00)
Premium	0.88*** (0.01)	0.02* (0.00)
PrevAcc	0.08*** (0.03)	0.02* (0.01)
IGeoAcc	0.00*** (0.00)	0.00*** (0.00)
λ		0.01** (0.00)
Constant	-7.41***	-0.09***

	(0.03)	(0.03)
Observations	1,286,743	1,286,743
Dummy fuel	YES	YES
Dummy year	YES	YES

Table 4: Robustness check. Test for the Heckman's model (1976) self-selection bias: a quasi-natural experiment with corporate cars**,** based on unit-cluster standard errors. Significance code: * p<0.10, ** p<0.05, ***p<0.01.

Panel I: GeoTrust	Eingenvalue	Proportion	Cumulative	
PC1	1.659	0.414	0.414	
PC2	0.966	0.241	0.656	
PC3	0.799	0.200	0.856	
PC4	0.574	0.144	1.000	
eingenvectors	PC1	PC2	PC3	PC4
GeoBlood	0.484	0.326	0.756	-0.293
GeoBikeLanes	0.564	0.400	-0.276	0.667
GeoLenghtCourt	-0.569	0.157	0.531	0.607
GeoCarTheft	-0.350	0.841	-0.262	-0.318
Panel II: GeoAcc	Eingenvalue	Proportion	Cumulative	
PC1=PCIGeoAcc	2.965	0.741	0.741	
PC2=PCIGeoClaim	1.047	0.236	0.978	
PC3	0.066	0.016	0.994	
PC4	0.020	0.005	1.000	
eingenvectors	PC1	PC2	PC3	PC4
IGeoAcc	0.573	-0.085	-0.328	0.7457
IGeoFatalities	0.165	0.984	0.054	0.0095
IGeoInjured	0.572	-0.063	-0.482	-0.660
IGeoAccByV	0.562	-0.138	0.810	-0.091

Table 5: Robustness check. Estimates of PCA applied to the geographical distribution of social capital and local accidents following PCA estimates.

	(1)	(2)	(3)	(4)
	BB	Accident	BB	Accident
BB		0.41*** (0.14)		-4.32*** (0.28)
GeoBlood	-0.00*** (0.00)			
GeoBikeLane	-0.00***			

	(0.00)			
GeoLenghtCourt	0.00***			
	(0.00)			
GeoCarTheft	0.00***			
	(0.00)			
BBGoogleT	0.00***			
	(0.00)			
Online	-0.00***			
	(0.00)			
Age	-0.00***	0.00***	-0.00***	-0.00
	(0.03)	(0.01)	(0.03)	(0.01)
Gender	0.00***	0.02***	0.00***	0.03***
	(0.00)	(0.00)	(0.00)	(0.01)
PrevAcc	-0.01***	0.13**	-0.00	0.01
	(0.00)	(0.03)	(0.01)	(0.09)
Premium	0.03***	0.23***	0.04***	0.36***
	(0.00)	(0.01)	(0.00)	(0.01)
CarAge	-0.00***	-0.01***	-0.00***	-0.01***
	(0.00)	(0.00)	(0.00)	(0.00)
Constant	-0.10***	-2.81***	-0.15***	-3.12***
	(0.00)	(0.03)	(0.01)	(0.08)
Observations	1,207,657	1,207,657	225,287	225,287
Dummy fuel	YES	YES	YES	YES
Dummy year	YES	YES	YES	YES

Table 6: Robustness check. Instrumental variables with BB as endogenous regressor. Probit Model (1) estimates the likelihood of black box adoption; in Model (2) BB is dealt with as endogenous regressors. Model (3) and (4) exclude online subscribers. Significance code: * p<0.10, ** p<0.05, ***p<0.01.

	N				
	Treated	Control	ATT	S.E.	t
Nearest Neighbor					
analytical	29,615	61,862	0.019	0.002	-9.246
bootstrapping	29,615	61,862	0.019	0.002	-10.041
Stratification					
analytical	29,615	1,195,218	0.019	0.002	-9.246
bootstrapping	29,615	1,195,218	0.019	0.002	-16.228

Table 7: Robustness check. Propensity Score Matching: Average Treatment Effects (ATT) on the Treated estimation with the Nearest

Neighbour Matching and stratification method about the black box adoption. Significance code: * p<0.10, ** p<0.05, ***p<0.01.