Code-based Trust Systems: An Integrative Model of How Rules of Code can Build Trust in Digital Transactions

Dr. Maria Sciarra *m.sciarra@ice.it*
Italian Trade & Investment Agency
Italy

Abstract

Rules-of-code are written logical instances of computing law constraining human action in a step-by-step finite sequence of actions so as to bear a sense of good faith and fair dealing behavior. Actual research on emerging technologies such as blockchain and artificial intelligence supports the view that the underlying rules-of-code influence the coordination of transactions. Emerging as a new category of institutional governance mechanism, the rules-of-code are hence becoming the primary object of trust. This paper draws attention to the implications of the rules-of-code for the trust-building process. Building on a systematic survey of the literature on institution-based trust, we capture those trusting concepts particularly relevant for developing a model of code-based trust. Contributions from the psychological theory of rule-governed behavior help better defining some trusting elements and their mutual relations.

Keywords: Institution-based Trust, Rule-governed Behavior, Credibility, Blockchain, Artificial Intelligence, Digital Economy.

1. INTRODUCTION

Trust is a central concept in organizational contexts of transactions between persons, groups or organization’s members. Trust encompasses both intrinsic and extrinsic types of willingness to reduce risks as well as transaction costs, even in conditions of uncertainty (Rousseau et al, 1998; Nooteboom, 2007).As an intrinsic willingness, trust breaks down at the micro level of transactions, where it takes the form of relation-based trust behaviors (Mayer, Davis, & Schoorman, 1995). As an extrinsic willingness, trust takes the form of institution-based trust. Institution-based trust involves a reasoned willingness to securely engage in any kind of transaction because of institutional governance mechanisms providing structural assurance and situational normality (Zucker, 1986; Shapiro, 1987; McKnight, Cummings, & Chervany, 1998). While most academic studies have focused on relation-based trust; current trends in organizational research are increasingly exploring institutional systems of code-based trust Lumineau, Wang & Schilke, 2021; Murray, Rhymer, & Sirmon, 2021). For instance, one trend in blockchain and artificial intelligence suggests that emerging technologies serve as an institutional governance mechanism to better support a sense of good faith and fair dealing behavior (Glynn & Kashin, 2018; De Filippi, Mannan, & Reijers, 2020; Lumineau, Wang & Schilke, 2021; Murray, Rhymer, & Sirmon, 2021). Compared to other traditional governance mechanisms, the underlying rules-of-code are expected to instill a higher level of perceived situational normality and structural assurance to the extent future facts are predictable (Davidson, De Filippi, & Potts, 2018; De Filippi, Mannan, & Reijers, 2020; Lumineau, Wang & Schilke, 2021). Expectations about the rules-of-code greatly increase the implication of a certain level of trust (De Filippi, Mannan, & Reijers, 2020; Lumineau, Wang & Schilke, 2021; Wong et al., 2024).

Although the topic of trust in the rules-of-code has been generating increased academic debate, research has tended just to mention trust in the rules-of-code as unavoidable ingredient of digital transactions. Some researchers have lamented that there is a need of a clear understanding of trust in the rules-of-code (De Filippi, Mannan, & Reijers, 2020; Glikson, & Wooley, 2020; Lumineau, Wang & Schilke, 2021; Wong et al., 2024). Considering this gap, the purpose of this article is to provide a definition of trust in the rule-of-code together with a presentation of a code-based trust model. Giving that the shift of the action repertoire from humans to a system of rules-of-code makes rules-of-code and institutions comparable, we refer to the literature of institution-based trust as the theoretical framework. Following an analytical procedure, we survey the literature of institution-based trust with specific regard to institutional credibility as important cue to evaluate the role of institutions for the trust-building process. This helps us to delineate the conceptual boundaries of trust in the rules-of-code. Thus, we have come to define trust in the rules-of-code as the willingness to depend on the rules-of-code, which impart a feeling of relative security. Then, we provide a complete integrative model of code-based trust including causal relations between trust in the rules-of-code, its antecedents, and its outcomes. Next contributions from the psychological theory of rule-governed behavior provide an additional ground to dig out how trust in the rules-of-code originates. In the latter theory, the perceived credibility characteristics of rules are a key concept for explaining the willingness to trust a rule-based system (Zettle, & Hayes, 1982; Skinner, 1984; Hayes, Zettle, & Rosenfard, 1989). Three characteristics –functionality, fairness, and immediacy –appear to reliably reflect antecedents to trust a code-based system and be related to agents' propensity to trust.

The contributions of our research are threefold. First, we deal with the challenge of rethinking how new digital technologies are impacting a social phenomenon like trust. Our consideration of the rules-of-code as a type of institution provides some useful insights into how this relational model can alter the way economic agents interact and build trust within a digital environment. Second, our study makes a more general contribution to the established literature of institution-based trust. As we argue throughout this paper, the psychology-oriented literature of rule-governed behavior provides an innovative foundation for investigating the role of an institutionalized system of rules in the trust-building process. In our view, that psychological dimension shapes the definition of an impersonal form of trust through its antecedents. The identification of characteristics related to a technology's credibility is a major novelty that we introduce with respect to the study of trust based on the rules-of-code construct and its causes. The findings highlight the importance of building trust based on different cognitive facets. Lastly, our study has practical managerial implications. Our work offers a valuable perspective for practitioners who are seeking an enhanced understanding of the implications and benefits of technology driven interactions for the trust-building process (Hawlitschek, Notheisen, & Teubner, 2018; Lukyanenko et al., 2022; Tan & Saraniemi, 2023; Bostrom et al., 2024).

The study is structured as follows. First, we introduce the novel challenges for the trust-building process posed by the use of rules-of-code in relation to transactions. We then discuss the rules-of-code as an institutional technology and provide a literature review of the institution-based trust literature. Following that, we introduce the theory of rule-governed behavior and discuss how it helps to define a code-based trust model. Next, we introduce and describe each structural component of the code-based trust model, providing illustrations of recent applications. Lastly, we discuss the theoretical contributions of our study and suggest directions for future research.

2. THEORETICAL BACKGROUND OF TRUST BUILDING IN CODE-DRIVEN TRANSACTIONS

2.1. Rules-of-code as Institutional Technology for Trust-building

Forms of conjoined agency between humans and technology are increasingly spreading across a variety of organizations (Agrawal, Gans, & Goldfarb, 2018; Kumar, & Kukreja, 2022). The range of technologies not only offers increased efficiency and expands the organizational repertoire of collaboration-oriented tools (e.g., virtual collaboration tools, workspace software, robots), but also varies in the locus of agency to intentionally constrain, supplement, and replace human action in protocol development and action selection (Glynn & Kashin, 2018; Bradley, 2021; Murray, Rhymer, & Sirmon, 2021; Dixit, 2022; Shah, Nasir, & Shah, 2024). The latter are enabled by a finite sequence of rules-of-code – that is, written logical instances of computing law that are arranged in a step-by-step fashion for the accomplishment of a task (Lessig, 2003; 2006).

Blockchain has recently emerged as a primary example of a setting in which the rules-of-code can automatically self-select actions when predefined contingent conditions arise (Murray, Rhymer, & Sirmon, 2021; Große et al., 2024). Blockchain comprises a decentralized and distributed ledger of digital records of transactions that are organized in a growing list of blocks, forming a permanent chain that is maintained by a peer-to-peer network of computing systems (Tapscott & Tapscott, 2016; Große et al., 2024). The peer-to-peer network lies at the heart of the blockchain. In this communication model, each computing system maintains the same copy of the ledger to continuously verify that data is accurate and available. Since no centralized authority exists, the rules-of-code determine the guiding principles of the network operations to ensure a high degree of resistance to malicious activity (Tapscott & Tapscott, 2016; Zhao, Fan, & Yan, 2016; Ølnes, Ubacht, & Janssen, 2017; Hsieh et al., 2018). A smart contract is a computing program containing immutable cause-effect statements that are automatically run to execute actions specific to an agreement when predetermined conditions of a transaction are met (Murray et al., 2019, Große et al., 2024). Smart contracts in the supply chain are one of the most common uses of blockchain (Manski, 2017; Queiroz & Wamba, 2019; Saberi et al., 2019; Lohmer, Bugert, & Lasch, 2020). For example, on the Hyper ledger blockchain platform developed by IBM, a smart contract could automatically state the responsibilities of each party in the purchase and delivery of goods, the penalty clauses, and the payment terms without the need to establish a layer of bureaucracy and seek out an intermediary to protect the parties against potential fraud. Funds could be automatically transferred to the supplier when the goods are delivered upon specific parameters, thereby enforcing transactions within a digital agentic layer of traceable action selection (Hsieh et al., 2018; Queiroz & Wamba, 2019; Saberi et al., 2019; Lohmer, Bugert, & Lasch, 2020; Murray, Rhymer, & Sirmon, 2021).

Artificial intelligence is a primary example of a setting in which the rules-of-code can provide predictive recommendations to guide the action selection (Ferràs-Hernández, 2018; Glikson & Wooley, 2020; Kellogg, Valentine, & Christin, 2020; Murray, Rhymer, & Sirmon, 2021). Artificial intelligence is a computing algorithm based on ordered rules-of-code that simulates human intelligence processes (Glikson & Wooley, 2020; Murray, Rhymer, & Sirmon, 2021; Dixit, 2022; Shah, Nasir, & Shah, 2024). Compared to human intelligence, artificial intelligence can interact with the environment to interpret and recognize data patterns (Simon & Frantz, 2003; Ferràs-Hernandez, 2018). Using sample input data (e.g., information from customer relationship management [CRM] software, enterprise databases, and the web), it can produce output that supports finding fraudsters, handling claims, and decision making. Most of the financial giants in the banking industry (e.g., Citi, Goldman Sachs, American Express) are now applying artificial intelligence to secure digital financial transactions under different conditions. The rules-of-code at the root of artificial intelligence can recognize suspicious activities vis-à-vis clients' behavior and prevent fraudulent transactions by triggering security mechanisms when something seems out if order. A similar application can be found in the public sector, where artificial intelligence is used for tax fraud detection. Likewise, online shopping retailers (e.g., Amazon) are using artificial intelligence to identify and remove fake reviews and to combat counterfeit products. Machine learning is a well-known sub field of artificial intelligence that focuses on solving complex business issues. The programs used in this area are based on both structured and unstructured supervised techniques of data processing. Structured machine learning describes a class of supervised algorithms that can recognize co-relational patterns from training data for providing guidelines regarding what the system should do without exposing it to harm (Glynn, & Kashin, 2018; Bradley, 2021). In contrast, unstructured machine learning describes a class of computing programs that can process multiple types of unlabeled data and learn from it how to formulate guidelines to achieve a task.

Popular applications of this new generation of technologies suggest that rules-of-code have value in the coordination of transactions (Lumineau, Wang & Schilke, 2021; Murray, Rhymer, & Sirmon, 2021; Große et al., 2024). Rules-of-code have emerged as a new category of economic governance mechanisms alongside the spectrum of institutions (Williamson, 1985). By supporting a sense of good faith and fair dealing behavior, rules-of-code may instill a certain level of perceived situational normality and structural assurance into a transaction. Situational normality stems from the appearance that things are customary and in proper order, which makes the agents feel sufficiently comfortable to engage in a transaction (Garfinkel, 1963; Lewis & Weigert, 1985; Baier, 2014). Structural assurance, in contrast, refers to the security one feels because of the presence of protective structures and safeguards (Zucker, 1986; Shapiro, 1987; Williamson, 1993).

Compared to other traditional governance mechanisms (e.g., formal and relational contracting), rules-of-code seem to suffer less from some systemic inefficiencies (Tapscott & Tapscott, 2016; Davidson, De Filippi, & Potts, 2018; De Filippi, Mannan, & Reijers, 2020; Lumineau, Wang & Schilke, 2021). The last global financial crisis brought to light some weaknesses in the traditional governance mechanisms (e.g., central authorities, intermediaries, formal and relational contracting) that allowed for systemic failure in the face of manipulation of the true state of reality (Bachmann & Inkpen, 2011). Ideally, rules-of-code should offer improved coordination at lower transaction costs because opportunism is controlled by obviating the risks of adding costs through fees and delays, creating friction, and generating opportunities for fraud (Tapscott & Tapscott, 2016; Davidson, De Filippi, & Potts, 2018; De Filippi, Mannan, & Reijers, 2020; Große et al., 2024). The computational logic of the rules-of-code has the merit of providing a unified view of the true state of reality – one that is credible in the eyes of all parties. The latter, in fact, is relevant for the problem of misplaced trust.

2.2. From Interaction-based Trust to the Emergence of Code-based Systems of Trust

Prior research has defined trust as a state of mind that an agent (a person, a group or organization's members) develops in situations of interdependence with others (Rousseau et al., 1998; Schoorman, Mayer, & Davis, 2007). It comprises the trustor's intention to accept that one can be vulnerable to the actions of another party based on some initial optimistic expectations that this latter will take a proper behavior (Mayer, Davis, & Schoorman, 1995; Rousseau et al., 1998). Among the literature in management and general business, the work of Mayer, Davis, and Schoorman (1995) is a reference point for a complete understanding of trust and its building process when face-to-face transactions occur. According to Mayer, Davis, and Schoorman (1995), trust originates from trusting beliefs about the trustee, as an individual person, a group or a member of an organization. Trusting beliefs encompass perceptions about the trustee's trustworthiness (ability, integrity, and benevolence). Compared to face-to-face transactions, code-based transactions should require less attention to the correct judgment of the trustee's trustworthiness. There is a shift of the primary object of trust from people to the rules-of-code as an impersonal object that performs important actions to the trustor (Antonopoulos, 2014; Davidson, De Filippi, & Potts, 2018; Rikken, Janssen, & Kwee, 2019; Lumineau, Wang, & Schilke, 2021; Große et al., 2024).

Although scholars have expressed a great deal of interest in the notion of trust in rules-of-code, the actual discussion is mainly focused in its outcomes and benefits (Hawlitschek, Notheisen, & Teubner, 2018; De Filippi, Mannan, & Reijers, 2020; Glikson & Woolley, 2020; Murray, Rhymer, & Sirmon, 2021; Lukyanenko et al., 2022; Tan & Saraniemi, 2023; Wong et al., 2024) leaving as idea complete understanding of what trust in rules-of-code is and how it is generated. One possible approach to fill this gap is to link the concept of trust in the rules-of-code to institutional trust. In the mainstream research of trust, institutional trust is positioned at the macro level of analysis to represent a value judgment about the institution's capability to credibly enforce a common behavioral pattern for the mutual benefit of the involved parties (Luhmann, 1979; Zucker, 1986; Giddens, 1990; Child & Möllering, 2003; Bachmann & Inkpen, 2011). Institutions are governance mechanisms that encompass a wide range of formal (e.g., property rights, laws, constitutions) and informal (e.g., conventions, codes of conduct) (North, 1990; Nooteboom, 2007; Bachmann & Inkpen, 2011; Cao & Lumineau, 2015). They are especially important when the trustor is not prepared to trust the trustee because of unfavorable assumptions about the trustee's future behavior (McKnight, Cummings, & Chervany, 1998; Child & Möllering, 2003; Nooteboom, 2007; Bachmann & Inkpen, 2011). Once the level of institutional trust exceeds the perception of being at risk, the trustor is prepared to securely deal with others (Zucker, 1986; McKnight, Cummings, & Chervany, 1998; Child & Möllering, 2003; Bachmann & Inkpen, 2011; Mishra & Mishra, 2013). This creates a condition to take an institution-based trust behavior, meaning that there is a reasoned willingness to securely engage in any kind of transaction (Zucker, 1986; Nooteboom, 2007; Bachman & Inkpen, 2011).

Although research in institutional trust as mostly followed a calculative perspective under the influence of transaction cost economics theory (Williamson, 1993; Nooteboom, 2007; Bachmann & Inkpen, 2011; Cao & Lumineau, 2015), the concept of institutional credibility emerges as important cue to evaluate the role of institutions (Zucker, 1986). In the next section, we go through a systematic survey of the literature to further delineate the conceptual boundaries of institutional credibility and to better gauge its relationship with trust in the rules-of-code.

3. METHODOLOGY

Building on Oliveira and Lumineau (2018), we apply a three-steps procedure to explore these earlier studies in social science to mark the boundaries of institutional credibility. First, we mark the conceptual boundaries of institutional credibility. Next, we specify the scope for the literature review and code the main manifestations of the characteristics of institutional credibility in group categories. Evidence from this cross-disciplinary review reveals that those group categories can be conceptually linked to the theory of rule-governed behavior.

3.1. Marking the Conceptual Boundaries of Institutional Credibility

We first search for conceptual and empirical articles that use the term “institutional credibility” in the domain of trust (108 articles in total). As shown in Table 1, we capture numerous related keywords (such as functionality, accountability, shared rules, transparency, clarity, fairness, and justice). Combining the keyword “institutional credibility” together with the other related keywords, we end up with over 2600 results in Scopus. Compared to other databases, like PubMed and Web of Science, we use Scopus because it covers a wider range of journals in the fields of social science (Falagas, Pitsouni, Malietzis, & Pappas, 2008). This allows us to have a more inclusive and multidisciplinary overview.

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 “unintended intentionality” OR “appropriateness” OR “coherence” AND “institutional credibility”	318
3	To identify words that appear in the definition of institutional credibility 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.

3.2. Specifying the Review Scope

We restrict our search to a list of top-tier journals that have published empirical, conceptual, or review articles in general management, business ethics, political science, sociology, and economics. Following this approach, we identify 291 initial articles. Starting from this pool of articles, we use a snowball approach to track contributions not included in Scopus (Greenhalgh & Peacock, 2005). In the end, we obtain a total of 326 articles potentially manifesting the characteristics of institutional credibility. Among those, we apply more restrictive criteria that may prevent the inclusion of contributions discussing institutional credibility only marginally. Those criteria regard: i)the degree of focus on institutional credibility as main subject of the article, and ii) the frame of reference to economic transactions. The final pool includes 116 relevant studies.

3.3. Manifesting the Characteristics of Institutional Credibility

Table 2 summarizes how institutional credibility manifests itself. In particular, the main manifestations of institutional credibility are often conveyed by similar meanings, which can be organized into three group categories: functionality, fairness, and immediacy.

Characteristics of institution’s credibility	Characteristics of technology’s credibility
Performance of delivering on promises and consistency Effectiveness Constancy, accuracy, and speed of feedback	Functionality
Neutrality, equity, and impartiality Formality, clarity, and correctness Transparency and accountability Procedural fairness and distributive justice	Fairness
Acting in the interests and respect Providing support Flexibility	Immediacy

TABLE 2: Characteristics of Institution’s Credibility.

To provide a conceptual step forward, we identify the cognitive theory of rule-governed behavior (Zettle & Hayes, 1982; Skinner, 1984) as potentially helpful for the definition of credibility and its dimensions in the domain of rule-governed systems.

3.4. The Theory of Rule-governed Behavior

A very large body of research in psychology shows that agentic behaviors rely on various kinds of rule systems, which help agents assess problems and make sense of reality by adding order, predictability, and reliability (Kramer, 2006). To take an example outside the sphere of business, children’s education represents 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. For example, from hearing the rule “Tell the truth, and you’ll be fine,” the child learns that telling the truth is the right thing to do and has positive consequences (Törneke, Luciano, & Salas, 2008). A rule is said to work if it is possible to monitor compliance and deliver consequences (Zettle & Hayes, 1982).

The decision to adopt a rule-governed behavior in the face of a discriminative stimulus of instructional control is influenced by some key reasons. One reason involves the set of beliefs about the credibility of the specific rule (Skinner, 1984). Credibility is a topic that has been addressed in the field of psychology to explain the willingness to rely in relation to multiple characteristics of a specific object under judgment (McCroskey & Young, 1981; Tseng & Fogg, 1999). For a rule to be credible, there must be a perceived correspondence between what it says and what it does for things to go well. To the extent the rule credibly provides a set of behaviors that facilitate social coordination that perceived correspondence envisions a trusting belief as antecedent of the intention to trust a rule-based system (Zettle & Hayes, 1982; Hayes, Zettle, & Rosenfard, 1989).

Functionality - Scholars focusing on rule-governed behavior consider functionality to be an essential element of rule credibility (Zettle & Hayes, 1982; Hayes & Rosenfard, 1989). Functionality is the expression of a generalized, comforting belief that a rule-governed system is useful, practical, and right for the purpose for which it is made. It originates from perceptions that things are bounded under structural assurance against the uncertainty of future events (McKnight, Cummings, & Chervany, 1998). Within the framework of an institutionalized rule-based system, functionality includes considerations of effectiveness, reliability, and consistency. Effectiveness refers to the process of developing the right protocol and selecting the right action to make things go well (Lane & Bachmann, 1996, 1997; Child & Möllering, 2003; Smith, 2011; Ho, 2016). Reliability refers to the ability of the rule-based system to perform under the stated conditions without manifesting points of failure that could cause a crisis (Giddens, 1990; North, 1990; La Porte, 1994; La Porte & Metlay, 1996; Ho, 2006; Sekhon et al., 2014). Strictly connected to reliability, consistency means using the same structure and format to always perform in a similar way (Giddens, 1990; North, 1990; Tyler & Lind, 1992; La Porte, 1994; La Porte & Metlay, 1996; Lane & Bachmann, 1996, 1997; Tyler & Degoey, 1996; Levi, 1998).

Fairness – Agents look for rules that are perceptually fair in applying an impartial and just treatment under the conditions found in typical situations (Hayes, Zettle, & Rosenfard, 1989). Thus, fairness refers to the perception of being in control and informed because the rule-governed system establishes a procedure to deal with the expected situational conditions (Levi, 1998; McKnight, Cummings, & Chervany, 1998; Tyler & Degoey, 1996; Husted & Folger, 2005). Those perceptions rise from considerations of transparency, neutrality, and accountability. Transparency gives insights into how a rule-based system shows a core value of openness in protocol development and action selection (Pavlou & Gifen, 2004; Smith, 2011), as well as formality and clarity (Zaheer, McEvily, & Perrone, 1998). Neutrality, meanwhile, is conceived as impartiality. This means acting equally toward the various interests and applying formal procedures that do not favor any party (Luhmann1979; Zucker 1986; Tyler & Lind, 1992; Tyler & Degoey 1996; Child & Möllering, 2003). Lastly, accountability entails the obligation to be answerable for the consequences after a situation has occurred (Biermann, 2007; Smith, 2011).

Immediacy - Skinner (1984) argues that rules should provide adaptive frames of proper behavior. Immediacy refers to the capability of offering a socially oriented closeness and support under all circumstances. For example, if some disturbance disrupts the usual practices of social coordination, rules may help to restore a mutually acceptable behavioral framework that supports ongoing social interactions (Braithwaite, 2002; Ho, 2006; Biermann, 2007; Arvanitidis, 2020). For an institutionalized rule-based system, immediacy includes moral concern and flexibility. On the one hand, moral concern refers to the process of serving the social interests of the parties engaging in a transaction (Tyler & Lind, 1992; Tyler & Degoey, 1996; Biermann, 2007; Smith, 2011; Sekhon et al., 2014; Arvanitidis, 2020). This is often related to good corporate governance in protocol development and action selection. On the other hand, flexibility is associated with the ability of structure to act and react rapidly in response to environmental changes (Lane & Bachmann, 1996, 1997).

4. A MODEL OF CODE-BASED TRUST

In light of the findings above, we build a conceptual model of code-based trust (Figure 1) that distinguishes between trusting beliefs, attitudes, intentions, behaviors, and other boundary factors. In the following sections, each component and its cause-effect relation arediscussed.

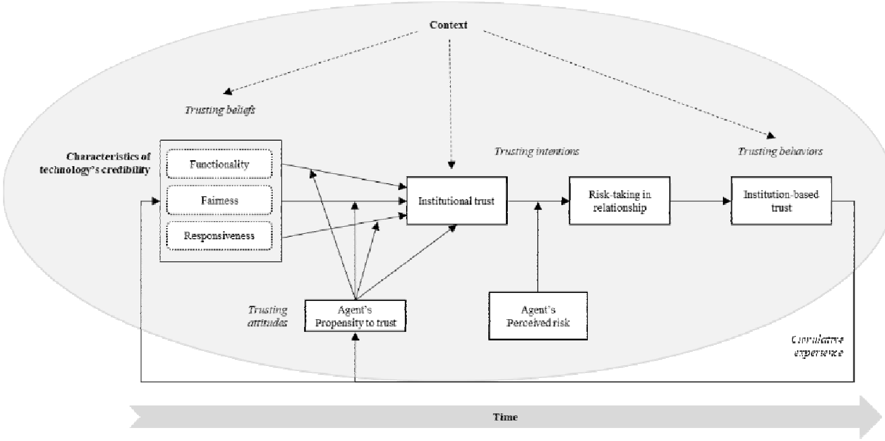

FIGURE 1: Model of Code-based Trust.

4.1. Trust in the Rules-of-code and Code-based Trust

Trust in rules-of-code lies at the heart of our model. It represents the willingness to depend on the rules-of-code, which impart a feeling of relative security. That feeling implies that the party is prepared to be vulnerable to the actions identified under the rules-of-code, given the initial optimistic expectation about the rules-of-code's role in both developing protocols and selecting the proper actions to limit opportunistic behavior (De Filippi, Mannan, & Reijers, 2020). Although this definition of trust in the rules-of-code shares some conceptual commonalities with institutional trust, it differs in the explication of the risk component from which the vulnerability originates.

Making oneself vulnerable to the rules-of-code means that the trustor might put themselves at risk of experiencing data privacy issues, security threats, volatility, and decreased corporate governance accountability (Manski, 2017; Murray et al., 2019; De Filippi, Mannan, & Reijers, 2020; Murray, Rhymer, & Sirmon, 2021). As an example, consider the case of a decentralized autonomous organization (DAO) that attempts to automate some managerial aspects of processing transactions without a centralized leadership. After raising $150 million USD through a token sale to fund the automation, the DAO is hacked owing to vulnerabilities in its code base. The bug reveals that users are exposed to the risk of fraudulent actions because the blockchain rule-governed system might be hacked or does not account for some contingent factors (Rikken, Janssen, & Kwee, 2019; De Filippi, Mannan, & Reijers, 2020). In the realm of artificial intelligence, volatility is a major risk that may bring to light incomplete or suboptimal protocols of practice. Teodorescu et al. (2021) point out that the structural limitations of artificial intelligence really depend on the training data. Such training data may not account for some complex socioeconomic scenarios or unexpected changes that prevent proper adaptation to general events (Murray, Rhymer, & Sirmon, 2021).

Within our model, trust in the rules-of-code is a necessary condition for code-based trust. Code-based trust is a trusting behavior reflecting the risk-taking decision in a specific situation at stake. It reflects the expectation that the rules-of-code will provide protective structures that support the most appropriate protocol development and action selection to maintain a properly ordered setting across risky situations. Thus, whether the level of trust in the rules-of-code exceeds the perceived risk involved in being vulnerable to the rules-of-code themselves, the trustor is prepared to engage in a code-based trust which is the behavioral manifestation of a risk-taking decision.

Proposition 1. The decision to follow a code-based trust behavior is directly related to the level of trust in the rules-of-code, given the trustor's threshold of perceived risk.

Having defined the rules-of-code as a class of institution à la Williamson (1985), this parallelism opens discussion of the substitute and complementary nature of code-based trust vis-à-vis relation-based trust. Most organizational scholars support the logic of a substitution effect between formal and informal forms of trust (Rousseau et al., 1998; Nooteboom, 2007; Cao & Lumineau, 2015). They claim that the specific nature of formal devices is conducive to achieving situational success more efficiently because they replace the need for "handshakes" with a priori bounded "protocol" behavior. Indeed, relational contracting tends to require a long history of repeated exchanges between parties (Carson, Madhok, & Wu, 2006; Nooteboom, 2007; Gulati & Sytch, 2008). By contrast, a trust-code-based decision may appear a more efficient strategy in the early stage of the relationship, where a lack of full and clear information creates concerns (De Filippi, Mannan, & Reijers, 2020; Lumineau, Wang & Schilke, 2021; Murray, Rhymer, & Sirmon, 2021). In such situations, there is a substitute effect towards code-based trust to the extent it can improve the verification and traceability of multistep transactions. By comparison, code- and relation-based trust would be complementary in situations involving high asset specificity at stake. High asset specificity requires face-to-face contacts to control for the effect of unpredicted changes in an environment over time (Carson, Madhok, & Wu, 2006). Since it is difficult to anticipate all possible future contingencies ex ante, a combination of formal devices and relation contracting often becomes necessary to deliver greater exchange performance. While code-based trust may enter the early stages of a digital transaction, it subsequently allows for building relation-based trust to complement the adaptive limits of rules-of-code over time.

Proposition 2. Code- and relation-based trust are substitutes with respect to the history of interactions; they are complements depending on asset specificity.

4.2. Characteristics of Technology's Credibility

In a technological framework, trusting beliefs refers to the way users perceive and evaluate the potential outcomes of the rules-of-code. Functionality focuses on the degree of practicability or capability of using the rules-of-code to cover specified tasks and user's needs in terms of both ease of use and utility. This includes the effectiveness with which the rules-of-code deliver correct results with precision. This ability is particularly emphasized when dealing with unknown traders in most elementary types of transactions (e.g., payment-processing systems, and transfer of materials within the supply chain). Interviews with blockchain users indicate that functionality is an important intrinsic attribute that captures the ability to provide proper and convenient safeguards against the risks related to dishonest behaviors (Queiroz & Wamba, 2019; Saberi et al., 2019; Lohmer, Bugert, & Lasch, 2020). Findings show that the rules-of-code may be perceived as highly effective in mitigating such risks, as most parts of the transaction are scrutinized by many participants within the peer-to-peer blockchain network (Manski, 2017; Wang et al., 2017; Davidson, De Filippi, & Potts, 2018; Murray et al., 2019). Having a peer-to-peer network allows for the validation of transactions as resistant and resilient to any type of failure and malicious errors more quickly and securely (Davidson, De Filippi, & Potts, 2018; De Filippi, Mannan, & Reijers, 2020; Wang et al., 2017). This aspect is also emphasized when exploring powered applications of artificial intelligence to create self-analytic models to uncover online fraud patterns in real-time, particularly in over-exposed industries like commercial banking and fintech (Kellogg, Valentine, & Christin, 2020). Early studies on artificial intelligence have illustrated that user's perception of functionality originate from the assessment of artificial intelligence ability to provide a competent and efficient protocol of actions (Hancock et al., 2011; Dressel & Farid, 2018; Glikson & Woolley, 2020; Kellogg, Valentine, & Christin, 2020; Murray, Rhymer, & Sirmon, 2021; Wong et al., 2024).

Fairness reflects the rules-of-code's adherence to standards, conventions, or regulations of proper practice in protocol development and action selection. Empirical studies confirm that users perceive the rules-of-code as a tool to penalize dishonest parties for their misbehavior, insofar as the rules-of-code operate without discrimination in the automatic execution of tasks when some conditions are satisfied (De Filippi, Mannan, & Reijers, 2020). For example, applications of blockchain-based smart contracts to the supply chain benefit from a system that tracks the authenticity and origin of materials and that incorporates the mathematical rigor of the rules-of-code to evaluate the legitimacy of claims about products (Queiroz & Wamba, 2019; Saberi et al., 2019; Lohmer, Bugert, & Lasch, 2020). While information is locked and transparency ensured, a consistent pattern of conduct is maintained that is based on impartial treatment and reflects the belief that the rules-of-code operate correctly in the customary situation of proper order (Maurer, Nelms, & Swartz, 2013). In the case of artificial intelligence, fairness is related de-biasing. Artificial intelligence practitioners tend to focus more on the placement of some procedural restrictions in relation to a justice approach. When it comes to artificial intelligence systems, a justice approach considers how they can advance equity rather than perpetuate a status quo of an elite group (Hancock et al., 2011; Dressel & Farid, 2018; Glikson & Woolley, 2020). An artificial intelligence-based model used by a bank to predict whether or not an individual will receive a loan based on the risk of default is perceived fair when the mathematical rigor of the rules-of-code – by design – allows to achieve an unbiased strictness on action selection. The pattern of conduct is expected to take care of non-discrimination of individual's protected attributes (Mittelstadt, 2019; Glikson & Woolley, 2020; Kellogg, Valentine, & Christin, 2020).

Immediacy has implications for the accomplishment of specified tasks and objectives of protocol development and action selection, especially given the dynamic global business environment. A rules-of-code system that is flexible enough to adapt its business rules may allow for better meeting users' needs. For example, with the expanding use of blockchain, more businesses are taking advantage of the flexibility. Given that blockchain is a decentralized application of distributed records, all stakeholders involved in the supply chain may benefit from the continuous growing real-time collection of information to enable adjustments to changes in business conditions more quickly (Queiroz & Wamba, 2019; Saberi et al., 2019; Lohmer, Bugert, & Lasch, 2020). At the same time, blockchain can aggregate different types of data into a synthesis (Schmidt & Wagner, 2019). That information integration helps sustain a belief that blockchain adoption can improve the supply chain resilience and responsiveness in view of high levels of environmental uncertainty (Manski, 2017; Saberi et al., 2019). Particularly, Manski and Bauwens (2020) have discussed how blockchain is paving the way to shared supply chains with collaborative and networked data flows as well as the integration of social and ecological externalities. Other studies confirm that users generally perceive artificial intelligence as being high in immediacy (Glikson & Woolley, 2020; Kellogg, Valentine, & Christin, 2020; Kaplan et al., 2023; Wong et al., 2024). This perception reflects artificial intelligence's envisioned ability to switch quickly between stimulus sets and see beyond conventional action protocols, thereby amplifying the spectrum of possible actions in relation to the given learning task in a variety of scenarios involving parties with a range of backgrounds and professional interests. As algorithms become more robust, pioneering work is addressing the versatile potential of artificial intelligence as expressed through the neural network learning rate. Examples include use-cases ranging from forecasting to credit card fraud detection and risk assessment (Mittelstadt, 2019; Kellogg, Valentine, & Christin, 2020).

Proposition 3. Trust in the rules-of-code is a function of the perceived credibility characteristic (functionality, fairness, and immediacy) of the rules-of-code.

Perceptions about technology's credibility characteristics are related to each other; each characteristic, however, varies independently. Characteristics of credibility can independently assume higher or lower levels, depending on how each characteristic is judged to meet positive expectations of beneficial actions (Mayer, Davis, & Schoorman, 1995; Rousseau et al., 1998). Less favorable perceptions of one or more credibility characteristics do not imply distrust, but rather lower levels of trust in the rules-of-code. In fact, distrust is a construct relating to negative expectations regarding another's actions (Lewicki, McAllister, & Bies, 1998).Empirical studies of blockchain have illustrated that perceptions of functionality and fairness are often high enough to build a minimum level of trust in the rules-of-code (Davidson, De Filippi, & Potts, 2018; Hawlitschek, Notheisen, & Teubner, 2018; De Filippi, Mannan, & Reijers, 2020; Lumineau, Wang & Schilke, 2021; Bostrom et al., 2024). The same cannot be said for immediacy. Blockchain-based smart contracts cannot always meet users' expectations to act and react properly in some situations. These situations include those involving not previously coded contingent factors (De Filippi & Wright, 2018; Murray et al., 2019; Murray, Rhymer, & Sirmon, 2021). For example, one cannot assume that smart contracts will ensure full compliance with all possible legal facets of the situation. Once a smart contract is executed, there is no way to undo or adjust it. If a change becomes necessary, the history of transactions remains unalterable. The only choice in such a case is likely to abort the smart contract and create new one with an extra fee to compensate from that computational cost (Murray et al., 2019). Another major problem with blockchain is the lack of maturity. This may leave room for software flaws to arise, which may have a tremendous impact on the perceived functionality of this technology (Manski, 2017; Murray et al., 2019; Murray, Rhymer, & Sirmon, 2021).

Early studies on artificial intelligence, by contrast, have illustrated that functionality and immediacy are primary antecedents of trust in the rules-of-code with this technology (Hancock et al., 2011; Dressel & Farid, 2018; Glikson & Woolley, 2020; Kellogg, Valentine, & Christin, 2020; Murray, Rhymer, & Sirmon, 2021; Wong et al., 2024). However, recent scandals involving artificial intelligence have revealed some controversies. When artificial intelligence is applied uncritically, the ensuing protocols and actions may result in unfair outcomes. One key challenge is the implications for data privacy (Glikson & Woolley, 2020; Kellogg, Valentine, & Christin, 2020; Murray, Rhymer, & Sirmon, 2021; Teodorescu et al., 2021; Wong et al., 2024). There is the potential that data might be used for unintended (bad) purposes. For example, Facebook's recent violations of U.S. fair housing laws have raised moral concerns about using artificial intelligence to target advertising – namely, its potential for discrimination (Benner, Thrush, & Isaac, 2019). Additionally, the quality of training data is not always suitable to cope with the bias problem. Once the artificial intelligence delivers suboptimal protocols of practice, perceptions of functionality are compromised (Mittelstadt, 2019; Teodorescu et al., 2021).

In sum, if functionality, fairness and immediacy are all perceived to be high, the rules-of-code would be believed highly reliable. That belief should be thought varying in a continuum, meaning that there might be situations in which one or more characteristics.

Proposition 4. Low levels of perceptions of one or more credibility characteristics negatively affect the total level of trust in the rules-of-code.

4.3. Agent's Propensity to Trust Technology

Consideration of credibility of technology characteristics can be different for trustors with a low-versus-high propensity to trust the rules-of-code (Lankton, McKnight, & Thatcher, 2014; Glikson & Woolley, 2020; Lukyanenko et al., 2022; Kaplan et al., 2023; Wong et al., 2024). Propensity to trust is a personal attitude that leads to a generalized willingness to trust in situations that others might argue do not warrant trust (Rotter, 1971). It captures the effect of personality characteristics and experiential factors (Sitkin & Pablo, 1992) in coloring perceptions of credibility and their direct influence on the amount of trust (Mayer, Davis, & Schoorman, 1995; Braithwaite, 2002). In the depiction of our model in Figure 1, the three arrows indicate that an agent's propensity to trust technology is expected to moderate the effects of perceived characteristics of technology credibility (trusting beliefs) on the willingness to trust the rules-of-code (trusting intentions). That moderating effect is given by two kinds of attitudes, which operate in a conjoint fashion: personal innovativeness and experience with technology.

On the one hand, personal innovativeness is the tendency one shows toward trying out new technologies (Rogers, 1995; Agarwal & Praasad, 1998; Agarwal & Karahanna, 2000). Users who are generally more inclined to embrace technology are more likely to positively augment their level of perceptions in such a way that technology's credibility characteristics are overestimated. This is expected to have a positive effect on the intention to trust the rules-of-code, even when a specific technology might appear less credible. Conversely, users who are generally less inclined to trust technology are more likely to decrease their level of perceptions, to the extent that technology's credibility characteristics are viewed with suspicion (Lankton, McKnight, & Thatcher, 2014). For example, several empirical studies of the blockchain ecosystem have shown that blockchain transactions are more welcomed by users with very advanced technological expertise (Manski, 2017). Advanced technological skills may help facilitate users' adoption of new technology (Manski, 2017; Lukyanenko et al., 2022). Similar findings have been found in the field of artificial intelligence. For instance, Wood, Lehdonvirta, and Graham (2018) reported that an elite group of "technological adepts" is emerging, with their divergence from the general population expected to create a technological divide.

On the other hand, experience with technology is linked to previous practical contacts, knowledge, feelings of usefulness, and ease of use (Davis, 1989; Igbaria, Iivari, & Maragahh, 1995). Earlier experience helps form an opinion and establish more realistic expectations about the credibility of technology (Agarwal & Karahanna, 2000; Dutton & Shepherd, 2006). Thus, users who have generally had a positive experience with technology are more likely to positively augment their level of perceptions of technology's credibility characteristics, even when their initial experience with a specific technology is limited. Scholars of blockchain have shown that a high level of satisfaction with some key aspects of this technology (e.g., increased user control of information, transparency and immutability, and maintenance of accurate data) is expected to a have a positive effect on users' perception of fairness (Manski, 2017). Conversely, users who have a bad experience with technology in relation to key unresolved technical challenges (e.g., cybersecurity and privacy concerns, limited user friendliness, and unsettled regulation) are more likely to demonstrate less favorable perceptions of blockchain functionality (Manski, 2017; De Filippi, Mannan, & Reijers, 2022). Evidence from studies of artificial intelligence confirm that users make trust-related assumptions about the technology's credibility based on whatever they have already experienced (Nomura, Kanda, & Suzuki, 2006; Kaplan et al., 2023). In some cases, a very bad experience with a single characteristic could lead users to lower their perceptions of technology's credibility in terms of one or more characteristics (Lankton, McKnight, & Thatcher, 2014).

Proposition 5. Trustor's personal innovativeness and experience with technology jointly moderates perceptions that rules-of-code are credible.

4.4. Context and Time

Earlier scholars highlighted the importance of context in influencing both the beliefs and the intention to trust (Sitkin & Pablo, 1992; Schoorman, Mayer, & Davis, 2007). The context of a transaction involves multiple factors, such as the stakes involved, the specific domain, the perception of similarity to known situations, social factors, and the alternatives available. These factors define the area of perceived risk; therefore, they characterize the assessment of the likelihood of a positive versus negative outcome (Coleman, 1994).

The context of digital transactions is characterized by some major socio-technical factors. First, the new generation of technologies is dramatically changing the human connection to technology. In the last few years, technology has become integrated into most facets of social life, albeit with a high level of specialization. While artificial intelligence, perhaps, is broadly established in most business models (Kellogg, Valentine, & Christin, 2020; Kaplan et al., 2023), the transformative potential of blockchain is generating interest and is expected to have a deep impact on those sectors characterized by more accelerated systems interconnectivity, such as finance and currency exchange, healthcare, government services, security, and supply chain management (Manski, 2017; Tapscott, & Tapscott, 2016; Hawlitschek, Notheisen, & Teubner, 2018). As technology has become pervasive in organizational practice, increased automation is expected to always be available. It is perceived functionality will change depending on the specific situation. For example, if a blockchain user needs to handle a high volume of transactions quickly, scalability is a major challenge. Currently, blockchain is limited to conducting 4.6 transactions per second; by comparison, VISA is capable of handling 1,700 transactions per second. Under these conditions, the only feasible use of blockchain is data tracking. Further, the level of asset specificity at stake is an important contextual factor. In some high-stakes situations, the rules-of-code may be perceived as being too disconnected from the user's influence. For example, an artificial intelligence system may decide on a course of action without any involvement of human judgment in case of unforeseeable future events (Glikson & Woolley, 2020; Murray, Rhymer, & Sirmon, 2021; Kaplan et al., 2023). Since the exact separation of the locus of agency between an individual, a group, or an organization and the rules-of-code remains to be determined, these facts have major implications for the technology's perceived immediacy.

Another critical aspect is the process by which trust evolves over time. Several theorists have suggested that the development of trust involves an active process of continuous reevaluation (Luhmann, 1979; Mayer, Davis, & Schoorman, 1995; Schoorman, Mayer, & Davis, 2007; Gulati & Sytch, 2008; Lankton, McKnight, & Thatcher, 2014; Haring et al., 2021). In our model, this active feature is represented by the feedback loop. It indicates that a long-lasting history of interaction supports the positive (or negative) adjustment of trusting beliefs over time. At the very beginning, trust in the rules-of-code might be fragile and consist of experimental attempts (De Filippi, Mannan, & Reijers, 2020; Glikson & Woolley, 2020; Lumineau, Wang & Schilke, 2021; Murray, Rhymer, & Sirmon, 2021). Trust is fragile at this stage because it is supported by little experience, which makes the perceived risk high. The lack of experience leads to relatively less meaningful perceptions. If the decision to trust the rules-of-code yields a favorable outcome, perceptions of technology credibility are, in turn, enhanced in magnitude and sufficient to sustain future intention to trust the rules-of-code. Conversely, these perceptions may decline when the decision to trust leads to an unfavorable outcome. Perceptions of functionality and fairness may emerge early, informed by insights from user reviews, surveys, proof of concepts, or certifications (Murray et al., 2019; Glikson & Woolley, 2020; Roeck, Sternberg, and Hofmann, 2020; Lumineau, Wang & Schilke, 2021; Murray, Rhymer, & Sirmon, 2021). As familiarity increases, more accurate evaluations are developed, including considerations about immediacy. Perceptions of immediacy take more time to develop. Their effect increases as the promise to establish a technological commonwealth is gradually corroborated by practical and qualitative observations of emergent uses of the rules-of-code in various businesses (Manski, 2017; De Filippi, Mannan, & Reijers, 2020; Glikson & Woolley, 2020; Lumineau, Wang & Schilke, 2021; Murray, Rhymer, & Sirmon, 2021).

Proposition 6. The effect of functionality and fairness on trust in the rules-of-code is more at the beginning prior to the development of meaningful perceptions of immediacy.

Proposition 7. The effect of perceived immediacy on trust in the rules-of-code increases over time as transactions are orchestrated by the rules-of-code.

5. CONCLUSION AND FUTURE DIRECTIONS

In the recent literature of technology, some authors have observed that the notion of trust in rules-of-code (Antonopoulos, 2014) represents a potentially fruitful area for advancing research about technology in society (Hawlitschek, Notheisen, & Teubner, 2018; Rikken, Janssen, & Kwee, 2019; Lumineau, Wang & Schilke, 2021; Lukyanenko et al., 2022; Tan & Saraniemi, 2023; Bostrom et al., 2024; Wong et al., 2024). In this study, we answer that call for high degrees of theoretical rigor regarding the study of trust in the rules-of-code. As Hawlitschek et al. (2018) and Bostrom et al. (2024) highlight, this is important both for theory and for practice, so as to successfully translate the technological hype into viable business applications. Adopting blockchain and artificial intelligence as exemplary institutional technologies (Davidson, De Filippi, & Potts, 2018), we present a definition of trust in the rules-of-code within the framework of the institution-based trust literature (Zucker, 1986; Bachmann & Inkpen, 2011). Although the institution-based trust literature deals with the mechanisms through which institutions influence the trust-building process, we acknowledge that it ignores important cognitive substrata that reside at the core of the trust-building process. Therefore, we integrate this stream of literature with the theory of rule-governed behavior (Zettle & Hayes, 1982; Skinner, 1984). That theory helps shed light on the cause–effect relationship between trusting beliefs and intention to trust in the rules-of-code. From the theory of rule-governed behavior, we derive the characteristics of technology credibility as antecedents of trust in the rules-of-code and discuss the substitution and complementary effects between code- and relation-based trust behavior.

First, our primary contribution is to clarify what trust in the rules-of-code is and how it is generated. Our proposed model describes complete causal relationships between trusting beliefs, attitudes, intentions, and behaviors. This model focuses on the cognitive substrata underlying the micro dynamics of trust within an institutional technology environment. Second, we propose a set of characteristics of technology's credibility (functionality, fairness, and immediacy) that act as antecedents for the volition to trust the rules-of-code. These characteristics have saliency for examining trust mechanisms. We expect our model encourages future research in light of novel technologies and related implications for business practice. Third, we increase understanding of ways to build trust in the rules-of-code from a practical standpoint. We explicitly examine three specific characteristics of technology's credibility that may affect the decision to engage in a code-based transaction. This analysis may help better understand the implications of new technology adoption for successful performance of dis-intermediated buying–selling transactions between unknown traders. From a practical perspective, this is important for marketers who seek to comprehend how to develop trust among their customers and, the other way around, to cope with the rise of new threats to trust in digital transactions (Tilson, Lyytinen, & Sørensen, 2010; Lumineau, Wang & Schilke, 2021).The latter concerns consumers' perceptions of being at risk in view of marketers' data use or fraudulent activities.

This study raises several issues that may suggest promising directions for future research related to trust in the rules-of-code. First, the goal of our work is limited in the scope. Notably, understanding the role of code-based trust in economic prosperity is beyond our scope. We are aware that this avenue is very promising, and more work needs to be done to obtain a sufficiently broad thesis that can 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 trust in the rules-of-code accumulates and depreciates because of societal and culture traits across different countries (Hawlitschek, Notheisen, & Teubner, 2018; Rikken, Janssen, & Kwee, 2019; De Filippi, Mannan, & Reijers, 2020; Lumineau, Wang & Schilke, 2021). Second, our argument for the complementary and supplementary relationships between a code- and relation-based trust model is simply introduced in this paper, but not fully explored. There is need for a more complete argument that would consider the processes and contextual conditions in which trust in the rules-of-code interfaces with relational trust. This line of research might potentially identify the optimal combinations of trust in the rules-of-code and relational trust in the context of digital transactions. Finally, our effort is limited to providing a more complete theoretical foundation for trust in the rules-of-code; we do not deal with the operationalization and full test of the model. Wedo, however, think that operationalization of this model would be beneficial. One strategy would be to identify the relevant measures through a survey-based approach. In addition to having been widely used in the trust literature (Schoorman, Mayer, & Davis, 2007), this research design could provide valuable insights. We invite scholars to take on this challenge using this or other different qualitative and quantitative methodologies.

6. REFERENCES

Agarwal, R., and Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research*, 9(2): 204-215.https://doi.org/10.1287/isre.9.2.204.

Agarwal, R., and Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS quarterly*, 24(4): 665-694.https://doi.org/10.2307/3250951.

Agrawal, A., Gans, J., and Goldfarb, A. (2018). *Prediction machines: the simple economics of artificial intelligence*. Harvard Business Press.

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

Arvanitidis, P., Economou, A., Grigoriou, G., and Kollias, C. (2020). Trust in peers or in the institution? A decomposition analysis of Airbnb listings' pricing. *Current Issues in Tourism*, 25(21): 3500-3517.https://doi.org/10.1080/13683500.2020.1806794.

Bachmann, R., and Inkpen, A. C. (2011). Understanding institutional-based trust building processes in inter-organizational relationships. *Organization Studies*, 32(2): 281-301.https://doi.org/10.1177/0170840610397477.

Bachmann, R., and Zaheer, A. (2006). *Handbook of Trust Research*. Cheltenham: Edward Elgar. https://doi.org/10.4337/9781847202819.

Baier, A. (2014). Trust and antitrust. In Feminist Social Thought (pp. 604-629). Routledge. https://doi.org/10.4324/9780203705841.

Benner, K., Thrush, G., and Isaac, M. (2019). *Facebook Engages in Housing Discrimination with its Ad Practices, U.S. Says*. The New York Times, Politics, March 28.

Bostrom, A., Demuth, J. L., Wirz, C. D., Cains, M. G., Schumacher, A., Madlambayan, D., & Williams, J. K. (2024).Trust and trustworthy artificial intelligence: A research agenda for AI in the environmental sciences. *Risk Analysis*, 44(6): 1498-1513. https://doi.org/10.1111/risa.14245.

Biermann, F. (2007). Earth system governance as a crosscutting theme of global change research. *Global Environmental Change*, 17(3-4): 326-337.https://doi.org/10.1016/j.gloenvcha.2006.11.010.

Bradley, V. M. (2021). Learning Management System (LMS) use with online instruction. *International Journal of Technology in Education*, 4(1): 68-92.

Braithwaite, J. (2002). *Restorative justice & responsive regulation*. Oxford University Press. https://doi.org/10.1093/oso/9780195136395.003.0002.

Cao, Z., and Lumineau, F. (2015). Revisiting the interplay between contractual and relational governance: A qualitative and meta-analytic investigation. *Journal of Operations Management*, 33: 15-42. https://doi.org/10.1016/j.jom.2014.09.009.

Carson, S. J., Madhok, A., and Wu, T. (2006). Uncertainty, opportunism, and governance: The effects of volatility and ambiguity on formal and relational contracting. *Academy of Management Journal*, 49(5): 1058-1077.https://doi.org/10.5465/amj.2006.22798187.

Child, J., and Möllering, G. (2003). Contextual confidence and active trust development in the Chinese business environment. *Organization Science*, 14 (1): 69–80. https://doi.org/10.1287/orsc.14.1.69.12813.

Coleman, J. S. (1994). *Foundations of social theory*. Harvard university press.

Davidson, S., De Filippi, P., and Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, 14(4): 639-658. https://doi.org/10.1017/S1744137417000200.

Davis, F.(1989). Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. *MIS Quarterly*, 13(3): 319-340.https://doi.org/10.2307/249008.

De Filippi, P., Mannan, M., and Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, 62: 101284. https://doi.org/10.1016/j.techsoc.2020.101284.

De Filippi, P., Mannan, M., and Reijers, W. (2022). The alegality of blockchain technology. *Policy and Society*, 41(3): 358-372. https://doi.org/10.1093/polsoc/puac006.

De Filippi P., andWright A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press, Cambridge, MA. https://doi.org/10.2307/j.ctv2867sp.

Dixit, S. (2022). Artificial intelligence and CRM: A case of telecom industry. In *Adoption and Implementation of AI in Customer Relationship Management*: 92-114. IGI Global. https://doi.org/10.4018/978-1-7998-7959-6.ch006.

Dressel, J., and Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1), 5580.https://doi.org/10.1126/sciadv.aao5580.

Dutton, W. H., and Shepherd, A. (2006). Trust in the Internet as an experience technology. *Information, Communication & Society*, 9(4): 433-451.https://doi.org/10.1080/13691180600858606.

Ferràs-Hernández, X. (2018). The future of management in a world of electronic brains. *Journal of Management Inquiry*, 27(2): 260-263.https://doi.org/10.1177/1056492617724973.

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

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

Glikson, E., and Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, 14(2): 627-660.https://doi.org/10.5465/annals.2018.0057.

Glynn, A. N., and Kashin, K. (2018). Front-door versus back-door adjustment with unmeasured confounding: Bias formulas for front-door and hybrid adjustments with application to a job training program. *Journal of the American Statistical Association*, 113(523): 1040-1049.https://doi.org/10.1080/01621459.2017.1398657.

Große, N., Möller, F., Schoormann, T., & Henke, M. (2024). Designing trust-enabling blockchain systems for the inter-organizational exchange of capacity. *Decision Support Systems*, 179, 114182.https://doi.org/10.1016/j.dss.2024.114182.
https://link.springer.com/article/10.1007/s12525-022-00592-6

Gulati, R., and Sytch, M. (2008). Does familiarity breed trust? Revisiting the antecedents of trust. *Managerial and Decision Economics*, 29(2-3): 165-190.https://doi.org/10.1002/mde.1396.

Hancock, P. A., Billings, D. R., Schaefer, K. E., Chen, J. Y., De Visser, E. J., andParasuraman, R. (2011). A meta-analysis of factors affecting trust in human-robot interaction. *Human Factors*, 53(5): 517-527.https://doi.org/10.1177/0018720811417254.

Haring, K. S., Phillips, E., Lazzara, E. H., Ullman, D., Baker, A. L., and Keebler, J. R. (2021). Applying the swift trust model to human-robot teaming. In *Trust in Human-Robot Interaction*: 407-427. Academic Press. https://doi.org/10.1016/B978-0-12-819472-0.00017-4.

Hawlitschek, F., Notheisen, B., and 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. https://doi.org/10.1016/j.elerap.2018.03.005.

Hayes, S. C., Zettle, R. D., and Rosenfarb, I. (1989). Rule-following. In *Rule-governed Behavior*: 191-220. Springer, Boston, MA.

Ho, P. (2006). Credibility of institutions: forestry, social conflict and titling in China. *Land Use Policy*, 23(4): 588-603. https://doi.org/10.1016/j.landusepol.2005.05.004.

Ho, P. (2016). An endogenous theory of property rights: opening the black box of institutions. *The Journal of Peasant Studies*, 43(6): 1121-1144. https://doi.org/10.1080/03066150.2016.1253560.

Hsieh, Y. Y., Vergne, J. P., Anderson, P., Lakhani, K., and Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. *Journal of Organization Design*, 7(1): 1-16. https://doi.org/10.1186/s41469-018-0038-1.

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. https://doi.org/10.1287/orsc.1040.0088.

Igbaria, M., Iivari, J., and Maragahh, H. (1995). Why do individuals use computer technology? A Finnish case study. *Information & Management*, 29(5): 227-238. https://doi.org/10.1016/0378-7206(95)00031-0.

Kaplan, A. D., Kessler, T. T., Brill, J. C., & Hancock, P. A. (2023). Trust in artificial intelligence: Meta-analytic findings. *Human factors*, 65(2): 337-359. https://doi.org/10.1177/00187208211013988.

Kellogg, K. C., Valentine, M. A., and Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals*, 14(1): 366-410.https://doi.org/10.5465/annals.2018.0174.

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

La Porte, T. R. (1994). Large technical systems, institutional surprises, and challenges to political legitimacy. *Technology in Society*, 16(3): 269-288.https://doi.org/10.1016/0160-791X(94)90002-7.

Kumar, R., and Kukreja R. (2022). Human Technology Interaction Amidst Covid-19. In Contemporary Issues and Challenges in Management Research, *International Journal of Business Research Management*: 40-50.

La Porte, T. R., and Metlay, D. S. (1996). Hazards and institutional trustworthiness: Facing a deficit of trust. *Public Administration Review*, 56(4): 341-347. https://doi.org/10.2307/976375.

Lane, C., and Bachmann, R. (1996). The social constitution of trust: Supplier relations in Britain and Germany. *Organization Studies*, 17: 365–395. https://doi.org/10.1177/017084069601700302.

Lane, C., and Bachmann, R. (1997). Co-operation in inter-firm relations in Britain and Germany: the role of social institutions. *British Journal of Sociology*, 48(2): 226-254.https://doi.org/10.2307/591750.

Lankton, N., McKnight, D. H., and Thatcher, J. B. (2014). Incorporating trust-in-technology into Expectation Disconfirmation Theory. *Journal of Strategic Information Systems*, 23(2): 128-145.https://doi.org/10.1016/j.jsis.2013.09.001.

Lessig, L. (2003). Law Regulating Code Regulating Law. *Loyola University Chicago Law Journal*, 35(1): 1-10.

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

Levi, M. (1998). A state of trust. In M. Levi and V. Braithwaite (Eds.), *Trust and Governance*: 77-101. New York: Russell Sage Foundation.

Lewicki, R. J., McAllister, D. J., and Bies, R. J. (1998). Trust and distrust: New relationships and realities. *Academy of Management Review*, 23(3): 438-458.https://doi.org/10.5465/amr.1998.926620.

Lewis, J. D., and Weigert, A. J. (1985). Social atomism, holism, and trust. *Sociological Quarterly*, 26(4): 455-471.https://doi.org/10.1111/j.1533-8525.1985.tb00238.x.

Lohmer, J., Bugert, N., and Lasch, R. (2020). Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: An agent-based simulation study. *International Journal of Production Economics*, 228: 107882. https://doi.org/10.1016/j.ijpe.2020.107882.

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

Lukyanenko, R., Maass, W., &Storey, V. C. (2022). Trust in artificial intelligence: From a Foundational Trust Framework to emerging research opportunities. *Electronic Markets*, 32(4): 1993-2020.https://doi.org/10.1007/s12525-022-00605-4.

Lumineau, F., and Oliveira, N. (2018). A pluralistic perspective to overcome major blind spots in research on interorganizational relationships. *Academy of Management Annals*, 12(1): 440-465.https://doi.org/10.5465/annals.2016.0033.

Lumineau, F., and Oliveira, N. (2020). Reinvigorating the study of opportunism in supply chain management. *Journal of Supply Chain Management*, 56(1): 73-87.https://doi.org/10.1111/jscm.12215.

Lumineau, F., Wang, W., andSchilke, O. (2021). Blockchain governance - A new way of organizing collaborations?. *Organization Science*, 32(2): 500-521.https://doi.org/10.1287/orsc.2020.1379.

Manski, S. (2017). Building the blockchain world: Technological commonwealth or just more of the same?. *Strategic Change*, 26(5): 511-522.https://doi.org/10.1002/jsc.2151.

Manski, S., and Bauwens, M. (2020). Reimagining new socio-technical economics through the application of distributed ledger technologies. *Frontiers in Blockchain*, 2 (29): 1-17. https://doi.org/10.3389/fbloc.2019.00029.

Maurer, B., Nelms, T. C., and Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. *Social Semiotics*, 23(2): 261-277.https://doi.org/10.1080/10350330.2013.777594.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3): 709-734. https://doi.org/10.5465/amr.1995.9508080335.

McCroskey, J. C., and Young, T. J. (1981). Ethos and credibility: The construct and its measurement after three decades. *Communication Studies*, 32(1): 24-34. https://doi.org/10.1080/10510978109368075.

McKnight, D. H., Cummings, L. L., and Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review*, 23(3): 473-490. https://doi.org/10.5465/amr.1998.926622.

Mishra, A. K., and Mishra, K. E. (2013). The research on trust in leadership: The need for context. *Journal of Trust Research*, 3(1): 59-69. https://doi.org/10.1080/21515581.2013.771507.

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1(11): 501-507. https://doi.org/10.1038/s42256-019-0114-4.

Murray, A., Rhymer, J. E. N., and Sirmon, D. G. (2021). Humans and technology: Forms of conjoined agency in organizations. *Academy of Management Review*, 46(3): 552-571. https://doi.org/10.5465/amr.2019.0186.

Murray, A., Kuban, S., Josefy, M., and 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*, 35(4): 622-641. https://doi.org/10.5465/amp.2018.0066.

Nomura, T., Kanda, T., and Suzuki, T. (2006). Experimental investigation into influence of negative attitudes toward robots on human–robot interaction. *AIand Society*, 20: 138-150. https://doi.org/10.1007/s00146-005-0012-7.

Nooteboom, B. (2007). Social capital, institutions and trust. *Review of Social Economy*, 65(1): 29-53. https://doi.org/10.1080/00346760601132154.

North, D. C. (1990). A transaction cost theory of politics. *Journal of Theoretical Politics*, 2(4): 355-367. https://doi.org/10.1177/0951692890002004001.

Ølnes, S., Ubacht, J., and Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, 34(3): 355-364. https://doi.org/10.1016/j.giq.2017.09.007.

Pavlou, P. A., and Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1): 37-59. https://doi.org/10.1287/isre.1040.0015.

Queiroz, M. M., and Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management*, 46: 70-82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021.

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

Roeck, D., Sternberg, H., and Hofmann, E. (2020). Distributed ledger technology in supply chains: a transaction cost perspective. *International Journal of Production Research*, 58(7): 2124-2141. https://doi.org/10.1080/00207543.2019.1657247.

Rogers, E. M. (1995). Lessons for guidelines from the diffusion of innovations. *Joint Commission Journal on Quality Improvement*, 21(7): 324-328. https://doi.org/10.1016/S1070-3241(16)30155-9.

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *American Psychologist*, 26(5), 443-452. https://psycnet.apa.org/doi/10.1037/h0031464.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3): 393-404. https://doi.org/10.5465/amr.1998.926617.

Saberi, S., Kouhizadeh, M., Sarkis, J., and Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7): 2117-2135. https://doi.org/10.1080/00207543.2018.1533261.

Schmidt, C. G., and Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management*, 25(4): 100552. https://doi.org/10.1016/j.pursup.2019.100552.

Schoorman, F. D., Mayer, R. C., and Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, 32(2): 344-354. https://doi.org/10.5465/amr.2007.24348410.

Sekhon, H., Ennew, C., Kharouf, H., and Devlin, J. (2014). Trustworthiness and trust: influences and implications. *Journal of Marketing Management*, 30(3-4): 409-430. https://doi.org/10.1080/0267257X.2013.842609.

Shah, A., Nasir, N., and Shah, A. (2024). Inclusive Design in AI-Driven Leadership: Implementation and Challenges in Small Businesses. International Journal of Research Management, 15(1): 19-42.

Shapiro, S. P. (1987). The social control of impersonal trust. *American Journal of Sociology*, 93: 623–658. https://doi.org/10.1086/228791.

Simon, H., and Frantz, R. (2003). Artificial Intelligence as a Framework for Understanding Intuition. *Journal of Economic Psychology*, 24(2): 265-277. http://dx.doi.org/10.1016/S0167-4870(02)00207-6.

Sitkin, S. B., and Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. *Academy of Management Review*, 17(1): 9-38.https://doi.org/10.5465/amr.1992.4279564.

Skinner, B. F. (1984). An operant analysis of problem solving. *Behavioral and Brain Sciences*, 7(4): 583-591. https://doi.org/10.1017/S0140525X00027412.

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. https://doi.org/10.1057/jit.2010.17.

Tan, T. M., & Saraniemi, S. (2023). Trust in blockchain-enabled exchanges: Future directions in blockchain marketing. *Journal of the Academy of Marketing Science*, 51(4): 914-939. https://doi.org/10.1007/s11747-022-00889-0.

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

Teodorescu, M. H., Morse, L., Awwad, Y., and Kane, G. C. (2021). Failures of Fairness in Automation Require a Deeper Understanding of Human-ML Augmentation. *MIS Quarterly*, 45(3): 1483-1500. http://doi.org/10.25300/MISQ/2021/16535.

Tilson, D., Lyytinen, K., and Sørensen, C. (2010). Research commentary - Digital infrastructures: The missing IS research agenda. *Information Systems Research*, 21(4): 748-759. https://doi.org/10.1287/isre.1100.0318.

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

Tseng, S., and Fogg, B. J. (1999). Credibility and computing technology. *Communications of the ACM*, 42(5): 39-44. https://doi.org/10.1145/301353.301402.

Tyler, T. R., and Degoey, P. (1996). Trust in organizational authorities. In *Trust in organizations: Frontiers of Theory and Research*: 331-356. Sage Publications. https://doi.org/10.4135/9781452243610.n16.

Tyler, T. R., and Lind, E. A. (1992). A relational model of authority in groups. *Advances in Experimental Social Psychology*, 25: 115-191. https://doi.org/10.1016/S0065-2601(08)60283-X.

Wang, J., Wu, P., Wang, X., and Shou, W. (2017). The outlook of blockchain technology for construction engineering management. *Frontiers of Engineering Management*, 4(1): 67-75. https://doi.org/10.15302/J-FEM-2017006.

Williamson, O. E. (1993). Calculativeness, trust, and economic organization. *The journal of Law and Economics*, 36(1, Part 2), 453-486. https://doi.org/10.1086/467284.

Williamson, O. E. (1985). *The Economic Institutions of Capitalism*. New York: The Free Press.

Wong, L. W., Tan, G. W. H., Ooi, K. B., & Dwivedi, Y. (2024). The role of institutional and self in the formation of trust in artificial intelligence technologies. *Internet Research*, 34(2): 343-370. https://doi.org/10.1108/INTR-07-2021-0446.

Wood, A. J., Lehdonvirta, V., and Graham, M. (2018). Workers of the Internet unite? Online freelancer organisation among remote gig economy workers in six Asian and African countries. *New Technology, Work and Employment*, 33(2): 95-112. https://doi.org/10.1111/ntwe.12112.

Zaheer, A., McEvily, B., and Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, 9(2): 141-159. https://doi.org/10.1287/orsc.9.2.141.

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

Zhao, J. L., Fan, S., and Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, 2(1): 1-7. https://doi.org/10.1186/s40854-016-0049-2.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. In B. M. Stawand L. L. Cummings (Eds.), *Research in Organizational Behaviour*, 8: 53-111. Greenwich, CT: JAI Press.