Journal of the Association for Information Systems

Volume 26 | Issue 1 | Article 6

2025

Uncovering the Structural Assurance Mechanisms in Blockchain Technology-Enabled Online Healthcare Mutual Aid Platforms

Zhen Shao
Harbin Institute of Technology, shaozhen@hit.edu.cn

Lin Zhang
Northwestern Polytechnical University, zhanglin0713@nwpu.edu.cn

Susan A. Brown
University of Arizona, suebrown@arizona.edu

Jose Benitez
Kent State University, jbenite1@kent.edu

Recommended Citation

Shao, Zhen; Zhang, Lin; Brown, Susan A.; and Benitez, Jose (2025) "Uncovering the Structural Assurance Mechanisms in Blockchain Technology-Enabled Online Healthcare Mutual Aid Platforms," *Journal of the Association for Information Systems*, 26(1), 128-170.
DOI: 10.17705/1jais.00901
Available at: https://aisel.aisnet.org/jais/vol26/iss1/6

Journal of the Association for Information Systems (2025) **26**(1), 128-170
doi: 10.17705/1jais.00901

RESEARCH ARTICLE

ISSN 1536-9323

Uncovering the Structural Assurance Mechanisms in Blockchain Technology-Enabled Online Healthcare Mutual Aid Platforms

Zhen Shao,[1] Lin Zhang,[2] Susan A. Brown,[3] Jose Benitez[4]

[1]School of Management, Harbin Institute of Technology, China, shaozhen@hit.edu.cn
[2]School of Management, Northwestern Polytechnical University, China, zhanglin0713@nwpu.edu.cn
[3]Eller College of Management, The University of Arizona, USA, suebrown@arizona.edu
[4]Ambassador Crawford College of Business and Entrepreneurship, Kent State University, USA, jbenite1@kent.edu

Abstract

How can assurance mechanisms be effectively enacted to promote users' behavioral outcomes on online healthcare mutual aid platforms? To answer this research question, this study draws upon institutional trust theory and develops a research model to examine the influence mechanisms of two specific structural assurances (i.e., policy assurance and technology assurance) on users' intentions and actual usage behaviors in a blockchain-enabled online healthcare mutual aid platform. We conducted a field survey in two time periods and employed structural equation modeling to test the research model. We found that both *policy assurance* that reflects institutional (i.e., legal, contractual, and regulatory) structures and *blockchain-enabled technology assurance* that describes reliable technical features (i.e., high data anonymity, immutability, transparency, and disintermediation) play salient roles in facilitating users' trust in the platform, which in turn affects their behavioral intentions and actual usage behaviors in the online healthcare mutual aid platform. The research findings provide a comprehensive understanding of how platform assurances influence users' behavioral outcomes in the evolving context of blockchain-enabled applications.

Keywords: Structural Assurance, Behavioral Intention, Actual Usage Behaviors, Blockchain Technology, Healthcare, Trust

Saonee Sarker was the accepting senior editor. This research article was submitted on November 18, 2022, and underwent three revisions. Lin Zhang is the corresponding author.

1 Introduction

Online healthcare mutual aid services have been widely adopted by insurers as a form of peer-to-peer (P2P) micro-insurance and have been identified as a more ethical and social alternative to standard insurance (Shao et al., 2022a). Essentially, a mutual aid service platform operates similarly to crowdfunding (Abdikerimova & Feng, 2022), where a group of people joins an insurance risk pool to support each other. It functions as a two-sided marketplace offering quotes for mutual aid claims, group financial protection, and other support services. When one of the members incurs an illness, they can make a claim to receive a payment shared by others (Shao et al., 2022a). Among the 70 global P2P micro-insurance platforms, online healthcare mutual aid platforms are recognized as one of the most popular P2P insurance platforms (e.g., Eusoh, Shuidihuzhu, Xianghubao, YuLife, etc.)[1] and have seen rapid development in practice.

[1] https://tracxn.com/d/trending-themes/Startups-in-P2P-Insurance (accessed July 10, 2022).

However, the utilization of online healthcare mutual aid platforms remains inadequate due to frequent incidents of fraud and the continuous flow of negative news (see Appendix A for details). Specifically, reports of fraudulent activities, such as false claims and the misappropriation of claim funds, have become increasingly common, fostering skepticism and apprehension among users who participate in online healthcare mutual aid platforms. Furthermore, the traditional methods employed to detect mutual aid claim fraud have primarily focused on post-event assurance and regulation mechanisms rather than proactive prevention (West & Bhattacharya, 2016) and have been proven inefficient and ineffective thus far (ISSA, 2022). Compounding these issues, the negative news coverage surrounding these incidents has further contributed to a grim perception of the industry, leading to distrust in online healthcare mutual aid platforms and hindering individuals from utilizing such platforms (Agarwal et al., 2010; Shao et al., 2022a). Consequently, concerning the potential loss of personal interest in mutual aid services, facilitating individuals' trust and ensuring their subsequent usage behaviors on online healthcare mutual aid platforms, while crucial for the sustainable growth and success of the online healthcare mutual aid ecosystem, has become a great challenge confronting both scholars and practitioners.

Prior information systems (IS) literature has identified the critical role of structure assurance in creating a trusted environment and formulating users' subsequent behavioral outcomes (Gefen et al., 2008; Mai et al., 2010; McKnight et al., 2002a, 2002b; Pavlou & Gefen, 2004; Shao et al., 2019). However, to our knowledge, most of the previous studies have focused on one specific assurance mechanism, such as policy statements or seals (Bansal & Gefen, 2010; Dimoka et al., 2012; Kim & Benbasat, 2009; Özpolat et al., 2013; Park et al., 2010), while little attention has been paid to the specific influence of technology assurance. As McKnight et al. (2002a, 2002b) argued, structure assurance refers to "institutional structures like guarantees, regulations, promises, legal recourse … [as well as] technological internet protections like data encryption safeguard." According to this view, structural assurance has two components—policy assurance, emphasizing the establishment of institutional (i.e., legal, contractual, regulatory) structures, and technology assurance, involving technical standards, security procedures, and protection mechanisms. Given today's digital world of escalating security threats, technology outages, data integrity, quality issues, and privacy mandates, technology assurance is considered to be a more robust solution than policy assurance (Shao et al., 2022b), which requires more attention. However, our understanding of the conceptualization and influence mechanism of technology assurance is still limited in the theoretical literature.

Notably, emerging technologies such as blockchain play salient roles in solving the persistent challenges faced by online healthcare mutual aid platforms and revolutionizing the landscape (Upadhyay, 2020). Blockchain technology, renowned for its cryptographic security, immutability, transparency, and decentralized nature, presents an opportunity to address the shortcomings of traditional assurance methods in the mutual aid ecosystem. In the blockchain case, for mutual aid healthcare platforms, technology assurance represents the implementation of blockchain technology to ensure that the mutual aid process is anonymous, transparent, immutable, and disintermediated. By leveraging the unique features of blockchain, online healthcare mutual aid platforms can establish a robust and tamper-proof technology assurance that enhances security, verifiability, and accountability throughout the entire mutual aid process and fund allocation (Liang et al., 2021; Rossi et al., 2019). Therefore, given the salience of blockchain in creating a safe and secure healthcare mutual aid environment, it is essential to integrate blockchain-enabled technology assurance with policy assurance and systematically examine their joint influence mechanisms on trust, users' intention, and actual usage behaviors in the emerging context. As such, the following research question is proposed: *How do platform assurances (i.e., policy assurance and blockchain-enabled technology assurance) affect individuals' behavioral intention and actual usage behaviors on blockchain-enabled healthcare mutual aid platforms?*

To address the research objectives, we drew on institutional trust theory to establish a theoretical model and collected field survey data from 205 users in two different time periods: (1) In the first period, we assessed users' perceptions towards the two platform assurances, trust, and behavioral intention; (2) in the second period, six months later, we captured users' actual usage behaviors. The research findings helped us develop a comprehensive understanding of users' behaviors in the emerging context of blockchain-enabled applications.

2 Theory and Hypotheses

In this section, we first delve into the institutional trust theory and its key components, namely institutional trust antecedents (i.e., assurance mechanisms), trust, and trust-related behaviors, which provide a solid theoretical foundation to develop our research model. Then, we incorporated the key components of institutional trust to facilitate the elucidation of concepts and hypothesized relationships in the specific context of online healthcare mutual aid services.

2.1 Institutional Trust Theory

The construct of trust originates from social psychology, referring to an individual's belief (trustor) that the other party (trustee) will act in a proper and socially acceptable manner and behavior (Zucker, 1986). Notably, institutional trust emerges as a pivotal mode by which trust is created in impersonal economic environments (Pavlou, 2002; Pavlou & Gefen, 2004). Institutional trust carries both theoretical and practical significance in the context of our study. Theoretically, the extant literature shows that institutional trust offers a valuable theoretical framework for understanding the trust-building process that occurs when individuals adopt and utilize specific IS, encompassing three key components (i.e., institutional trust antecedents, trust, and trust-related behaviors) (Avgerou, 2013; McKnight et al., 2002a; Pavlou, 2002). Specifically, institutional trust antecedents are conceptualized from the structural assurance perspective, representing an individual's perception of the general institutional environment (Gefen et al., 2003; Kim et al., 2009; Lu et al., 2016; McKnight et al., 2002a, 2002b; Shao & Yin, 2019a). Trust refers to the degree to which an individual believes that the other party will act in proper behaviors regarding its ability (i.e., the trustee is competent to satisfy users' requirements), benevolence (i.e., the trustee can act in the users' best interest), and integrity (i.e., the trustee is honest and can keep promises) (Bhattacherjee, 2002; Liu & Liu, 2019), while trust-related behaviors are individuals' decision-making results, including sharing information (Bansal et al., 2015), making purchase decisions (Fang et al., 2014), and adopting online platforms (Pavlou, 2002; Shao & Yin, 2019b). Institutional trust theory provides a theoretical lens for our study, suggesting that individuals rely on structural assurance mechanisms to foster the formation of trust, which further facilitates their behaviors in online healthcare mutual aid platforms (Fang et al., 2014; Kim et al., 2016).

Moreover, institutional trust also holds practical relevance for online healthcare mutual aid services, as supported by anecdotal evidence (see Appendix A for detailed information). First, users depend upon the competence and expertise of online healthcare mutual aid platforms to participate in mutual aid services in an expected manner (Shao et al., 2022a). However, according to practical reports, more than 70.4% of donors harbor distrust in online healthcare mutual aid platforms, since there have been fraudulent incidents involving allegations of illegal fundraising and misappropriation (see Appendix A). These incidents have instilled doubts among users regarding mutual aid platforms' assurances of safeguarding their interests. Second, reports[2] have revealed platform staff members incentivizing patients/recipients to withhold information or using preexisting templates to gain public sympathy for the purpose of fundraising. Staff members may receive commissions based on the total amount raised, invoking concerns that online healthcare mutual aid platforms' initiatives may prioritize the platform's interests (see Appendix A). Consequently, online healthcare mutual aid platforms often deliberately avoid conducting comprehensive claim reviews and may conceal information about aid and capital flow. These practices have caused user doubts regarding online healthcare mutual aid platforms' commitments, regulations, promises, and available legal remedies (Abdikerimova & Feng, 2022). These instances thus underscore the importance of establishing effective structural assurance mechanisms to promote users' trust in online healthcare mutual aid services.

Therefore, we draw upon the institutional trust lens to examine individuals' trust formation mechanism and subsequent trust-related behaviors in blockchain-enabled healthcare mutual aid platforms. We provide a detailed elucidation of the concepts in our research context, as noted in Table 1 and the subsequent sections.

Table 1. Conceptualization of Core Constructs

Key components	Construct	Conceptualization	Sources
Institutional trust antecedents	Policy assurance	Users' perceptions of the extent to which online healthcare mutual aid platforms establish institutional (i.e., legal, contractual, and regulatory) structures.	Kim & Benbasat, 2009
	Blockchain-enabled technology assurance	Users' perceptions of the extent to which online healthcare mutual aid platforms establish technological safeguards and preventive measures with high data anonymity, immutability, transparency, and disintermediation.	Hughes et al., 2008; Ostern, 2018; Shao et al., 2022a; Underwood, 2016
Trust	Trust in the platform	Users' belief that online healthcare mutual aid platforms will behave properly in terms of ability, benevolence, and integrity.	Bhattacherjee, 2002; Shao et al., 2019
Trust-related behaviors	Intention to use	Users' intention to use online healthcare mutual aid platforms.	Bhattacherjee & Lin, 2015
	Actual usage behavior	Users' frequency and intensity of using online healthcare mutual aid platforms per month.	Moores & Chang, 2006

[2] https://www.chinanews.com.cn/m/gn/2016/09-08/7997616.shtml

2.2 Assurance Mechanisms as Institutional Antecedents and Trust

Originating from institutional trust literature (Zucker, 1986), structural assurance has aroused the attention of scholars in the IS discipline. One of the earliest and most popular conceptualizations of assurance mechanisms was proposed by McKnight et al. (2002b, p. 304-305), who defined it as "the belief that the web has protective legal or technological structures that assure that web business can be conducted in a safe and secure manner." Over the past decade, structural assurance has been widely applied in various research contexts, including e-commerce (Gefen et al., 2003; Kim et al., 2016; Pavlou, 2002, 2011), mobile commerce (Dimoka et al., 2012; Hui et al., 2007; Mai et al., 2010; McKnight et al., 2004; Pavlou & Gefen, 2004), internet finance (Kim et al., 2009; Kim & Benbasat, 2009), and the sharing economy (Hawlitschek et al., 2018). Prior studies on structural assurance have mostly focused on one specific type of policy assurance, referring to policy statements regarding agreements, contracts, regulations, laws, and guarantees, as well as policy assurance seals and icons granted by independent third-party certifying bodies (e.g., banks, accountants, consumer unions, etc.) (Bansal et al., 2015; Kim et al., 2009; Kim & Benbasat, 2009; Shao et al., 2019; Shao & Yin, 2019b; Smith et al., 2011). Compared with policy assurance, only a handful of studies attend to technology assurance (Li et al., 2008; McKnight et al., 2002a, 2002b, 2004). Furthermore, to the best of our knowledge, the extant literature has mostly considered structural assurance to be a first-order construct, without distinguishing between policy assurance and technology assurance, and few studies have examined the joint influence of the two assurance mechanisms on individuals' trust and behavioral intentions (see Appendix B for a detailed overview).

Reflecting the context of online healthcare mutual aid services, we divide structural assurance into two dimensions—policy assurance and blockchain-enabled technology assurance—which can be distinguished based on their underlying mechanisms. Inspired by information security literature (Dhillon et al., 2021; Tee & Murugesan, 2018; Tennyson & Salsas-Forn, 2002; Viaene et al., 2002; Wang & Kogan, 2018) and assurance literature (Bansal et al., 2015; Hawlitschek et al., 2018; Kim et al., 2009; Pavlou, 2002; Shao et al., 2022a), we summarize the characteristics and key functions of policy assurance and blockchain-enabled technology assurance in Table 2.

On the one hand, policy assurance primarily revolves around establishing rules, guidelines, and protocols to ensure preventive controls, compliance, and the detection of potential issues or violations (Viaene et al., 2002). Such policy assurance involves setting up policies and procedures that govern users' behaviors and activities on online healthcare mutual aid platforms. Meanwhile, policy assurance aims to detect noncompliant behaviors or policy violations and take appropriate actions to address them (Gefen et al., 2003), such as monitoring user activities, conducting audits, and enforcing penalties or sanctions for speculation or deception when necessary (Abdikerimova & Feng, 2022).

On the other hand, blockchain-enabled technology assurance acts as an innovative technology assurance solution that leverages digital technologies to proactively prevent potential risks (e.g., unauthorized access, misuse, potential threats, or breaches) and protect users' interests on the emerging online healthcare mutual aid platforms. For instance, enabled by blockchain technology, Xianghubao is recognized as one of the largest online platforms providing basic healthcare mutual aid services (see the description in Appendix C for reference). The platform has implemented blockchain technology to ensure the security of online transactions and avoid the deceitful behaviors of other members. Specifically, blockchain technology enables the efficiency of technology assurance to support members' queries and audits, leading to lower fraudulent claims due to the characteristics of disintermediation, immutability, anonymity, and transparency.

First, the disintermediation of blockchain technology enables claim transactions to operate in a P2P network without the interference of intermediaries (Queiroz & Wamba, 2019), thus facilitating cost-efficient transactions and reducing the complexity of claim execution on the platform (Kamble et al., 2020). Second, data stored on the platform (e.g., registration, certification, and claim information) is permanently recorded in a chronologically ordered manner and is accessible to all participants. Thus, the immutability of blockchain technology benefits identity and data verification and consequently prevents data corruption and insurance fraud (Hughes et al., 2019). Third, this technology allows the identity information of members (e.g., name, address, and telephone number) to remain undisclosed on the platform (Kamble et al., 2020). Therefore, blockchain technology enables users to maintain high data anonymity, thereby ensuring identity privacy and security. Fourth, when a claim occurs on the platform, a tamper-proof blockchain certificate is disclosed to all members, recording the number of members who have shared the claim payment, the number of claims, and the corresponding case details. As such, the transparency of medical claims enables users to track their donations until they are provided with a blockchain certificate to verify that their donations have been received, thus enhancing users' perceptions of visible and transparent claim information stored on the blockchain (see the description in Appendix C for reference of the four blockchain-enabled technology assurance mechanisms).

Table 2. Summary of Policy Assurance and Blockchain-Enabled Technology Assurance

Assurance	Key features	Essential functions	References
Policy assurance	• Including self-generated policy statements, policy arguments, and seals from independent intermediaries. • Policy assurance establishes rules, monitors compliance, and restricts online healthcare mutual aid platforms from disclosing.	Policy assurance is *the fundamental assurance that focuses on preventive controls, post-event detection, and regulation mechanisms*, including critical functions, e.g., the collective claim-sharing clause, the scope of claims, membership rules, detailed statements regarding sanctions for noncompliance, online dispute resolution mechanisms, privacy protection, and overall platform governance.	Bansal et al., 2015; Dimoka et al., 2012; Gefen et al., 2003; Hui et al., 2007; Kim & Benbasat, 2009; Kim et al., 2016; Mai et al., 2010; Özpolat et al., 2013; Park et al., 2010; Pavlou, 2002
Blockchain-enabled technology assurance	• Including stand-alone assurance technologies (i.e., blockchain) that have specific roles and functions to support high data security. • Blockchain-enabled technology assurance integrates advanced blockchain technology features that refine the platform assurance without user intervention.	Blockchain-enabled technology assurance is *the proactive prevention-oriented assurance that leverages digital technological safeguards and preventive measures to mitigate risks and protect users' interests* and encompasses key functions, e.g., substantial security improvements in terms of high data anonymity, immutability, transparency, and disintermediation.	Hawlitschek et al., 2018; Saha et al., 2016; Shao et al., 2022a

Policy assurance and trust: Based on institutional trust theory (Bansal et al., 2015; McKnight et al., 2002b), users tend to use policy assurances, e.g., regulations and third-party guarantees, to make trust inferences about a platform (Kim et al., 2009). For instance, Jha and Shah (2021) argued that the informational and normative aspects of arguments have significant effects on perceived credibility. In the context of online healthcare mutual aid services, policy assurance primarily depends on establishing rules and monitoring compliance and is established by experienced experts or third-party agents (Shao et al., 2022a). Its purpose is to conduct audits and enforce penalties or sanctions for speculation or deception when necessary (Bansal et al., 2015; Kim & Benbasat, 2009), focusing on identifying fraud in specific mutual aid cases (Abdikerimova & Feng, 2022). Thus, when users perceive that policy assurance can enable appropriate actions to address noncompliant mutual aid behaviors or policy violations (Gefen et al., 2003), they are more likely to trust the ability of online healthcare mutual aid platforms to safeguard their interests. Moreover, in the specific context of online healthcare mutual aid services, policy assurance encompasses resources such as calling on a jury of participating users to engage in a deliberation process in the case of disputed mutual aid claims. The jury mechanism empowers users' rights, thereby improving their confidence in the benevolence of the online healthcare mutual aid platform. Additionally, online healthcare mutual aid platforms (e.g., Xianghubao) can define responsibilities (e.g., collective claim-sharing clause, the scope of claims, membership rules, and guarantee details) and set up explicit and detailed policies such as rigorous access restrictions (e.g., users with a Sesame credit score of 650 and above can join the platforms),[3] health requirements (e.g., users need to satisfy basic health criteria for registering as members), and transparent feedback policy (e.g., the platform guarantees to provide information regarding the diagnosed illness, the hospitals where beneficiaries receive treatment, and the amount of mutual aid money). Such policy assurances are beneficial to enhancing the fairness of dealings, which in turn increases users' confidence in the integrity of the online healthcare mutual aid platform. The above analysis thus leads to the following hypothesis:

H1: Policy assurance is positively associated with trust in an online healthcare mutual aid platform.

[3] Sesame Credit is a private credit score developed by Ant Group, like the FICO score in the US. Similar to using credit scores to evaluate the risk of lending money to consumers in banks and credit card companies, Sesame Credit is used to evaluate applicants' trustworthy profiles by analyzing their online transactions and behavior data in the usage of all Alibaba products, spanning over insurance, historical payment, shopping, and mobility data. Sesame Credit is a three-digit number, ranging from 350 to 950, and the higher the score, the better the personal credit. A credit score of 650 is set up as the lower limit score for joining Xianghubao.

Blockchain-enabled technology assurance and trust: In the context of emerging technology applications, technological safeguards, such as technological encryption protection, are also beneficial for promoting trust (Carvalho, 2021; McKnight et al., 2002a, 2002b, 2004; Mou & Cohen, 2015). Technology structures can establish users' general expectations, in turn guiding users' trust perceptions (Li et al., 2008). For example, Nicolaou and McKnight (2011) argued that technological internet protection has a positive effect on users' intention to use electronic data exchange systems. In our research context, technology assurance is manifested in blockchain technology, which encompasses features such as disintermediation, immutability, anonymity, and transparency. First, users can perceive the disintermediation feature afforded by blockchain technology by signing a smart consensus-based contract and experiencing the claim transaction process. Online healthcare mutual aid platforms can notify all other node users about the claim information when claims occur on one node (i.e., a patient) without the participation of third parties. Second, users' perception of data immutability features can be enhanced by tamper-proof blockchain signals. By checking the mutual aid transaction history, users can find each claim data is registered in the blockchain by creating digital encryption using hash functions with a date and time stamp. Third, users can perceive anonymity because blockchain ensures the anonymization of identity data presented on online healthcare mutual aid platforms. Fourth, users can perceive the transparency feature of blockchain technology through the disclosure of comprehensive claim records to all users. These records include details such as the number of members who participated in the payment and specific claim information.

In the context of online healthcare mutual aid services, blockchain-enabled technology assurance can play a salient role in influencing trust beliefs, specifically regarding the ability, benevolence, and integrity of the platform. For instance, during the settlement of a claim payment, the verification process involves all users in the blockchain network. If there are no objections from the users during the public review, the claim-sharing funds are automatically transferred from the P2P network based on blockchain consensus. This disintermediation feature of blockchain can enhance users' confidence in the capability of the online healthcare mutual aid platform to execute claim payment decisions effectively by fulfilling its responsibilities and obligations. Meanwhile, blockchain technology can protect information from malicious tampering via verifiable processes and can maintain the safety of the mutual aid transaction history, which would enhance users' confidence in the ability of the online healthcare mutual aid platform to ensure a rational and secure execution of procedures. Moreover, the cryptography feature of blockchain (e.g., cryptographic hash) can protect users from privacy leaks by ensuring the anonymization of identity data, which would strengthen users' confidence in the benevolence of the online healthcare mutual aid platform and its commitment to their privacy and overall welfare. Additionally, a transaction record containing block information and certificate authority could be released when a claim occurs. This transparency feature would reduce information asymmetry by ensuring that all users have access to the same information, demonstrating the openness and fairness of the online healthcare mutual aid platform, thereby enhancing users' belief in the integrity of the online healthcare mutual aid platform. Therefore, since blockchain technology ensures disintermediation, immutability, anonymity, and transparency of the claim process, users' belief in the ability, benevolence, and integrity of the online healthcare mutual aid platform should be enhanced accordingly. The above analysis leads to the following hypothesis:

H2: Blockchain-enabled technology assurance is positively associated with trust in an online healthcare mutual aid platform .

2.3 Trust in the Platform, Behavioral Intention, and Actual Usage Behaviors

Trust-related outcomes refer to the results and consequences stemming from establishing trust in a particular context (McKnight et al., 2002a). In particular, behavioral intention is recognized as a salient trust-related outcome (Li et al., 2008; Shao et al., 2019; Shao & Yin, 2019b), which captures an individual's willingness to perform the actual behaviors. Given the popularity of blockchain technology, scholars have focused on examining users' behavioral intention towards blockchain-enabled applications across various contexts, including supply chain management (Queiroz & Wamba, 2019), financial services (Wang et al., 2019), and the sharing economy (Hawlitschek et al., 2018). For example, Hawlitschek et al. (2018) posited that trust positively affects renting intentions regarding blockchain-enabled peer-to-peer sharing services.

Despite the attention paid to blockchain technology and its applications by IS scholars in several research contexts, most of the extant literature focuses on organizational-level adoptions. To the best of our knowledge, only a handful of empirical studies have investigated individuals' behavioral intention regarding blockchain-enabled applications (Liang et al., 2021; Shao et al., 2022a). Moreover, existing research has mostly considered behavioral intention to be a salient proxy for actual behaviors and has measured individuals' behavioral intention using cross-sectional data (Kamble et al., 2020; Queiroz & Wamba, 2019; Wong et al., 2020). Indeed, few studies have provided deep insight into individuals' actual usage behaviors towards blockchain-enabled applications after the initial adoption stage.

This study incorporates both the intention to use and actual usage behaviors in its theoretical model to effectively explain the individual's decision-making process on blockchain-enabled healthcare mutual aid platforms. On the one hand, when users believe that a mutual aid platform is reliable and can provide online healthcare mutual aid services with ability, benevolence, and integrity, their behavioral intentions will be enhanced accordingly. As mentioned above, joining an online healthcare mutual aid platform entails risks such as the potential for fraudulent activities and the misuse of funds (see Appendix A). However, trust plays a crucial role in alleviating users' concerns about such potential risks by enabling them to subjectively dismiss the apprehension of undesirable fraudulent activities associated with online healthcare mutual aid platforms. On the other hand, following a deductive logic (Ajzen, 1991), users' intentions can further influence their actual usage behaviors on online healthcare mutual aid platforms. Therefore, we propose the following hypotheses:

H3: Trust in an online mutual aid platform is positively associated with the intention to use it.

H4: The intention to use an online mutual aid platform is positively associated with actual usage behavior.

Drawing upon the institutional trust lens, this study integrates policy assurance and blockchain-enabled technology assurance, to examine their joint influences on users' behavioral intention and actual usage behaviors through the mediation mechanism of trust in the platform. We incorporated individual characteristics (i.e., gender, age, experience, monthly income, familiarity with blockchain technology, altruism, perceived innovativeness) as control variables to rule out other potential influences on the intention to use and actual usage behaviors, as suggested in prior literature (Agarwal & Karahanna, 2000; Venkatesh et al., 2012). The proposed research model is described in Figure 1.

3 Research Methodology

3.1 Data Collection

We conducted an online survey and collected data from the target population (i.e., actual users of Xianghubao). We selected sojump.com, one of China's most popular online questionnaire platforms, to edit and distribute the questionnaires to the target samples through online links. Sojump.com is a widely recognized survey platform for conducting academic research in China and offers numerous benefits, including ease of administration, random sampling, quality monitoring, and the ability to collect data from multiple time points. The questionnaire comprised four sections. In the first section, we clearly articulated the research motivation of this study. In particular, we assured the respondents that their participation would be anonymous and that the collected data would only be used for academic research. In the second section, we screened the sample following two steps. First, we asked the respondents whether they had previously used the Xianghubao platform. Those who answered "No experience" were excluded from the study. Second, we asked the respondents whether they had focused on the detailed policies and blockchain-enabled technology assurance established by the Xianghubao platform (see details in Appendix C).

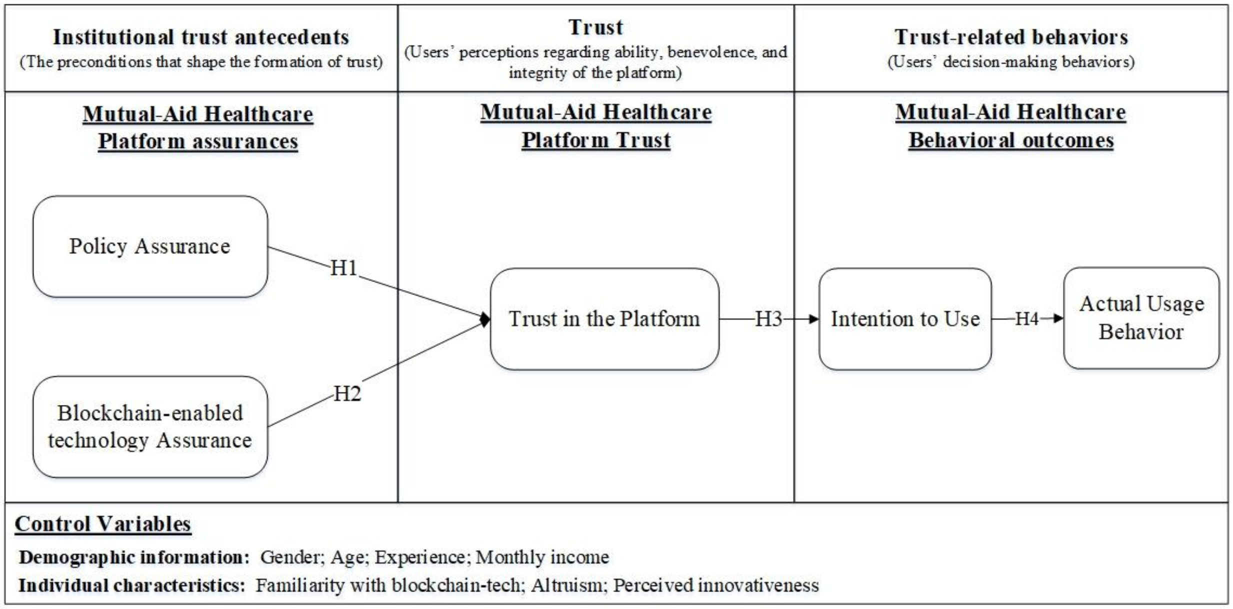
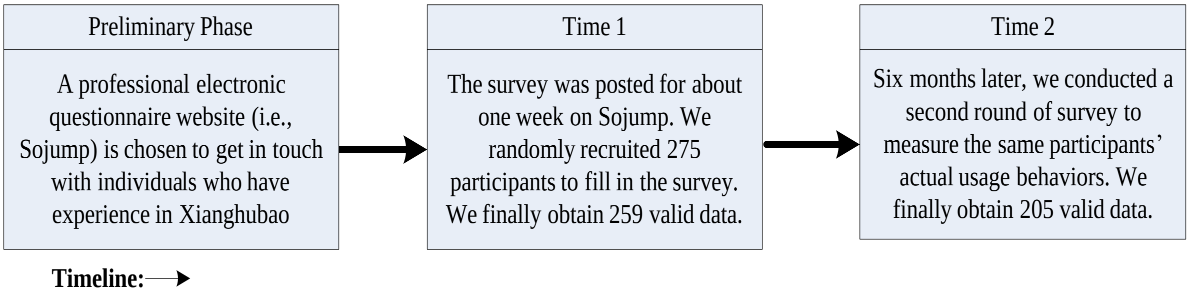

Institutional trust antecedents
(The preconditions that shape the formation of trust)
Trust
(Users' perceptions regarding ability, benevolence, and integrity of the platform)
Trust-related behaviors
(Users' decision-making behaviors)
Mutual-Aid Healthcare Platform assurances
Mutual-Aid Healthcare Platform Trust
Mutual-Aid Healthcare Behavioral outcomes
Policy Assurance
Blockchain-enabled technology Assurance
H1
H2
Trust in the Platform
H3
Intention to Use
H4
Actual Usage Behavior
Control Variables
Demographic information: Gender; Age; Experience; Monthly income
Individual characteristics: Familiarity with blockchain-tech; Altruism; Perceived innovativeness

Figure 1. Research Model

Those who answered “Yes” were identified as target samples and were asked to complete further questions regarding their experience and responses. Those who answered “No” were excluded from the study. After that, we clearly articulated the detailed policies and blockchain-enabled technology assurance established by the Xianghubao platform to the remaining respondents. We then provided them with actual pictures/screenshots of the described assurances and asked them to evaluate their perceptions toward platform assurances. This nonintrusive, retrospective self-reported approach was intended to ensure that the respondents formed accurate perceptions about the assurance mechanisms of Xianghubao.[4] In the third section, we collected information about respondents’ individual characteristics. In the fourth section, the respondents were asked to evaluate the platform assurances (i.e., policy assurance, blockchain-enabled technology assurance), their trust in the platform, and their behavioral intentions towards the platform. We included two attention-trap questions (e.g., please select “strongly disagree” for this question) at different sections of the survey.

We received 275 total responses and screened out invalid responses based on the following criteria: (1) questionnaires with a short completion time, 2) questionnaires with straight-line answers (e.g., all 1 or all 7), (3) questionnaires with other undesired behavioral patterns (i.e., high rate of missing values), and (4) questionnaires with inaccurate answers to the attention-trap questions. In the end, we excluded 16 responses with invalid data, leaving us with 259 responses with valid data. To measure participants’ actual usage behaviors on the Xianghubao platform, we administered a second online survey to the same group of participants (i.e., 259 samples) six months later; 205 of them returned the completed questionnaires (79.2% response rate). At the beginning of data collection, we informed the participants that monetary compensation would be provided to those respondents who successfully finished the two rounds of surveys during the two periods (i.e., Time 1 and Time 2). Figure 2 describes the data collection process.

Across the two time periods, we received 205 complete and valid responses, which were used for the statistical analysis. We performed a statistical power analysis to determine the minimum sample size required to estimate the proposed model. Two methods were adopted in calculating the minimum sample size for the proposed model. We first employed the gamma-exponential method (Kock & Hadaya, 2018). Given a significant path coefficient of 0.2 and a statistical power of 0.8 (Kock & Hadaya, 2018), we obtained a minimum sample size of 155 for the study. A priori power analysis was further conducted by using the statistical software G*Power version 3.1 (Faul et al., 2009). For an effect size of 0.15, a desired statistical power level of 0.95, a construct number of 10, and a confidence level of 0.95, the required minimum sample size to estimate our model is 172. Overall, the sample size of 205 satisfied the required statistical power and significance. Table 3 describes the demographics of the overall sample, which are consistent with those of regular Xianghubao users in China.[5] As noted in Table 3, 49.8% of our respondents were men, and a majority of the respondents were between 30 and 45 years old, with a monthly income ranging from 3000 RMB to 5000 RMB. Additionally, 62.4% of the respondents had more than six months of use experience.



Preliminary Phase

A professional electronic questionnaire website (i.e., Sojump) is chosen to get in touch with individuals who have experience in Xianghubao

Time 1

The survey was posted for about one week on Sojump. We randomly recruited 275 participants to fill in the survey. We finally obtain 259 valid data.

Time 2

Six months later, we conducted a second round of survey to measure the same participants’ actual usage behaviors. We finally obtain 205 valid data.

Figure 2. Data Collection Process

[4] While we took several steps to address users’ understanding of blockchain assurance, it is possible that some respondents may not have been knowledgeable enough to answer the questions accurately. To account for this, we included the control variable of familiarity with blockchain technology, allowing respondents to self-evaluate their knowledge regarding blockchain technology during the survey. The calculation results showed an average value of 4.907 for this construct, indicating that a majority of users (74.6%) are familiar with blockchain technology, while 18% of them have some level of knowledge about the technology. The above findings further suggest that the respondents were knowledgeable enough to participate in the study.

[5] https://weibo.com/3192193027/Ii9ikaPRh?type=comment#_rnd1576740749768

Table 3. Sample Characteristics (N = 205).

Demographics	Categorization	*N*	%	Demographics	Categorization	*N*	%
Gender	Male users Female users	102 103	49.8% 50.2%	Age	Below 30 30-45 Above 45	74 87 44	36.1% 42.4% 21.5%
Monthly income	Below 3000 3000-5000 5001-8000 Above 8000	55 108 27 15	26.8% 52.7% 13.2% 7.3%	Use experience	Less than 6 months 6-12 months Above 12 months	77 103 25	37.6% 50.2% 12.2%

Regarding the actual usage behaviors, 83.4% of respondents reported accessing and utilizing the Xianghubao platform at least once per month, with 83.9% of respondents reporting utilizing only one function, namely the claim publicity service. When claims occur, the smart contract and consensus algorithms of blockchain technology automatically deduct funds from members' accounts twice per month. Consequently, users typically review and confirm shared payments monthly. This guarantees the equitable distribution of mutual aid costs among members, aligning with previous literature (Shao et al., 2022a). However, since the claim publicity service provides detailed claim records with end-to-end traceable, transparent, and tamper-proof information (e.g., the flow of claim funds) and since users generally prioritize aid information and capital flow (Shao et al., 2022a), they typically prefer utilizing the functionality of claim publicity service.

3.2 Instrument Design

Drawing on previous literature, we designed an instrument to measure the constructs. We developed the survey items in English and then translated them into a Chinese version. We employed the back-translation technique to avoid language differences (e.g., nuance and interpretation), as suggested by previous literature (Moore & Benbasat, 1991). Further, three bilingual speakers assisted in the process to confirm there were no semantic discrepancies. A pilot study was conducted with 37 participants who have experienced using the Xianghubao platform, and a few revisions were made based on the feedback from the participants and the psychometric test of the constructs. The scale development and specific instrument are illustrated in Appendix D, Appendix E, and Appendix F.

3.2.1 Independent Variables

The construct of policy assurance was measured using the scales established by Kim and Benbasat (2009). Trust was operationalized based on Bhattacherjee's (2002) study in terms of ability, benevolence, and integrity. Following the previous literature (Petter et al., 2007; Posey et al., 2014), we conceptualized blockchain-enabled technology assurance as a second-order formative construct, comprising four first-order dimensions, namely disintermediation, immutability, anonymity, and transparency (see Appendix D for detailed scale development). Moreover, we developed three items for familiarity with blockchain technology based on its definition and Gefen et al.'s (2003) study. To enhance the validity of the newly developed instrument and ensure the content validity of the construct (Moore & Benbasat, 1991), we conducted a pretest with two blockchain experts and 16 Xianghubao users. All items in our study were operationalized using a 7-point Likert scale, anchoring from 1 (strongly disagree) to 7 (strongly agree), with a neutral value of 4.

3.2.2 Dependent Variables

We referred to Bhattacherjee and Lin's (2015) study to measure the dependent variable of behavioral intention. Based on previous research, actual usage behavior is commonly measured by three dimensions: duration, frequency, and intensity (see Appendix E). In our context, duration refers to the length of time individuals have used the Xianghubao platform, frequency represents how many times individuals use the Xianghubao platform per month, and intensity describes the number of features individuals use on the Xianghubao platform. Considering that the duration of days is automatically accumulated once users join the Xianghubao platform, it cannot reflect users' voluntary behaviors (Wu & Du, 2012). Therefore, we used frequency and intensity to operationalize actual usage behaviors and asked participants about their actual usage during the last six months (Moores & Chang, 2006).

3.2.3 Control Variables

Prior studies show that gender, age, experience, and income are important factors in e-commerce (Venkatesh et al., 2012; Venkatesh & Morris, 2000). According to an official Xianghubao report,[6] 60% of actual users are born between 1980-1999. As experience increases, the attractiveness of novelty that contributes to behavioral outcomes will diminish, and users will decide whether

[6] https://weibo.com/3192193027/Ii9ikaPRh?type=comment#_rnd1576740749768

to continue using the Xianghubao platform for more pragmatic purposes, such as gaining benefits and reducing costs (Venkatesh et al., 2012). Moreover, over two thirds of participants on the Xianghubao platform earn less than RMB 8300 per month,[7] indicating that individuals with middle or low levels of disposable income are more likely to join the healthcare mutual aid platform. Thus, we controlled for gender, age, experience, and monthly income.

Furthermore, social psychologists suggest that familiarity perceptions can increase individuals' willingness to participate in emerging technologies (Gefen et al., 2003). In the case of online healthcare mutual aid platforms, users' familiarity with blockchain technology may facilitate their behavioral intentions. Second, prior research on social networks suggests that individuals are motivated to engage in activities or join a community if they enjoy helping others (Wasko & Faraj, 2005; Zhang et al., 2017). Users with higher levels of altruism may be more likely to join online healthcare mutual aid platforms (Zhang et al., 2017). Third, prior studies suggest that perceived innovativeness may enhance individuals' confidence in adopting emerging technologies (Agarwal & Karahanna, 2000). Thus, we incorporated the aforementioned three individual-level contextual factors (i.e., familiarity with blockchain technology, altruism, and perceived innovativeness) as control variables.

3.3 Analysis Strategy

We adopted partial least squares path modeling (PLS-PM) to test the proposed research model. PLS is recognized as a full-fledged variance-based structural equation modeling analysis due to its suitability for exploratory and confirmatory IS research (Benitez et al., 2020). Compared to the covariance-based approach, PLS-PM is better able to deal with models that contain both formative and reflective constructs. We employed the statistical software WarpPLS (Version 8.0) to analyze the structural model (Kock, 2022, 2023)[8]. Following a two-stage process, we first evaluated the measurement model using the confirmatory factor analysis (CFA) (Chin, 1998, 2010) and principal components analysis (PCA) (Posey et al., 2014). Specifically, we conducted CFA to assess the psychometric properties of the scales with reflective items (i.e., policy assurance, trust in the platform, actual usage behavior) and employed PCA to evaluate the formative construct (i.e., blockchain-enabled technology assurance) using the multiple indicators multiple causes (MIMIC) model (Posey et al., 2014). We then tested the research model using PLS-PM analysis.

3.3.1 Measurement Model Analysis

We used CFA techniques to evaluate the measurement properties of our reflective latent constructs. Following the criterion suggested by Benitez et al. (2020) and Kock (2022), we calculated the model fit and quality indices, including classic indices (e.g., Tenenhaus GOF, Simpson's paradox ratio, etc.) and additional indices (standardized root mean squared residual, standardized mean absolute residual, etc.). As presented in Appendix G, the model fit statistics suggest good model fit with the empirical data.

The reflective measurement model was examined in terms of construct reliability, convergent validity, and discriminant validity. We assessed the construct reliability using the indicator of composite reliability (CR). As illustrated in Appendix H, the CRs for each construct exceed the criteria value of 0.7 (Fornell & Larcker, 1981), indicating adequate construct reliability. We then assessed the convergent validity by calculating the factor loadings and average variance extracted (AVE) from each construct. The results indicate that each construct's factor loadings and AVEs are well above the threshold value. Discriminant validity was assessed based on the approach of Fornell-Larcker criterion, by comparing the square root of one factor's AVE to its correlations with each other factor (Fornell & Larcker, 1981). We also assessed discriminant validity using heterotrait-monotrait ratio (HTMT) approach by comparing the ratio of the between-trait correlations to the within-trait correlations (Henseler et al., 2015). The calculated HTMT values are all below the 0.85 threshold, thus satisfying the criteria (see Appendix I and J for details). Overall, the above analysis suggests a good discriminant validity of the measurement model (Benitez et al., 2020).

Given that internal consistency examinations of the formative construct (i.e., blockchain-enabled technology assurance) with CRs and AVEs calculations are methodologically inappropriate, we conducted the PCA to test the validity of the formative construct (Posey et al., 2014). We first computed CRs and AVEs for the first-order reflective measures (i.e., disintermediation, immutability, anonymity, and transparency) before using the PCA approach (shown in Appendix H). We then evaluated the validity of blockchain-enabled technology assurance as a second-order formative construct using the MIMIC model (Petter et al., 2007; Posey et al., 2014) based on the following measurement guidelines. The first step generated and validated items relative to blockchain-enabled technology assurance. Items/indicators for both formative and reflective components were developed according to the construct definition. Specifically, the

[7] https://antcloud-cnhz02-athomeweb-01.oss-cn-hzfinance.aliyuncs.com/attachme-nt/2020-06-13/3f900e1a-d421-49ba-a635-bb9792a0179f.pdf

[8] We utilized the factor-based PLS algorithm within the WarpPLS software, a tool that produces estimates for both true composites and factors while explicitly considering measurement error. For a detailed discussion of the algorithm, please refer to Kock (2023).

formative indicators of blockchain-enabled technology assurance were measured by averaging the indicator scores of the first-order constructs (i.e., disintermediation, immutability, anonymity, and transparency). Based on Posey et al. (2014), we incorporated reflective indicators at the higher construct level to address statistical constraints encountered with formative constructs. This addition allowed more unique pieces of information (i.e., nonredundant entries in the sample covariance matrix) to be produced and examined the formative construct by itself in a measurement model. Thus, we measured a reflective blockchain-based technology assurance construct using three reflective items, as shown in Appendix F. The second step assessed the MIMIC model's internal validity by examining the relative contributions (i.e., beta weights) of the first-order formative indicators to the reflective construct of blockchain-enabled technology assurance. As shown in Appendix K, all path weights between the first-order formative indicators and blockchain-enabled technology assurance are significant. The third step tested multicollinearity among the first-order formative indicators. The variance inflation factor (VIF)[9] value for each first-order indicator is far below the threshold of 3.3, indicating that multicollinearity did not present a serious issue for our study (Petter et al., 2007; Posey et al., 2014). Overall, the results suggest that the formative indicators provided good coverage of blockchain-enabled technology assurance. Therefore, we operationalized the construct of blockchain-enabled technology assurance as formative by using the standardized latent variable scores (LVS) of the first-order constructs (Benitez et al., 2020).

3.3.2 Results of Hypotheses Testing

We used PLS-PM to analyze the proposed model and hypotheses and generated the path coefficients and statistical significance of the path relationships. The explanatory power of the structural model was assessed by calculating the amount of variance (R^2) explained in the endogenous variable. As illustrated in Figure 3, our theoretical model explicates 70.8% variance in trust, 36.2% variance in intention to use, 19.1% variance in frequency of usage, and 25.8% variance in intensity of usage, respectively, demonstrating a good explanatory power of the model. This study also calculated the value of f^2 to quantify the significant effects of the exogenous latent variables (Benitez et al., 2020). The findings indicate that the impact of policy assurance on trust in the platform, as measured by the f^2 value, is substantial at 0.50, representing a large effect, while the f^2 value for the influence of blockchain-enabled technology assurance on trust in the platform is 0.13, reflecting a medium effect. Moreover, the relationship between trust in the platform and behavioral intention is characterized by a medium effect, with an f^2 value of 0.17. Furthermore, the f^2 values for the influences of behavioral intention on the frequency and intensity of usage are 0.19 and 0.26, respectively, signifying medium effects. We also compared the results of three alternative models. As noted in Appendix L, our proposed model explains more variance in endogenous variables than other models, further demonstrating the validity of our research model.

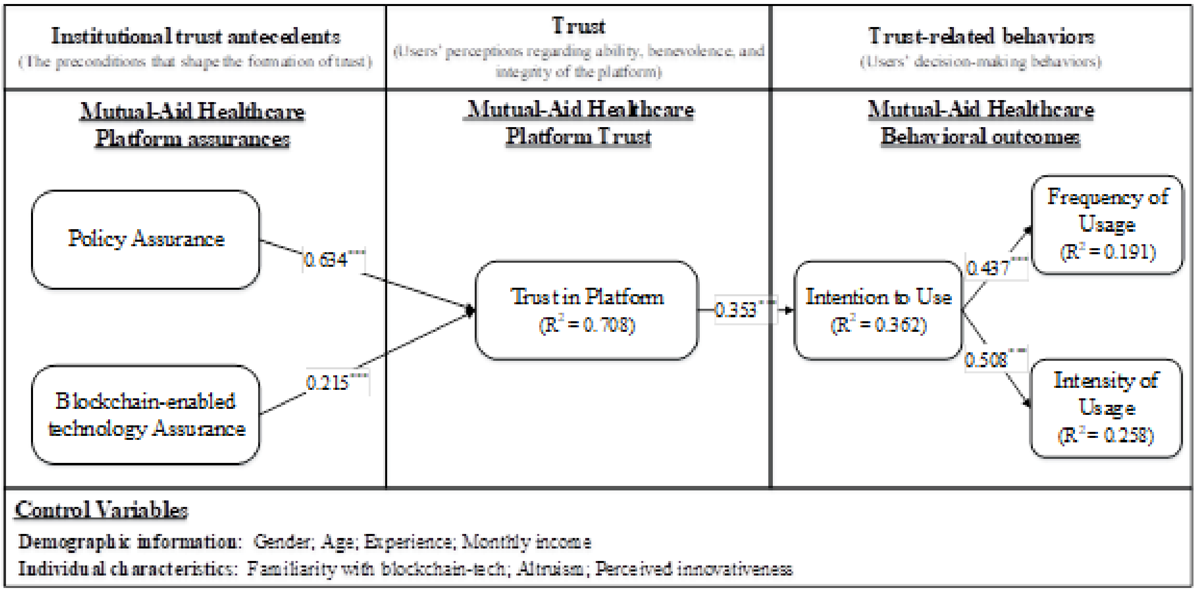

Institutional trust antecedents
(The preconditions that shape the formation of trust)
Trust
(Users' perceptions regarding ability, benevolence, and integrity of the platform)
Trust-related behaviors
(Users' decision-making behaviors)
Mutual-Aid Healthcare Platform assurances
Mutual-Aid Healthcare Platform Trust
Mutual-Aid Healthcare Behavioral outcomes
Policy Assurance
Blockchain-enabled technology Assurance
0.634***
0.215***
Trust in Platform (R² = 0.708)
0.353***
Intention to Use (R² = 0.362)
0.437***
0.508***
Frequency of Usage (R² = 0.191)
Intensity of Usage (R² = 0.258)
Control Variables
Demographic information: Gender; Age; Experience; Monthly income
Individual characteristics: Familiarity with blockchain-tech; Altruism; Perceived innovativeness

Figure 3. Structural Model Evaluation

[9] Following the guidelines of Benitez et al. (2020), collinearity among indicators of the formative variable should be investigated by means of the variance inflation factor (VIF), as high multicollinearity can lead to insignificant estimates and unexpected signs of the weights. Traditionally, VIF values above 3.3 are regarded as indications of problematic multicollinearity.

Figure 3 provides the results of our hypothesized path relationships. We note that policy assurance (β = 0.634, p < 0.001) and blockchain-enabled technology assurance (β = 0.215, p < 0.001) are positively associated with trust in the platform. Thus, both H1 and H2 are supported. As the results from Figure 3 show, trust is positively associated with intention to use (β = 0.353, p < 0.001); thus, H3 is supported. Additionally, intention to use is positively associated with the two dimensions of actual usage behaviors, i.e., frequency of usage (β = 0.437, p < 0.001) and intensity of usage (β = 0.508, p < 0.001); thus, H4 is supported. Regarding the control variables, experience exerted a significant influence on intention to use (β = 0.308, p < 0.001), indicating that users with more experience towards the Xianghubao platform are more likely to use the platform. Perceived innovativeness positively influenced intention to use (β = 0.146, p < 0.05), suggesting that users with higher perceived innovativeness are more likely to participate in blockchain-enabled mutual aid services.

3.3.3 Mediation Test Results

We followed Kock (2014) to test the mediation effects using the statistical software WarpPLS (version 8.0). This study established direct links between the two structural assurances (independent variables, IV) and intention to use and actual usage behaviors (dependent variables, DV), respectively, and retested the structural model to examine the mediation effect of trust (mediator variable, M). Following Kock's (2014) criteria, a mediating effect is considered significant when an indirect relationship (IV → M → DV) exists at the 5% significance level. Additionally, a partial effect is supported if IV significantly impacts DV directly, while a full mediation is supported if the direct relationship between IV and DV is not significant. As noted in Appendix O, the results suggest that the indirect effects of policy and blockchain-enabled technology assurance on intention to use are significantly mediated by trust, while their direct effects on intention are nonsignificant. Therefore, our findings indicate that trust fully mediates the influences of policy and blockchain-enabled technology assurances on intention to use. Furthermore, the results show that the indirect effect of policy and blockchain-enabled technology assurances on actual usage behaviors are fully mediated by trust and intention to use, while their direct effects on actual usage behaviors are nonsignificant. Additionally, the empirical results show that f^2 values for the indirect influences of assurance mechanisms range from 0.005 to 0.077, indicating no effect to a small effect (see details in Appendix O). These results imply that while assurance mechanisms contribute to outcomes through mediators, the mediation effects are relatively modest and have limited practical application (Benitez et al., 2020).

3.3.4 Common Method Biases Analysis and Endogeneity Test

We conducted robustness checks to address potential common method bias (CMB) and endogeneity issues (Sarstedt et al., 2020). As most of our data was self-reported by the respondents, there was a potential for CMB resulting from the consistency motif, social desirability, and common scale formats (Podsakoff et al., 2003). Therefore, we performed several remedies to reduce the potential for CMB (James et al., 2019).[10] However, the results may nevertheless be vulnerable to response bias if respondents used a consistent response pattern instead of assessing questions on their merits. We thus conducted multiple tests to test the for CMB, including the Harman one-factor test, the marker variable technique, and the full collinearity variance inflation factors (FCVIFs) method (Kock & Lynn, 2012; Podsakoff et al., 2003; Williams et al., 2010). As described in Appendix M, all criteria were satisfied, indicating CMB did not present a serious concern for our study.

We further conducted procedural precautions to reduce the potential issue of endogeneity (Benitez et al., 2016, 2018; Venkatesh et al., 2020). First, we collected data in two periods (i.e., Time 1 and Time 2), which could help reduce the endogeneity issue (Venkatesh et al., 2020). Second, we employed the Gaussian copulas method (Hult et al., 2018) and introduced instrumental variables (Kock, 2022; Kock & Sexton, 2017) to address the endogeneity of IVs (i.e., two structural assurances). As reported in Appendix N, the results of the two approaches do not suggest any endogeneity threats. Overall, the above analysis supports the robustness of our structural model results (Hult et al., 2018).

[10] First, we reminded participants that their anonymity was assured and that the collected data would only be used for academic research. Second, we asked "attention trap" questions at multiple points in the survey by asking participants to select a particular response from the Likert-scale items. For example, participants were asked to select "Strongly Agree" as the answer to a specific question. We excluded participants who did not select the right answer and discarded their responses since this indicated that they were not cognitively engaged in the survey.

4 Implications and Conclusions

4.1 Theoretical Implications for IS Research

4.1.1 Reconceptualization of Assurance Mechanisms towards IS Usage

This study is one of the first to conceptualize and measure policy assurance and technology assurance separately in the IS usage context. Prior literature has mostly considered structural assurance as a first-order construct that concentrates on statements, arguments, or seals (Bansal et al., 2015; Dimoka et al., 2012; Kim et al., 2009; Kim & Benbasat, 2009; Özpolat et al., 2013; Park et al., 2010) while ignoring the significant role of technology assurance enabled by emerging digital technologies. To the best of our knowledge, this study is among the first to juxtapose policy and technology assurances to delineate their conceptual disparities and distinct roles. While policy assurance is indeed indispensable, it typically intervenes after IS noncompliance or policy violations have arisen. In contrast, technology assurance provides proactive prevention, allowing problems to be averted before they manifest. Researchers have argued for the efficacy of digital technologies in detecting and thwarting attacks, identifying fake websites, and preemptively detecting intrusions (Dhillon et al., 2021; Tee & Murugesan, 2018; Wang & Kogan, 2018). Our research findings are consistent with such observations, underscoring that the continual progress of digital technologies allows for the timely detection of potential noncompliant usage behaviors within IS, thereby facilitating the implementation of corresponding measures for prevention and correction. Therefore, our study enriches the conceptualization and measurement of structural assurance by dividing it into two separate dimensions (i.e., policy assurance and technology assurance), which are pivotal for a comprehensive understanding of impersonal assurance mechanisms in bolstering secure IS usage.

4.1.2 Contextualization of Trust-Building Precursors in the Blockchain Technology Context

Our study contributes to the "institutional trust" literature by explicating how contextualized assurance mechanisms build institutional-based trust in a blockchain-enabled mutual aid healthcare context. Although prior IS studies have conceptualized structural assurance and explored its impact on trust (Gefen et al., 2003; McKnight et al., 2002b, 2004; Pavlou & Gefen, 2004, 2005; Shao et al., 2019), our understanding regarding the influences of different assurance dimensions is still limited, especially in the emerging context of blockchain technology applications. The research findings presented here extend the previous IS literature by uncovering the distinguished influence mechanisms of policy assurance and blockchain-enabled technology assurance on institutional trust regarding magnitude and significance. Furthermore, in contrast to previous studies (e.g., Shao et al., 2022), this study develops a multidimensional measurement scheme of blockchain-enabled technology assurance as a second-order formative construct, which enables a comprehensive modeling of contextualized technology assurance through four potentially disparate dimensions of blockchain technology, including anonymity, immutability, transparency, and disintermediation (Cenfetelli & Bassellier, 2009). The research findings enrich the "institutional trust" literature and deepen our understanding regarding the role of different assurance mechanisms on trust in the blockchain-enabled mutual aid healthcare context. Future research is expected to uncover the trust-building mechanism that drives the adoption of blockchain technology.

4.1.3 Elaboration of Trust-Related Behaviors in Blockchain-Enabled Healthcare Platforms

Our established research model employs a longitudinal field study to illuminate the trajectory of assurance mechanisms, trust, behavioral intentions, and their subsequent impact on actual usage behaviors on blockchain-enabled mutual aid healthcare platforms (Veiga et al., 2014; Venkatesh & Davis, 2000). Previous studies have mostly focused on initial trust formation in blockchain-enabled applications (Ostern, 2018; Shao et al., 2022), which often emerges amid a dearth of credible and substantial information, rendering it inherently fragile, as users must often rely on limited knowledge or hearsay (McKnight et al., 1998). In contrast, our research focuses on the experiential trust of actively engaged users who have already gained practical experience with platform assurances. Our research findings align with the view of institutional trust (Colquitt & Rodell, 2011; Fang et al., 2014), emphasizing the significance of experiential trust derived from institutional structures in promoting users' willingness to engage in the prolonged usage of online healthcare mutual aid platforms. Our longitudinal field study also extends the previous IS literature by capturing the dynamics of users' evolving decision-making processes on blockchain-enabled mutual aid healthcare platforms. We encourage future studies to leverage longitudinal data to provide a comprehensive understanding of the user's journey on online healthcare mutual aid platforms in order to shed light on the transition from experiential trust to tangible action.

4.2 Practical Implications

Regarding practical implications, this study provides management guidelines for both platform administrators and healthcare organizations. Administrators need to recognize that both policy assurance and technology assurance are important in stimulating users' active participation in online healthcare mutual aid platforms. On the one hand, administrators need to establish clear institutional statements, strict auditing rules, and prompt feedback policies for each healthcare mutual aid case to protect the benefits of both donors and recipients during the mutual aid process. On the other hand, administrators also need to implement emerging blockchain technologies to ensure the immutability, anonymity, transparency, and disintermediation of the mutual aid process. Specifically, in contrast to traditional static assurance statements, administrators should offer users the opportunity to frequently engage with both policy and technology assurances for each mutual aid claim. For instance, in the context of Xianghubao, users can actively participate in the approval process in cases of disputed mutual aid claims, thereby reinforcing their evaluation of policy guarantees. Users can also access tamper-resistant claim information and observe the flow of mutual aid funds through a secure blockchain certificate within each claim occurrence. These experiences enable users to develop a comprehensive understanding of the distinctive policy assurance and blockchain-enabled technology assurance over time, which can significantly enhance users' trust in the online healthcare mutual aid platform. Thus, administrators should enact effective legal policies and implement advanced technological structures to guarantee the credibility of the online healthcare platform and safeguard users from unexpected accidents. Notably, administrators need to pay attention to diverse platform assurances (i.e., policy assurance plus blockchain-enabled technology assurance) to encourage the adoption and sustained usage of emerging blockchain-enabled online healthcare platforms.

The popularity of Xianghubao also suggests guidelines for regulators of online healthcare organizations and other P2P micro-insurance schemes. Institutional support is a key factor for platform development. Given the crucial role of institutional regulations in signifying the rationality of online healthcare mutual aid platforms, it is essential for regulators to establish clear policies for their long-term continuous development. Specifically, regulators of online healthcare organizations could provide official support to online healthcare mutual aid platforms and encourage greater participation from the public to foster the success of online healthcare mutual aid services.

4.3 Limitations and Future Research Directions

This study has several limitations that suggest avenues for future research. First, our study focused on Xianghubao as one representative blockchain-enabled healthcare platform in China. A follow-up study could extend our sample size to a diversity of users on other healthcare platforms. For example, future studies could extend our samples to users of different blockchain-enabled platforms to further examine the external validity and generalizability of our research findings.

Second, our study used the survey method to test the research model. Although we found that common method bias did not persent a serious issue for our study, future studies might consider applying qualitative methodologies (e.g., content analysis) to explore the most important mechanisms of structural assurances on online healthcare mutual aid platforms. We also strongly encourage future studies to categorize actual usage behaviors into specific dimensions (i.e., frequency and intensity) and measure them using both objective and subjective methods.

Third, this study examines the concept of technology assurance within the specific context of blockchain-enabled technology. However, it is important to note that technology assurance holds the potential for broader applications. Future studies are encouraged to use the multidimensional measurement scheme to explore and operationalize technology assurance in other technological domains. For instance, in the context of cloud computing or internet of things (IoT), the specific operationalizations of these dimensions may vary based on the unique characteristics of the respective technologies. Therefore, future research could identify and measure technology assurance as a multidimensional construct, extending its theoretical implications and enhancing its potential value in other emerging contexts.

Fourth, our study focuses on the influences of structural assurances on behavioral intentions and actual usage behaviors without considering other possible factors. Future studies could draw upon other theoretical perspectives (e.g., the lens of technology affordance or justice theory) to investigate users' behaviors in blockchain-enabled online healthcare mutual aid platforms. Moreover, our study adds individual characteristics as control variables to rule out other potential influences on the research model. Future studies could also consider incorporating additional important variables (e.g., ease of use or perceived usefulness) to contribute to a more comprehensive understanding of our research model. We encourage future studies to delve into the boundary conditions of our research model by incorporating relevant moderators, specifically by examining if the two structural assurances exhibit different influences on trust and behavioral intention under different conditions. It would be interesting to investigate if users with more experience have received or contributed to more payments on the blockchain and if the results differ across men and women. Additionally, if users experience health issues after joining the Xianghubao platform, their medical needs may influence actual usage behaviors. Further studies are encouraged to explore these factors.

Fifth, this study includes policy assurance and technology assurance as major trust-building antecedents in the research model. Future studies could examine other salient antecedents of trust (e.g., familiarity with platform). Future studies could also incorporate other trust targets (e.g., trust in the members) in the research model to examine the nomological network relationships among multiple trust targets.

4.4 Conclusion

This study extends the extant literature (Kamble et al., 2020; Queiroz & Wamba, 2019; Wong et al., 2020) by adopting a longitudinal field study and collecting data in two periods to assess users' behavioral intention and actual usage behaviors in the emerging context of blockchain technology. Based on a comprehensive review of the blockchain literature and theoretical discussion of structural assurances, we present a theoretical framework and introduce the concept of blockchain-enabled technology assurance into the realm of online healthcare mutual aid services. Through an exploration of the distinctions between policy assurance and blockchain-enabled technology assurance, we conceptualize the essence of blockchain-enabled technology assurance by separating it into four dimensions—disintermediation, immutability, anonymity, and transparency. This study also draws insights from institutional trust theory and formulates a comprehensive research model to uncover the mediating effect of trust between structural assurances and behavioral outcomes. Our research findings show that policy and blockchain-enabled technology assurances are important cornerstones for users to build trust in online healthcare mutual aid platforms. Overall, the findings provide a comprehensive understanding of the significant role of blockchain in building users' trust relationships and driving their behaviors in the digital landscape in terms of commercial applications, online markets, and economies.

Acknowledgments

We gratefully acknowledge the research sponsorship received from the National Natural Science Foundation of China (72271069), the Ministry of Education of Humanities and Social Science Project (22YJA630070), the Philosophy and Social Sciences of Heilongjiang Province (22GLB107), the Fundamental Research Funds for the Central Universities (D5000240050), the Government of Spain, and the European Regional Development Fund (European Union) (Research Projects PID2021-124725NB-I00, PID2021-124396NB-I00, and TED2021-130104B-I00).

References

Abdikerimova, S., & Feng, R. (2022). Peer-to-peer multi-risk insurance and mutual aid. *European Journal of Operational Research*, *299*(2), 735-749.

Agarwal, R., Gao, G., DesRoches, C., & Jha, A. K. (2010). Research commentary-the digital transformation of healthcare: Current status and the road ahead. *Information Systems Research*, *22*(4), 419-428.

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly*, *24*(4), 665-694.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Andersen, J. V., & Bogusz, C. I. (2019). Self-organizing in blockchain infrastructures: Generativity through shifting objectives and forking. *Journal of the Association for Information Systems*, *20*(9), 11.

Avgerou, C. (2013). Explaining trust in IT-mediated elections: A case study of e-voting in Brazil. *Journal of the Association for Information Systems*, *14*(8), 2.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138-150.

Bansal, G., Zahedi, F., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*(6), 624-644.

Benbasat, I., Gefen, D., & Pavlou, P. A. (2008). Trust in online environments. *Journal of Management Information Systems*, *24*(4), 5-11.

Benitez, J., Henseler, J., Castillo, A., & Schuberth, F. (2020). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. *Information & Management*, *57*(2), Article 103168.

Benitez, J., Henseler, J., & Roldán Salgueiro, J. L. (2016). How to address endogeneity in partial least squares path modeling. *Proceedings of the 22nd Americas Conference on Information Systems*.

Benitez, J., Ray, G., & Henseler, J. (2018). Impact of information technology infrastructure flexibility on mergers and acquisitions. *MIS Quarterly*, *42*(1), 25-43.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems*, *19*(1), 211-241.

Bhattacherjee, A., & Lin, C.-P. (2015). A unified model of IT continuance: Three complementary perspectives and crossover effects. *European Journal of Information Systems*, *24*(4), 364-373.

Carvalho, A. (2021). Bringing transparency and trustworthiness to loot boxes with blockchain and smart contracts. *Decision Support Systems*, *144*, Article 113508.

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly*, 33(4), 689-707.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, *295*(2), 295-336.

Chin, W. W. (2010). How to write up and report PLS analyses. In V. Esposito Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of partial least squares* (pp. 655-690). Springer.

Colquitt, J. A., & Rodell, J. B. (2011). Justice, trust, and trustworthiness: A longitudinal analysis integrating three theoretical perspectives. *Academy of Management Journal*, *54*(6), 1183-1206.

Devaraj, S., Easley, R. F., & Crant, J. M. (2008). Research note—How does personality matter? Relating the five-factor model to technology acceptance and use. *Information Systems Research*, *19*(1), 93-105.

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems*, *30*(4), Article 101693.

Dimoka, A., Hong, Y., & Pavlou, P. A. (2012). On product uncertainty in online markets: Theory and evidence. *MIS Quarterly*, *36*(2), 395-426.

Fang, Y., Qureshi, I., Sun, H., McCole, P., Ramsey, E., & Lim, K. H. (2014). Trust, satisfaction, and online repurchase intention. *MIS Quarterly*, *38*(2), 407-A9.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149-1160.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.

Gefen, D., Benbasat, I., & Pavlou, P. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems*, *24*(4), 275-286.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51-90.

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

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135.

Hughes, J. N., Luo, W., Kwok, O.-M., & Loyd, L. K. (2008). Teacher-student support, effortful engagement, and achievement: A 3-year longitudinal study. *Journal of Educational Psychology*, *100*(1), 1-14.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114-129.

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, *31*(1), 19-33.

Hult, G. T. M., Hair Jr, J. F., Proksch, D., Sarstedt, M., Pinkwart, A., & Ringle, C. M. (2018). Addressing endogeneity in international marketing applications of partial least squares structural equation modeling. *Journal of International Marketing*, *26*(3), 1-21.

ISSA. (2022). *Detecting fraud in health care through emerging technologies*. International Social Security Association. https://ww1.issa.int/analysis/detecting-fraud-health-care-through-emerging-technologies

James, T. L., Wallace, L., & Deane, J. K. (2019). Using organismic integration theory to explore the associations between users' exercise motivations and fitness technology feature set use. *MIS Quarterly*, *43*(1), 287-312.

Jha, A. K., & Shah, S. (2021). Disconfirmation effect on online review credibility: An experimental analysis. *Decision Support Systems*, *145*, Article 113519.

Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. *International Journal of Information Management*, *52*, Article 101967.

Kim, & Benbasat, I. (2009). Trust-assuring arguments in B2C e-commerce: Impact of content, source, and price on trust. *Journal of Management Information Systems*, *26*(3), 175-206.

Kim, D., Yim, M.-S., Sugumaran, V., & Rao, H. R. (2016). Web assurance seal services, trust and consumers' concerns: an investigation of e-commerce transaction intentions across two nations. *European Journal of Information Systems*, *25*(3), 252-273.

Kim, Shin, B., & Lee, H. G. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal*, *19*(3), 283-311.

Kock, N. (2014). Advanced mediating effects tests, multi-group analyses, and measurement model assessments in PLS-based SEM. *International Journal of E-Collaboration*, *10*(1), 1-13.

Kock, N. (2022). *WarpPLS user manual: Version 8.0.* ScriptWarp Systems.

Kock, N. (2023). Contributing to the Success of PLS in SEM: An Action Research Perspective. *Communications of the Association for Information Systems*, *52*(1), 730-734.

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, *28*(1), 227-261.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems*, *13*(7), 546-580.

Kock, N., & Sexton, S. (2017). Variation sharing: a novel numeric solution to the path bias underestimation problem of PLS-based SEM. *International Journal of Strategic Decision Sciences*, *8*(4), 46-68.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, *17*(1), 39-71.

Liang, T.-P., Kohli, R., Huang, H.-C., & Li, Z.-L. (2021). What Drives the Adoption of the Blockchain Technology? A Fit-Viability Perspective. *Journal of Management Information Systems*, *38*(2), 314-337.

Lim, K. H., Sia, C. L., Lee, M. K. O., & Benbasat, I. (2006). Do I trust you online, and if so, will I buy? An empirical study of two trust-building strategies. *Journal of Management Information Systems*, *23*(2), 233-266.

Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*, *4*(1), 65-97.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114-121.

Liu, Y., & Liu, Y. (2019). The effect of workers' justice perception on continuance participation intention in the crowdsourcing market. *Internet Research*, *29*(6), 1485-1508.

Lu, B., Zhang, T., Wang, L., & Keller, L. R. (2016). Trust antecedents, trust and online microsourcing adoption: An empirical study from the resource perspective. *Decision Support Systems*, *85*, 104-114.

Mai, B., Menon, N. M., & Sarkar, S. (2010). No free lunch: Price premium for privacy seal-bearing vendors. *Journal of Management Information Systems*, *27*(2), 189-212.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002a). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002b). 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., Kacmar, C. J., & Choudhury, V. (2004). Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A two-stage model of initial trust in a web business. *Electronic Markets*, *14*(3), 252-266.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192-222.

Moores, T. T., & Chang, J. C.-J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly*, *30*(1), 167-180.

Mou, J., & Cohen, J. F. (2015). Antecedents of trust in electronic-service providers: results from a meta-analysis. *Pacific Asia Journal of the Association for Information Systems*, *7*(1), 1-30.

Nicolaou, A. I., & McKnight, D. H. (2011). System design features and repeated use of electronic data exchanges. *Journal of Management Information Systems*, *28*(2), 269-304.

Ostern, N. (2018). Do you trust a trust-free transaction? Toward a trust framework model for blockchain technology. *Proceedings of the 38th International Conference on Information Systems*.

Özpolat, K., Gao, G., Jank, W., & Viswanathan, S. (2013). Research note—The value of third-party assurance seals in online retailing: An empirical investigation. *Information Systems Research*, *24*(4), 1100-1111.

Park, I., Bhatnagar, A., & Rao, H. R. (2010). Assurance seals, on-line customer satisfaction, and repurchase intention. *International Journal of Electronic Commerce*, *14*(3), 11-34.

Park, S., & Gupta, S. (2012). Handling endogenous regressors by joint estimation using copulas. *Marketing Science*, *31*(4), 567-586.

Pavlou, P. A. (2002). Institution-based trust in interorganizational exchange relationships: the role of online B2B marketplaces on trust formation. *The Journal of Strategic Information Systems*, *11*(3-4), 215-243.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, *35*(4), 977-988.

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

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, *30*(1), 115-143.

Pavlou, P. A., & Gefen, D. (2005). Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role. *Information Systems Research*, *16*(4), 372-399.

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *31*(4), 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879-903.

Posey, C., Roberts, T., Lowry, P. B., & Bennett, B. (2014). Multiple indicators and multiple causes (MIMIC) models as a mixed-modelling technique: A tutorial and an annotated example. *Communications of the Association for Information Systems*, *36*, 179-204.

Queiroz, M. M., & 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.

Rossi, M., Mueller, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems*, *20*(9), 1390-1405.

Saha, P., Bose, I., & Mahanti, A. (2016). A knowledge based scheme for risk assessment in loan processing by banks. *Decision Support Systems*, *84*, 78-88.

Sarker, S., Henningsson, S., Jensen, T., & Hedman, J. (2021). The use of blockchain as a resource for combating corruption in global shipping: An interpretive case study. *Journal of Management Information Systems*, *38*(2), 338-373.

Sarstedt, M., Ringle, C. M., Cheah, J.-H., Ting, H., Moisescu, O. I., & Radomir, L. (2020). Structural model robustness checks in PLS-SEM. *Tourism Economics*, *26*(4), 531-554.

Shao, Z., & Yin, H. (2019a). Building customers' trust in the ridesharing platform with institutional mechanisms: An empirical study in China. *Internet Research*, *29*(5), 1040-1063.

Shao, Z., & Yin, H. (2019b). Building customers' trust in the ridesharing platform with institutional mechanisms. *Internet Research*, *29*(5), 1040-1063.

Shao, Z., Zhang, L., Brown, S. A., & Zhao, T. (2022a). Understanding users' trust transfer mechanism in a blockchain-enabled platform: A mixed methods study. *Decision Support Systems*, *155*, Article 113716.

Shao, Z., Zhang, L., Li, X., & Guo, Y. (2019). Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. *Electronic Commerce Research and Applications*, *33,* Article 100823.

Shao, Z., Zhang, L., Li, X., & Zhang, R. (2022b). Understanding the role of justice perceptions in promoting trust and behavioral intention towards ride-sharing. *Electronic Commerce Research and Applications*, *51*, Article 101119.

Sia, C. L., Lim, K. H., Leung, K., Lee, M. K. O., Huang, W. W., & Benbasat, I. (2009). Web strategies to promote internet shopping: is cultural-customization needed? *MIS Quarterly*, *33*(3), 491-512.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015.

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.

Szajna, B. (1996). Empirical evaluation of the revised technology acceptance model. *Management Science*, *42*(1), 85-92.

Tee, W. J., & Murugesan, R. K. (2018). Trust network, blockchain and evolution in social media to build trust and prevent fake news. *Proceedings of the 4th International Conference on Advances in Computing, Communication & Automation*.

Tennyson, S., & Salsas-Forn, P. (2002). Claims auditing in automobile insurance: fraud detection and deterrence objectives. *Journal of Risk and Insurance*, *69*(3), 289-308.

Turel, O., Yuan, Y., & Connelly, C. E. (2008). In justice we trust: predicting user acceptance of e-customer services. *Journal of Management Information Systems*, *24*(4), 123-151.

Underwood, S. (2016). Blockchain beyond Bitcoin. *Communications of the ACM*, *59*(11), 15-17.

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management*, *54,* Article 102120.

Veiga, J. F., Keupp, M. M., Floyd, S. W., & Kellermanns, F. W. (2014). The longitudinal impact of enterprise system users' pre-adoption expectations and organizational support on post-adoption proficient usage. *European Journal of Information Systems*, *23*, 691-707.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186-204.

Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, *24*(1), 115-139.

Venkatesh, V., Thong, J. Y. L., Chan, F. K. Y., Hoehle, H., & Spohrer, K. (2020). How agile software development methods reduce work exhaustion: Insights on role perceptions and organizational skills. *Information Systems Journal*, *30*(4), 733-761.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157-178.

Veiga, J. F., Keupp, M. M., Floyd, S. W., & Kellermanns, F. W. (2014). The longitudinal impact of enterprise system users' pre-adoption expectations and organizational support on post-adoption proficient usage. *European Journal of Information Systems*, *23*, 691-707.

Venkatesh, V., Speier, C., & Morris, M. G. (2002). User acceptance enablers in individual decision making about technology: Toward an integrated model. *Decision Sciences*, *33*(2), 297-316.

Viaene, S., Derrig, R. A., Baesens, B., & Dedene, G. (2002). A comparison of state-of-the-art classification techniques for expert automobile insurance claim fraud detection. *Journal of Risk and Insurance*, *69*(3), 373-421.

Wang, W., & Benbasat, I. (2008). Attributions of trust in decision support technologies: A study of recommendation agents for e-commerce. *Journal of Management Information Systems*, 24(4), 249-273.

Wang, L., Luo, X. R., & Lee, F. (2019). Unveiling the interplay between blockchain and loyalty program participation: A qualitative approach based on Bubichain. *International Journal of Information Management*, *49*, 397-410.

Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, *30*, 1-18.

Wasko, M. M., & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, *29*(1), 35-57.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, *57*, 47-66.

Williams, L. J., Hartman, N., & Cavazotte, F. (2010). Method variance and marker variables: A review and comprehensive CFA marker technique. *Organizational Research Methods*, *13*(3), 477-514.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45-55.

Wong, L.-W., Leong, L.-Y., Hew, J.-J., Tan, G. W.-H., & Ooi, K.-B. (2020). Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among Malaysian SMEs. *International Journal of Information Management*, *52*, 101997.

Wu, J., & Du, H. (2012). Toward a better understanding of behavioral intention and system usage constructs. *European Journal of Information Systems*, *21*(6), 680-698.

Wu, J., & Holsapple, C. (2014). Imaginal and emotional experiences in pleasure-oriented IT usage: A hedonic consumption perspective. *Information & Management*, *51*(1), 80-92.

Zhang, X., Guo, X., Ho, S. Y., Lai, K., & Vogel, D. (2021). Effects of emotional attachment on mobile health-monitoring service usage: An affect transfer perspective. *Information & Management*, *58*(2), Article 103312.

Zhang, X., Liu, S., Deng, Z., & Chen, X. (2017). Knowledge sharing motivations in online health communities: A comparative study of health professionals and normal users. *Computers in Human Behavior*, *75*, 797-810.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840-1920. *Research in Organizational Behavior*, *8*, 53-111.

Appendix A: Examples of Fraudulent Incidents in Online Healthcare Mutual Aid Platforms

Considering that specific references or statistics regarding the amount of mutual aid claim fraud in China are unavailable, we thoroughly searched reliable news websites and government reports to gather relevant information on this topic. These sources offer potential insights into the situation pertaining to fraudulent activities and accessible data within the realm of mutual aid platforms in China.

Table A1. Mutual Aid Claims Fraud Examples

	The description of fraud events	**Consequences**
People’s Daily https://www.chinanews.com.cn/m/gn/2016/09-08/7997616.shtml	• A leukemia-stricken girl appealed for help on the online healthcare mutual aid platform to raise the required **400,000 yuan (around 61,538 US dollars)** for treatment. Later, it was discovered that life-saving funds had disappeared.	A majority of users complained about the inadequate structural mechanisms for the use of donations on the online healthcare mutual aid platform.
	• A girl orchestrated a scheme by concocting inspirational articles and portraying a story of a financially struggling female college student with a long-term illness. Through this act, she deceived kind-hearted individuals into donating over **150,000 yuan (around 23,300 US dollars)** from the online healthcare mutual aid platform. • A boy falsely claimed that his father had died in the explosion that occurred in Tianjin. Utilizing the online healthcare mutual aid platform, he managed to acquire nearly **100,000 yuan (around 15,500 US dollars)**.	Impacted by similar negative news, 46.3% of users had doubts about the authenticity and security of online healthcare mutual aid platforms. Additionally, 10.2% of them believed that frequent “donation fraud scandals” exhaust public sympathy, resulting in a lack of trust in platforms.
	• A Chinese student studying in Germany raised **5 million yuan (around 780,000 US dollars)** through the online healthcare mutual aid platform for leukemia treatment but was questioned about whether they had already benefited from medical insurance.	These types of events have led users to strongly question whether online healthcare mutual aid platforms can provide fair and impartial mutual aid evaluation services and whether the collection, recording, and decision-making of publicly funded mutual aid claims can be conducted objectively and fairly.
Xinhua net http://www.xinhuanet.com/politics/2017-12/03/c_1122048905.htm	• A young man‘s mother was diagnosed with breast cancer, requiring a self-funded medical expense of 6,800 yuan. However, he managed to raise **300,000 yuan (around $46,837 US dollars)** through the online healthcare mutual aid platform for his mother, which greatly exceeded the actual cost of treatment.	A majority of users have expressed concerns about the limited capacity of online healthcare mutual aid platforms to thoroughly verify mutual aid claims prior to their release or effectively prevent the spread of false information. This has resulted in a significant crisis of trust among donors.
Workercn https://www.workercn.cn/32843/201911/08/191108022131148.shtml	• A man initiated a fundraising campaign on an online healthcare mutual aid platform for his seriously ill son, raising a total amount of **153,136 yuan (around 23,812 US dollars)** with contributions from **over 6,000 individuals**. However, he violated the agreement and misappropriated the raised funds for personal use.	Due to the opacity and uncertainty surrounding the utilization and flow of funds raised on online healthcare mutual aid platforms, such platforms risk being labeled as illegal fundraising or misappropriation, undermining public in such crowdfunding platforms.
Xinhua News http://m.xinhuanet.com/2019-12/11/c_1125336153.htm	• Xinhua News revealed various issues associated with an online healthcare mutual aid platform, including staff members encouraging patients to conceal information for fundraising purposes, receiving commissions based on the amount raised, and utilizing preexisting templates to garner public sympathy. For example, as of 2019, one health mutual aid platform had cumulatively raised over **25.5 billion yuan (around 3.96 billion US dollars)**. However, the management	These concerns have garnered significant public attention. During investigations, people complained about issues with certain online healthcare mutual aid platforms, such as inadequate online verification of claim information, evasion of legal responsibilities, and lack of transparency in the management and utilization of funds.

	and utilization of these funds remained completely opaque, and the platform refused to disclose any relevant information.	
Nhnews http://nh.cnnb.com.cn/system/2019/05/31/011996116.shtml	• A renowned actor was hospitalized for a sudden cerebral hemorrhage, and his family initiated a crowdfunding campaign on the online healthcare mutual aid platform with a target amount of **1 million yuan (about 154,000 US dollars)**. Surprisingly, despite owning property and a vehicle in Beijing, the actor raised funds by presenting as a "poor household."	This incident sparked a strong social response, leading to public concerns regarding the fairness of online healthcare mutual aid platforms in making decisions.
People.cn http://opinion.people.com.cn/n1/2019/1205/c1003-31490692.html	• An online healthcare mutual aid platform enacted intentional promotion of crowdfunding initiatives to protect their own interests and enhance user engagement, which has raised concerns. Throughout this process, the platform often failed to conduct thorough reviews or even attempt to conceal information, leading to a lack of oversight regarding the utilization of donations.	Such news raised significant societal concerns. Public doubt has arisen regarding the fairness and impartiality of the investigation and review mechanisms employed by the online medical mutual aid platform, resulting in a decline in trust.
Sina https://finance.sina.com.cn/wm/2020-11-24/doc-iiznctke3062129.shtml?cre=tianyi&mod=pcpager_news&loc=11&r=9&rfunc=100&tj=none&tr=9 http://k.sina.com.cn/article_3884144141_e783560d01901tlxa.html	• Criminal gangs set up fraudulent websites and forged links to the online healthcare mutual aid platform to deceive donors and obtain funds. Over **30,000 individuals** were deceived, and the total amount involved exceeded **500,000 yuan (around 78,125 US dollars)**.	Both donors and recipients shared three main concerns that can be summarized as follows: First, ensuring the authenticity of the patients/recipients' identity and their true financial circumstances. Second, determining the precise amount of funds necessary for the treatment of the illness or condition. Third, clarifying how the raised funds will be utilized. More than 70.4% of donors have concerns regarding "insufficient regulatory mechanisms," "lack of transparency in fund allocation," and "distrust towards the relevant platform."
GWM.cn https://m.gmw.cn/baijia/2022-11/16/36164043.html	• A case emerged involving a nationwide network of fraudulent fundraisers who collaborated with a hospital and deceived compassionate individuals through an online healthcare mutual aid platform. The raised funds were not utilized for patient treatment. The total amount involved in the case exceeded **3 million yuan (around 458,000 US dollars)**. • Fundraising intermediaries proactively reached out to patients and their families who initiated fundraising campaigns, assisting in promoting the fundraising links. They charged a commission ranging from 30% to 70% based on the amount raised.	The healthcare crowdfunding platform continued to improve its institutional management mechanisms by strengthening the verification process for qualifications, beneficiary information, fundraising activities, medical documentation, and withdrawals. The development of validation algorithms, data models, and other related aspects was enhanced to ensure that patients in urgent need can receive timely and effective assistance through the platform.

Appendix B. Literature Review of Structural Assurances

Following the approach suggested by Wolfswinkel et al. (2013), we used the keyword “structural assurance” and conducted a comprehensive literature review in the online database to gather authoritative articles from prominent information systems (IS) journals, i.e., *EJIS*, *ISJ*, *ISR*, *JAIS*, *JIT*, *JMIS*, *JSIS*, and *MISQ* (the Association for Information Systems Senior Scholars Basket). We established three criteria to ensure the selection of relevant papers: (1) focusing on the research topic of structural assurance, (2) clearly conceptualizing structural assurance, and (3) applying the SEM technique and describing measurement items. We identified the most relevant papers through this rigorous process and synthesized the definitions and measurement approaches of structural assurances identified in the leading IS journals, as presented in Table B1.

Table B1. Definitions and Measures of Structural Assurances in IS Literature

Source	Focused assurance	Definition	Nature	Sample items
Bansal et al., 2015	Privacy statements	“Mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website.” (p. 625)	Policy focus	Operationalized as a higher-order construct with four dimensions: **Privacy policy adequacy of collection:** the privacy policy’s assurance (1) to collect only the necessary information (not adequate at all / very adequate) (2) to not collect private information for other purposes (not adequate at all / very adequate) (3) to limit information collection only to the minimum requirement (not adequate at all / very adequate) **Privacy policy adequacy of errors:** the privacy policy’s assurance (1) to correct the error promptly (not adequate at all / very adequate) (2) to view and correct errors promptly (not adequate at all / very adequate) (3) to check information for errors (not adequate at all / very adequate) (4) to maintain the accuracy of private information (not adequate at all / very adequate) **Privacy policy adequacy of unauthorized secondary use:** the privacy policy’s assurance (1) to restrict unauthorized secondary use (not adequate at all / very adequate) (2) to authorize before using it for other purposes (not adequate at all / very adequate) (3) to not share with others (not adequate at all / very adequate) (4) to decide the way information is used (not adequate at all / very adequate) **Privacy policy adequacy of unauthorized access:** the privacy policy’s assurance (1) to control tightly (not adequate at all / very adequate) (2) to achieve protection (not adequate at all / very adequate) (3) to thwart unauthorized access (not adequate at all / very adequate) (4) to devote effort to prevent theft (very low / very high)
Dimoka et al., 2012	Product assurance	“Expert information provided by third parties on the product’s true characteristics and help them predict how the product will perform in the future.” (p. 12)	Policy focus	**Operationalized as a higher-order construct with three dimensions:** (1) *Product inspection:* a binary variable based on whether the used car was inspected by an independent third party *and* had an inspection report that was made publicly available to buyers. (2) *Product history report:* a binary variable based on whether the used car’s online description made the history report available to buyers, either through Carfax or Autocheck. (3) *Product warranty:* a binary variable based on whether the car came with a manufacturer’s warranty or a warranty from an extended warranty firm.
Gefen et al., 2003	Structural assurance	“An assessment of success due to safety nets such as legal recourse, guarantees,	Policy focus	**Operationalized as a reflective construct with four items:** (1) I feel safe conducting business with the online vendor because the Better Business Bureau will protect me.

		and regulations that exist in a specific context." (p. 65)		(2) I feel safe conducting business with the online vendor because it provides a 1-800 number (3) I feel safe conducting business with the online vendor because of its statements of guarantees (4) I feel safe conducting business with the online vendor because I accessed its site through a well-known, reputable portal.
Hui et al., 2007	Privacy assurance	"Privacy statements and privacy seals [that] help consumers make a more accurate assessment of the risks of disclosing personal information to websites." (p .20)	Policy focus	**Three scenarios are created for privacy assurance:** (1) no assurance (2) assurance by means of a privacy statement (3) assurance by means of both a privacy statement and privacy seal.
Kim & Benbasat, 2009	Assuring arguments	"Statements of a claim and its supporting statements used in an Internet store to address trust-related concerns" (p. 176)	Policy focus	**Binary variable: the presence or absence of trust-assuring arguments**
Kim et al., 2009	Structural assurance	"Structural assurances in the form of agreements, contracts, regulations, policies, laws, feedback forums, guarantees, escrow services and others" (p. 289)	Policy focus	**Operationalized as a reflective construct with four items:** (1) Mobile banking firms guarantee compensation for monetary losses that might occur during service usage. (2) Mobile banking firms guarantee the protection of customers' personal information. (3) Mobile banking firms publish a policy on the protection of transactional data. (4) Mobile banking firms publish a policy on customer protection from accidents.
Kim et al., 2016	Web assurance seals	"Online consumers' perceptions of e-commerce sites, that is, how a website assures its consumers to make transactions using that site." (p. 4)	Policy focus	**Operationalized as a reflective construct with four items:** (1) The presence of a third-party seal on e-commerce websites makes me feel comfortable. (2) The presence of a third-party seal on e-commerce websites makes me feel safer in terms of privacy. (3) The presence of a third-party seal on an e-commerce website makes me feel safer in terms of security. (4) When I purchase from a website, the certification of websites for trustworthiness by other institutions such as TRUSTe are important to me.
Li et al., 2008	Organizational assurance	"Safeguards such as promises, contracts, regulations, and guarantees are in place." (p. 47)	Policy & technology focus	**Operationalized as two reflective constructs with three items:** *Organizational structural assurance:* (1) I feel assured that legal structures adequately protect me from any problem with government services (2) I feel confident that regulations, laws, and social norms make it safe for me to use government agencies (3) In general, government services are robust and safe *Technology structural assurance:* (1) I feel assured that technological structures are adequate at protecting me from any problems with information systems (2) I feel confident that technological advances make it safe for me to use information systems (3) In general, information systems are robust and safe
Mai et al., 2010	Privacy seal	"Policies [that] are posted on a firm's site and inform customers about the types of	Policy focus	**Binary variable: the presence or absence of a privacy seal**

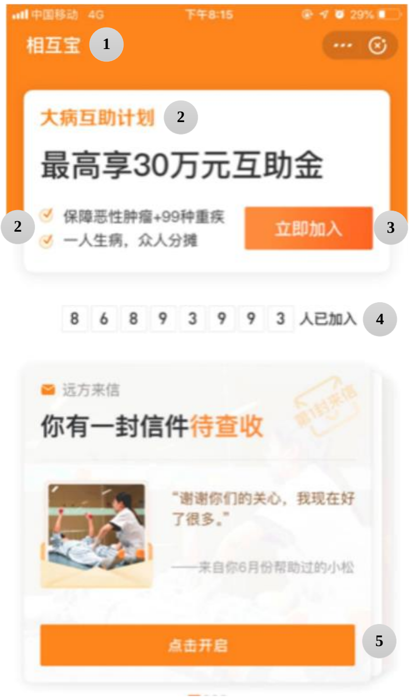
		personally identifiable information that is collected and ways such information are used or shared with other entities.” (p. 191)		
I. Park et al., 2010	Assurance seal	“Third-party assurance seals [that] are provided by the vendors through a third party (after an independent audit and investigation) and serve to guarantee the privacy policy of the online vendors.” (p. 12)	Policy focus	**Operationalized as assurance seals that are provided by a number of companies**
McKnight et al., 2002a, 2002b	Structural assurance	“One believes that structures like guarantees, regulations, promises, legal recourse, or other procedures are in place to promote success.” (p. 339)	Policy & technology focus	**Operationalized as a reflective construct with four items:** (1) The internet has enough safeguards to make me feel comfortable using it to transact personal business. (2) I feel assured that legal and technological structures adequately protect me from problems on the Internet. (3) I feel confident that encryption and other technological advances on the Internet make it safe for me to do business there. (4) In general, the Internet is now a robust and safe environment in which to transact business.
Özpolat et al., 2013	Assurance seals	“Third-party mechanisms [that] endeavor to provide independent verification of a retailer’s quality.” (p. 1102)	Policy focus	**Binary variable: the presence or absence of third-party seals**
Pavlou, 2002	Institutional structure	“The belief that a party has about the security of a situation because of guarantees, safety nets, and other structures.” (p. 219)	Policy focus	**Five specific institution-based mechanisms are established: perceived monitoring, perceived legal bonds, perceived accreditation, perceived feedback, and perceived cooperative norms**
Nicolaou & McKnight, 2011	Structural assurance	“One’s sense of security from guarantees, safety nets, or other impersonal structures inherent in a specific context.”(p. 274)	Policy & technology focus	**Operationalized as a reflective construct with three items:** (1) The data exchange provided by PanAmerican Industries has enough safeguards to make me feel comfortable using it to transact business. (2) I feel assured that legal and technological structures adequately protect me from problems on this data exchange. (3) I feel confident that encryption and other technological advances on this data exchange make it safe for me to do business there.

Appendix C: Description of Xianghubao

Xianghubao, which literally means “peer-to-peer healthcare mutual aid service,” was launched in October 2018. The aim of Xianghubao is to support a certain group of people in forming an insurance risk pool. Xianghubao provides its users with a basic health plan against 100 types of critical illnesses, including thyroid cancer, breast cancer, lung cancer, critical brain injury, and acute myocardial infarction. An individual with a critical illness or life-threatening injury is entitled to receive lump-sum cash payouts, which are shared equally by all other members in the pool.

In particular, Xianghubao is one of the first online healthcare platforms to implement blockchain technology to support the overall mutual aid process. Users are provided with a blockchain-enabled smart contract during the enrollment process. Thus, they can deduct the collective claims-sharing cost without intermediaries. Additionally, users are protected by a blockchain-based cryptographic private key; thus, their private data (e.g., identity information, payment account, etc.) can be kept anonymous.

At the same time, when a claim occurs, blockchain technology ensures that the claim information is issued and confirmed by all users, which cannot be tampered with. Users can query the entire tamper-resistant claim information and see the mutual aid funds flow. If there is no objection to the claim publicity, the mutual aid cost will be evenly shared by each user, and a tamper-proof blockchain certificate will be disclosed to all users. The certificate information includes the number of members who have shared the claims payment, the number of claims, and the claim details (e.g., basic information of insureds, details of illness, claims amount, etc.).



最高享30万元互助金

保障恶性肿瘤+99种重疾

一人生病，众人分摊

你有一封信件待查收

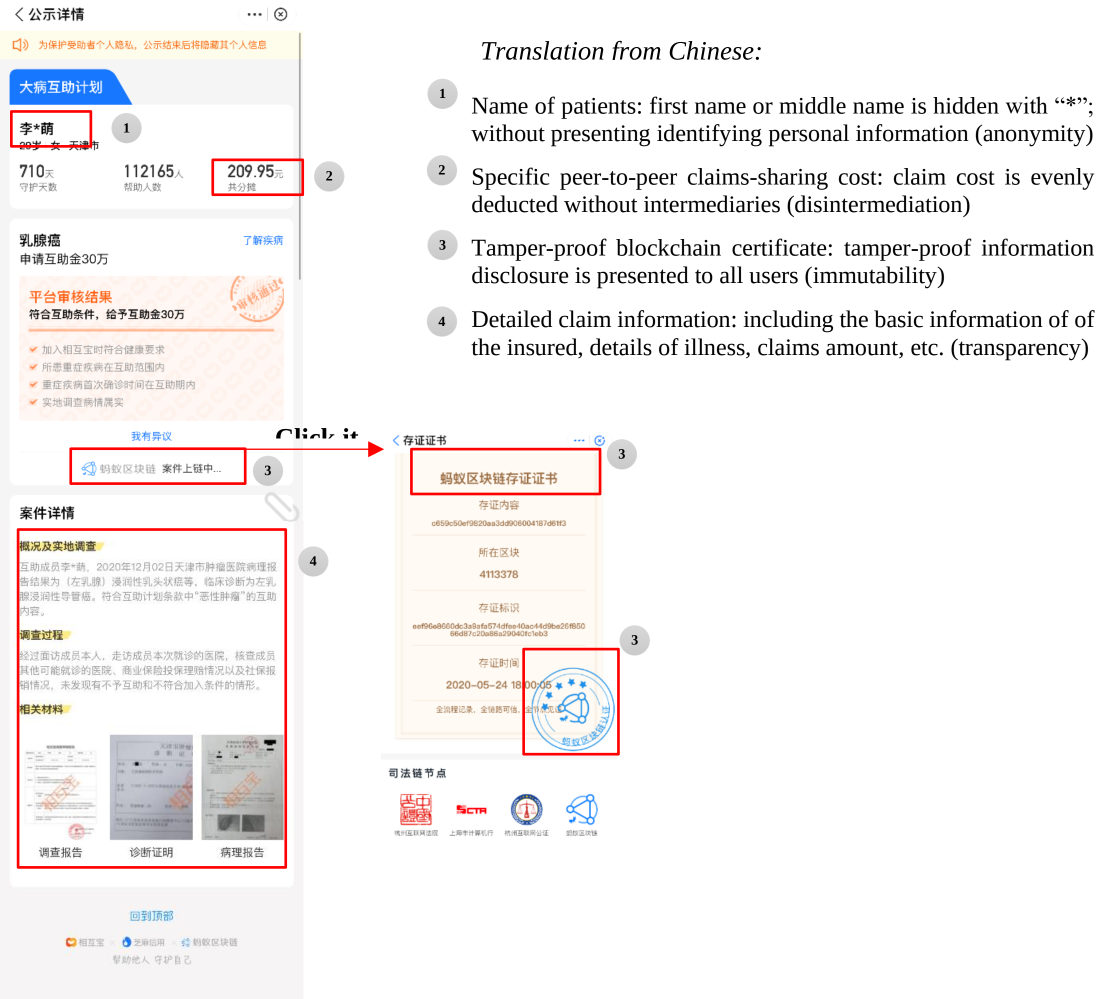
“谢谢你们的关心，我现在好了很多。”

——来自你6月份帮助过的小松

Translation from Chinese:

1. Name of the mutual aid platform
2. Click it to see detailed platform insurance policies
3. “Join in as a user” option
4. Number of joined users updated in real time
5. Upcoming Events

Figure C1. Screenshot of the Xianghubao Homepage



公示详情

为保护受助者个人隐私，公示结束后将隐藏其个人信息

大病互助计划

李*萌
20岁 | 女 | 天津市

710天 守护天数 | 112165人 帮助人数 | 209.95元 共分摊

乳腺癌
申请互助金30万

了解疾病

平台审核结果
符合互助条件，给予互助金30万

- ✓ 加入相互宝时符合健康要求
- ✓ 所患重症疾病在互助范围内
- ✓ 重症疾病首次确诊时间在互助期内
- ✓ 实地调查病情属实

我有异议

蚂蚁区块链 案件上链中...

案件详情

概况及实地调查

互助成员李*萌，2020年12月02日天津市肿瘤医院病理报告结果为（左乳腺）浸润性乳头状癌等，临床诊断为左乳腺浸润性导管癌。符合互助计划条款中“恶性肿瘤”的互助内容。

调查过程

经过面访成员本人，走访成员本次就诊的医院，核查成员其他可能就诊的医院、商业保险投保理赔情况以及社保报销情况，未发现有不予互助和不符合加入条件的情形。

相关材料

调查报告 诊断证明 病理报告

回到顶部

相互宝 × 芝麻信用 × 蚂蚁区块链
帮助他人 守护自己

Click it

存证证书

蚂蚁区块链存证证书

存证内容
c659c50ef9820aa3dd906004187d61f3

所在区块
4113378

存证标识
eef96e8660dc3a9afa574dfee40ac44d9be26f850
66d87c20a86a29040fc1eb3

存证时间
2020-05-24 18:00:05

全流程记录，全链路可信，全节点见证

蚂蚁区块链认证

司法链节点

杭州互联网法院 上海市计算机行 杭州互联网公证 蚂蚁区块链

Translation from Chinese:

1. Name of patients: first name or middle name is hidden with “*”; without presenting identifying personal information (anonymity)
2. Specific peer-to-peer claims-sharing cost: claim cost is evenly deducted without intermediaries (disintermediation)
3. Tamper-proof blockchain certificate: tamper-proof information disclosure is presented to all users (immutability)
4. Detailed claim information: including the basic information of of the insured, details of illness, claims amount, etc. (transparency)

Figure C2. Screenshot of the Detailed Blockchain-enabled Technology Assurance on the Xianghubao Platform

Appendix D: Scale Development of Blockchain-enabled Technology Assurance

We first confirmed the formative nature of blockchain-enabled technology assurance based on three rules. First, no single dimension can adequately explain blockchain-enabled technology assurance, implying that the four specific dimensions describe characteristics/ingredients rather than the manifestations of blockchain-enabled technology assurance (Benitez et al., 2020). Second, the definitions of the four dimensions are clearly distinguished, with each capturing a very distinct facet of blockchain-enabled technology assurance. In other words, the four dimensions are not interchangeable because deleting any one of them would significantly change the meaning of blockchain-enabled technology assurance (MacKenzie et al., 2011). Third, the four dimensions do not closely correlate with each other. For example, higher levels of data anonymity in online healthcare mutual aid platforms do not necessarily guarantee greater levels of immutability, transparency, and disintermediation of online transactions. Thus, it is appropriate to model blockchain-enabled technology assurance as a formative construct (Benitez et al., 2020).

We then developed the scales of blockchain-enabled technology assurance following the procedures suggested by MacKenzie et al. (2011). First, we conceptualized the construct of blockchain-enabled technology assurance into four dimensions (i.e., anonymity, immutability, transparency, and disintermediation) and developed the indicators for each dimension based on previous literature on blockchain (Hughes et al., 2019; Ostern, 2018; Schuetz & Venkatesh, 2019; Shao et al., 2022). Specifically, we measured the dimensions of disintermediation and immutability based on their definition and a review of previous literature (Hughes et al., 2019; Ostern, 2018; Underwood, 2016). While the dimensions of anonymity and transparency were measured and adapted based on Shao et al. (2022a). Second, to ensure the content validity of the newly developed construct (i.e., blockchain-enabled technology assurance), we constructed a matrix in which definitions of the four specific dimensions are listed at the top of the columns, and the items are listed in the rows (MacKenzie et al., 2011). In particular, we invited 18 respondents who had rich academic and practical experience in the domain of blockchain-enabled healthcare mutual aid services. We provided the matrix table to the respondents and asked them to rate the extent to which each item captures the four dimensions using a 7-point Likert scale (see Table D1). We found that the mean rating of the specific item on the hypothesized dimension is significantly higher than that on any other dimension. Furthermore, we asked them to provide suggestions for items that were not clear or not easy to understand. The feedback resulted in some minor modifications. For example, "The health mutual aid contents on the Xianghubao platform is transparent with the implementation of blockchain technology" was revised as "With the implementation of blockchain technology, the health mutual aid process on the Xianghubao platform is transparent." Detailed revised items are presented in Appendix G. Third, we conducted a pilot study and evaluated the validity of blockchain-enabled technology assurance as a second-order formative construct by assessing two criteria (i.e., path weights and multicollinearity) and testing the MIMIC model. All criteria were satisfied (Benitez et al., 2020; MacKenzie et al., 2011), proving the validity of the second-order blockchain-enabled technology assurance operationalization (see details in Table D2 and Figure D1).

Table D1. Example of Item Rating Task to Assess Content Adequacy

Definitions of the four dimensions of blockchain-enabled technology assurance	**Disintermediation (DI)** is the extent to which a user believes that the healthcare platform provides strong peer-to-peer equal health mutual aid services without intermediaries **Immutability (IM)** is the extent to which a user believes that the healthcare platform uploads transaction data that cannot be changed, edited, or tampered **Anonymity (AN)** is the extent to which a user believes that the healthcare platform ensures anonymous identity information of members **Transparency (TR)** is the extent to which a user believes that the healthcare platform tracks and records the corresponding case details and transaction history			
Based on the definitions, please indicate the extent to which you agree or disagree that each of the following item attributes to each specific dimension (1: Strongly disagree, 2: Disagree, 3: Slightly disagree 4: Neither agree nor disagree, 5: Slightly agree, 6: Agree, 7: Strongly agree)				
Rater number = 001*	**DI**	**IM**	**AN**	**TR**
Blockchain technology enables members to enjoy equal rights on the Xianghubao platform	5	1	1	1
Blockchain technology provides the direct transactions of peers in a secure way by replacing a cascade of middlemen on the Xianghubao platform	7	1	1	1
The Xianghubao platform performs the health mutual aid service without the need for intermediaries	7	1	1	1
Blockchain technology ensures the uploaded information on the Xianghubao platform beyond the power of an individual to change	2	7	1	1
Blockchain technology guarantees the transactions on the Xianghubao platform unalterable	1	6	1	1
Blockchain technology makes changing information impossible on the Xianghubao platform	1	7	1	1
Blockchain technology hides members' true identities on the Xianghubao platform	1	1	6	3
Blockchain technology enables the anonymity of members when joining in the health mutual aid service	1	1	7	1

Blockchain technology helps keep members' information anonymous on the Xianghubao platform	1	1	7	1
The health mutual aid process on Xianghubao platform is transparent with the implementation of blockchain technology	1	1	1	7
The Xianghubao platform provides members with deep access to understand the health mutual aid work process with the implementation of blockchain technology	1	1	1	5
The Xianghubao platform provides members with in-depth knowledge about how the health mutual aid service operates with the implementation of blockchain technology	1	1	1	6
Note: *we only presented one rater (one of the 18 respondents) as an exemplary case evidence				

Table D2. Path Weights and VIF for Formative Indicators (Pilot Study)

Formative indicators relationships	**Path Weights**	**VIF**
Transparency → Blockchain-enabled technology assurance	0.362^{**}	2.635
Anonymity → Blockchain-enabled technology assurance	0.253^{*}	1.246
Immutability → Blockchain-enabled technology assurance	0.309^{**}	1.429
Disintermediation → Blockchain-enabled technology assurance	0.361^{**}	2.685
Note: t-test are significant at: $^{*}p < 0.05$; $^{**}p < 0.01$		

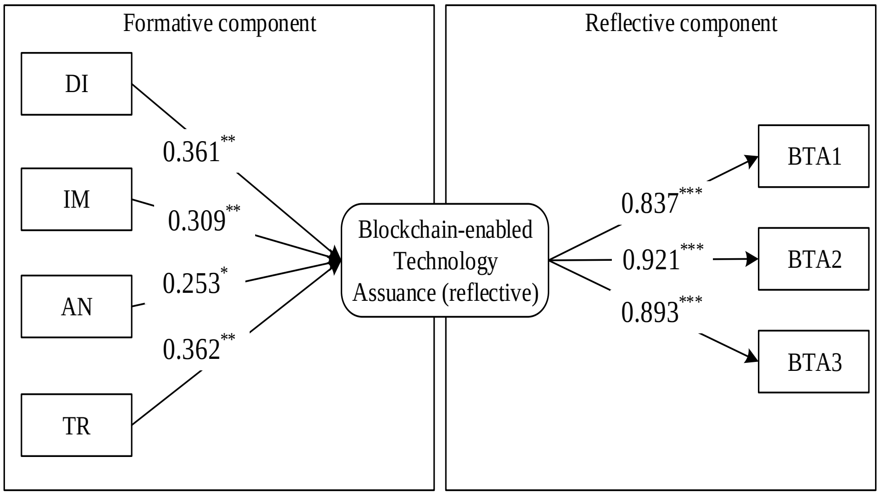


Figure D1. MIMIC Analysis (Pilot study)

Note: t-tests are significant at: $^{***}p < 0.001$; for formative items, the number represents path weight; for reflective items, the number represents factor loading; DI represents disintermediation; IM represents immutability; AN represents anonymity; TR represents transparency.

Appendix E: Literature Review of Scale Measurements of Actual Behavior

Definition	Dimensions	Method	Specific operationalization	Reference
Actual behavior is defined as a user's employment of an IS to perform a task	Duration	Objective method	Amount of time recorded in the system logs	Venkatesh et al., 2002
		Subjective method	Duration of time stayed in a system (ordinal scale)	Moores & Chang, 2006; Veiga et al., 2014; Wu & Holsapple, 2014
	Frequency	Objective method	Number of transactions/sent messages/use times recorded in the system logs	Pavlou & Gefen, 2005; Szajna, 1996
		Subjective method	The frequency of usage over a given period (ordinal scale)	Lim et al., 2006; Limayem & Hirt, 2003; Moores & Chang, 2006; Pavlou & Fygenson, 2006; Sia et al., 2009; Szajna, 1996; Venkatesh et al., 2012; Wu & Holsapple, 2014
	Intensity	Objective method	Number of performed activities or experienced features recorded in the system logs	Devaraj et al., 2008; Zhang et al., 2021
		Subjective method	Usage of a variety of features (ordinal scale)	Moores & Chang, 2006; Venkatesh et al., 2012

Appendix F: Questionnaire Design

Constructs	Items
Main constructs in our model	
Policy assurance (PA)	PA1: The Xianghubao platform has enough rules and policy statements PA2: I feel assured that the Xianghubao platform provides adequate contractual guarantees PA3: The Xianghubao platform provides protective regulatory and legal guarantees
Blockchain-enabled technology assurance (BTA, reflective)	BTA1: Blockchain technology makes me feel safe in joining the health mutual aid service BTA2: Blockchain technology makes me feel comfortable towards the Xianghubao platform BTA3: In general, blockchain technology provides secure algorithms and encryption protocols to reduce the risk of data corruption or fraud.
Disintermediation (DI, as a formative indicator of BTA)	DI1: Blockchain technology enables members to enjoy equal rights without an intermediary on the Xianghubao platform DI2: Blockchain technology provides the direct transactions of peers in a secure way by replacing a cascade of middlemen on the Xianghubao platform DI3: The Xianghubao platform performs the health mutual aid service without the need for intermediaries
Immutability (IM, as a formative indicator of BTA)	IM1: Blockchain technology ensures the uploaded information on the Xianghubao platform is beyond the power of an individual to change IM2: Blockchain technology guarantees the transactions on the Xianghubao platform are unalterable IM3: Blockchain technology makes changing information impossible on the Xianghubao platform
Anonymity (AN, as a formative indicator of BTA)	AN1: Blockchain technology hides members' true identities on the Xianghubao platform AN2: Blockchain technology enables the anonymity of members when joining in the health mutual aid service AN3: Blockchain technology could help keep members' information anonymous on the Xianghubao platform
Transparency (TR, as a formative indicator of BTA)	TR1: With the implementation of blockchain technology, the health mutual aid process on the Xianghubao platform is transparent TR2: With the implementation of blockchain technology, the Xianghubao platform provides members with deep access to understand the health mutual aid work process TR3: With the implementation of blockchain technology, the Xianghubao platform provides members with in-depth knowledge about the transparent flow of capital for each claim
Trust in the platform (TR)	TR1: The Xianghubao platform is competent and effective in handling the health mutual aid service TR2: The Xianghubao platform would act in members' best interests TR3: The Xianghubao platform is honest and can be trusted at all times
Intention to use (IU)	IU1: If I could, I would like to continue my use of the Xianghubao platform IU2: I intend to continue using the Xianghubao platform rather than discontinue its use IU3: I intend to continue using the Xianghubao platform in the future
Actual usage behavior	**Frequency of usage (USF)**: On average, how frequently did you open and use the Xianghubao platform for the last six months: (1)less than once per month; (2)1-2 times per month; (3)3-4 times per month; (4)More than 5 times per month **Intensity of usage (USI):** Please indicate whether you used the following functionalities in the Xianghubao platform for the last six months (we use a five-point scale for this item, and each scale lists different functionalities, including: (1)Publicity Column; (2)News Column; (3)Mutual Aid Activities Column; (4)Health Services Column; (5) Health Tips
Control variables	
Familiarity with blockchain technology (FBT)	FBT1: I am familiar with blockchain technology through experiencing related applications FBT2: I am familiar with blockchain technology through reading news or other materials FBT3: I am familiar with blockchain technology through communicating with others
Altruism (AL)	AL1: I like helping other people AL2: It feels good to help others solve their problems AL3: I enjoy helping others since it results in my own achievements
Perceived innovativeness (PI)	PI1: If I heard about new information technology, I would look for ways to experiment with it PI2: I like to experiment with new information technologies PI3: In general, I am enthusiastic about trying new information technologies
Marker	
Self-management of learning (SM)	SM1: When it comes to learning, I am a self-directed person SM2: I am able to manage my learning time effectively and easily complete assignments on time. SM3: When it comes to learning, I set goals and have a high degree of initiative.

Appendix G: Model Fit and Quality Indices

Classic indices	Suggested threshold	Conclusion	Additional indices	Suggested threshold	Conclusion
Model fit of the model at the first-order level					
Average path coefficient (APC) = 0.218	Normally acceptable fit is indicated by a *p*-value associated with an APC which is equal to or lower than 0.05; that is, significant at the 0.05 level	✓	Standardized root mean squared residual (SRMR) = 0.065	Generally, SRMR values lower than 0.1 indicate an acceptable fit	✓
Average *R*-squared (ARS) = 0.426	Normally acceptable fit is indicated by a *p*-value associated with an ARS which is equal to or lower than 0.05; that is, significant at the 0.05 level	✓			
Average adjusted *R*-squared (AARS) = 0.416	Normally acceptable fit is indicated by a *p*-value associated with an AARS which is equal to or lower than 0.05; that is, significant at the 0.05 level	✓	Standardized mean absolute residual (SMAR) = 0.049	Generally, SMAR values lower than 0.1 indicate an acceptable fit	✓
Average block VIF (AVIF) = 1.379	Generally, AVIF values lower than 3.3 indicate an acceptable fit	✓			
Average full collinearity VIF (AFVIF) = 1.784	Generally, AFVIF values lower than 3.3 indicate an acceptable fit	✓	Standardized chi-squared with 324 degrees of freedom (SChS) = 9.437 P<0.001	Normally acceptable fit is indicated by a *p*-value associated with a SChS that is equal to or lower than 0.05; that is, significant at the 0.05 level	✓
Tenenhaus GoF (GoF) = 0.609	Small if equal to or greater than 0.1, medium if equal to or greater than 0.25, and large if equal to or greater than 0.36	✓			
Simpson's paradox ratio (SPR) = 0.867	Generally, values of the SPR equal to or greater than 0.7 indicate an acceptable fit	✓	Standardized threshold difference count ratio (STDCR) = 0.994	Generally, values of the STDCR equal to or greater than 0.7 indicate an acceptable fit	✓
R-squared contribution ratio (RSCR) = 1.000	Generally, values of the RSCR equal to or greater than 0.9 indicate an acceptable fit	✓			
Statistical suppression ratio (SSR) = 0.933	Generally, values of the SSR equal to or greater than 0.7 indicate an acceptable fit	✓	Standardized threshold difference sum ratio (STDSR) = 0.970	Generally, values of the STDSR equal to or greater than 0.7 indicate an acceptable fit	✓
Nonlinear bivariate causality direction ratio (NLBCDR)=1.000	Generally, values of the NLBCDR equal to or greater than 0.7 indicate an acceptable fit	✓			
Model fit of the model at the second-order level					
Average path coefficient (APC) = 0.163	Normally acceptable fit is indicated by a *p*-value associated with an APC which is equal to or lower than 0.05; that is, significant at the 0.05 level	✓	Standardized root mean squared residual (SRMR) = 0.060	Generally, SRMR values lower than 0.1 indicate an acceptable fit	✓
Average *R*-squared (ARS) = 0.380	Normally acceptable fit is indicated by a *p*-value associated with an ARS which is equal to or lower than 0.05; that is, significant at the 0.05 level	✓			
Average adjusted *R*-squared (AARS) = 0.368	Normally acceptable fit is indicated by a *p*-value associated with an AARS which is equal to or lower than 0.05; that is, significant at the 0.05 level	✓	Standardized mean absolute residual (SMAR) = 0.046	Generally, SMAR values lower than 0.1 indicate an acceptable fit	✓

Average block VIF (AVIF) = 1.250	Generally, AVIF values lower than 3.3 indicate an acceptable fit	✓			
Average full collinearity VIF (AFVIF) = 1.892	Generally, AFVIF values lower than 3.3 indicate an acceptable fit	✓	Standardized chi-squared with 324 degrees of freedom (SChS) = 5.958, *p* < 0.001	Normally acceptable fit is indicated by a *p*-value associated with a SChS that is equal to or lower than 0.05; that is, significant at the 0.05 level	✓
Tenenhaus GoF (GoF) = 0.565	Small if equal to or greater than 0.1, medium if equal to or greater than 0.25, and large if equal to or greater than 0.36	✓			
Simpson's paradox ratio (SPR) = 0.842	Generally, values of the SPR equal to or greater than 0.7 indicate an acceptable fit	✓	Standardized threshold difference count ratio (STDCR) = 1.000	Generally, values of the STDCR equal to or greater than 0.7 indicate an acceptable fit	✓
R-squared contribution ratio (RSCR) = 0.994	Generally, values of the RSCR equal to or greater than 0.9 indicate an acceptable fit	✓			
Statistical suppression ratio (SSR) = 0.895	Generally, values of the SSR equal to or greater than 0.7 indicate an acceptable fit	✓	Standardized threshold difference sum ratio (STDSR) =1.000	Generally, values of the STDSR equal to or greater than 0.7 indicate an acceptable fit	✓
Nonlinear bivariate causality direction ratio (NLBCDR) = 0.974	Generally, values of the NLBCDR equal to or greater than 0.7 indicate an acceptable fit	✓			

Appendix H: Construct Validity and Reliability

Construct	Items	Factor loadings	Composite reliability	AVE
Policy assurance	PA1	0.924	0.943	0.846
	PA2	0.920		
	PA3	0.916		
Disintermediation	DI1	0.870	0.886	0.723
	DI2	0.890		
	DI3	0.787		
Immutability	IM1	0.866	0.899	0.746
	IM2	0.895		
	IM3	0.830		
Anonymity	AN1	0.871	0.912	0.774
	AN2	0.890		
	AN3	0.800		
Transparency	TR1	0.890	0.906	0.762
	TR2	0.875		
	TR3	0.854		
Trust in the platform	TP1	0.883	0.907	0.766
	TP2	0.837		
	TP3	0.904		
Intention to use	IU1	0.962	0.973	0.922
	IU2	0.958		
	IU3	0.960		
Familiarity with blockchain technology	FBT1	0.923	0.939	0.837
	FBT2	0.918		
	FBT3	0.902		
Altruism	AL1	0.866	0.926	0.806
	AL2	0.915		
	AL3	0.912		
Perceived innovativeness	PI1	0.874	0.894	0.740
	PI2	0.895		
	PI3	0.807		

Appendix I: Combined Loadings and Cross-loadings

Table I. Combined Loadings and Cross-Loadings

Items	PA	DI	IM	AN	TR	TP	IU	FBT	ALT	PI
PA1	**0.924**	0.371	0.217	0.363	0.376	0.589	0.313	0.129	0.150	0.176
PA2	**0.920**	0.399	0.304	0.373	0.393	0.653	0.333	0.206	0.243	0.205
PA3	**0.916**	0.340	0.331	0.345	0.392	0.706	0.347	0.115	0.194	0.182
DI1	0.326	**0.870**	0.447	0.385	0.581	0.327	0.175	0.320	0.267	0.233
DI2	0.362	**0.890**	0.457	0.417	0.570	0.295	0.193	0.266	0.310	0.159
DI3	0.338	**0.787**	0.393	0.322	0.525	0.325	0.209	0.187	0.235	0.153
IM1	0.321	0.456	**0.866**	0.342	0.422	0.338	0.137	0.164	0.268	0.133
IM2	0.276	0.535	**0.895**	0.368	0.580	0.343	0.153	0.240	0.300	0.135
IM3	0.199	0.323	**0.830**	0.347	0.433	0.343	0.152	0.171	0.153	0.074
AN1	0.369	0.415	0.399	**0.871**	0.489	0.367	0.163	0.186	0.243	0.151
AN2	0.374	0.364	0.333	**0.890**	0.479	0.389	0.229	0.245	0.232	0.146
AN3	0.291	0.390	0.344	**0.880**	0.535	0.324	0.276	0.252	0.199	0.140
TR1	0.321	0.627	0.518	0.501	**0.890**	0.422	0.265	0.297	0.248	0.206
TR2	0.425	0.554	0.450	0.454	**0.875**	0.438	0.196	0.296	0.297	0.164
TR3	0.357	0.541	0.486	0.538	**0.854**	0.428	0.306	0.266	0.314	0.145
TP1	0.691	0.377	0.397	0.371	0.514	**0.883**	0.329	0.220	0.248	0.247
TP2	0.521	0.273	0.272	0.326	0.307	**0.837**	0.336	0.141	0.224	0.172
TP3	0.636	0.319	0.364	0.376	0.462	**0.904**	0.455	0.216	0.279	0.230
IU1	0.368	0.248	0.166	0.250	0.298	0.430	**0.962**	0.185	0.195	0.251
IU2	0.307	0.181	0.157	0.199	0.251	0.389	**0.958**	0.122	0.175	0.243
IU3	0.362	0.220	0.168	0.281	0.293	0.412	**0.960**	0.181	0.205	0.271
FBT1	0.159	0.313	0.269	0.247	0.345	0.218	0.148	**0.923**	0.300	0.352
FBT2	0.152	0.256	0.147	0.230	0.287	0.211	0.187	**0.918**	0.207	0.330
FBT3	0.135	0.269	0.193	0.232	0.267	0.177	0.130	**0.902**	0.214	0.345
AL1	0.231	0.309	0.260	0.291	0.309	0.316	0.187	0.228	**0.866**	0.266
AL2	0.198	0.321	0.283	0.208	0.305	0.222	0.141	0.250	**0.915**	0.223
AL3	0.145	0.232	0.213	0.192	0.269	0.237	0.210	0.229	**0.912**	0.207
PI1	0.178	0.197	0.125	0.146	0.184	0.231	0.263	0.376	0.187	**0.874**
PI2	0.181	0.212	0.166	0.140	0.207	0.236	0.227	0.347	0.284	**0.895**
PI3	0.166	0.140	0.045	0.140	0.112	0.168	0.192	0.235	0.191	**0.807**

Note: PA represents policy assurance; DI represents disintermediation; IM represents immutability; AN represents anonymity; TR represents transparency; TP represents trust in the platform; IU represents intention to use; FBT represents familiarity with blockchain technology; ALT represents altruism; PI represents perceived innovativeness

Appendix J: Descriptive Statistics and Correlation Matrix

Criterion	**Construct**	***M***	***SD***	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**	**(11)**	**(12)**	**(13)**	**(14)**	**(15)**	**(16)**
Fornell-Larcker criterion	1.PA	5.200	1.003	0.920															
	2.DI	5.610	0.910	0.402	0.850														
	3.IM	5.602	0.990	0.309	0.510	0.864													
	4.AN	5.280	1.171	0.392	0.443	0.407	0.880												
	5.TR	5.717	0.845	0.421	0.658	0.555	0.569	0.873											
	6.TP	4.930	0.980	0.706	0.370	0.395	0.409	0.491	0.875										
	7.IU	4.158	1.501	0.360	0.225	0.170	0.253	0.292	0.428	0.960									
	8.USF	1.122	0.383	0.146	0.040	-0.001	0.134	0.101	0.178	0.421	N/A								
	9.USI	1.195	0.445	0.132	-0.010	-0.022	0.079	0.071	0.130	0.498	0.737	N/A							
	10.FBT	4.907	1.050	0.163	0.305	0.222	0.259	0.328	0.221	0.169	-0.013	-0.009	0.915						
	11.AL	6.016	0.982	0.213	0.320	0.281	0.255	0.327	0.287	0.200	0.032	0.050	0.263	0.898					
	12.PI	3.325	1.114	0.204	0.214	0.133	0.165	0.197	0.248	0.265	0.199	0.194	0.374	0.258	0.860				
	13.Gender	1.502	0.501	-0.048	0.166	0.177	0.180	0.126	0.025	0.039	-0.091	-0.011	-0.025	-0.058	-0.195	N/A			
	14.Age	1.946	0.956	0.044	-0.050	-0.103	0.012	-0.074	0.029	0.016	0.085	0.021	0.077	-0.008	0.013	-0.107	N/A		
	15.Income	2.010	0.834	-0.181	-0.050	-0.004	-0.185	-0.046	-0.125	-0.105	-0.157	-0.192	0.035	0.072	-0.023	-0.094	0.074	N/A	
	16.UE	1.746	0.660	0.182	0.037	0.059	0.070	0.125	0.206	0.401	0.472	0.531	0.176	0.042	0.171	0.032	0.017	-0.165	N/A
HTMT criterion	1.PA	5.200	1.003	N/A															
	2.DI	5.610	0.910	0.470	N/A														
	3.IM	5.602	0.990	0.354	0.619	N/A													
	4.AN	5.280	1.171	0.445	0.532	0.484	N/A												
	5.TR	5.717	0.845	0.480	0.797	0.661	0.671	N/A											
	6.TP	4.930	0.980	0.803	0.449	0.470	0.481	0.579	N/A										
	7.IU	4.158	1.501	0.385	0.258	0.191	0.280	0.326	0.474	N/A									
	8.USF	1.122	0.383	0.153	0.044	0.055	0.145	0.110	0.193	0.431	N/A								
	9.USI	1.195	0.445	0.138	0.031	0.061	0.099	0.078	0.139	0.509	0.737	N/A							
	10.FBT	4.907	1.050	0.180	0.356	0.256	0.294	0.375	0.251	0.182	0.014	0.010	N/A						
	11.AL	6.016	0.982	0.239	0.379	0.326	0.296	0.381	0.333	0.218	0.033	0.054	0.295	N/A					
	12.PI	3.325	1.114	0.236	0.261	0.164	0.198	0.234	0.295	0.298	0.220	0.215	0.432	0.303	N/A				
	13.Gender	1.502	0.501	0.050	0.183	0.194	0.195	0.137	0.042	0.040	0.091	0.011	0.040	0.062	0.214	N/A			
	14.Age	1.946	0.956	0.046	0.068	0.112	0.026	0.081	0.042	0.017	0.085	0.021	0.081	0.024	0.030	0.107	N/A		
	15.Income	2.010	0.834	0.190	0.060	0.042	0.200	0.050	0.137	0.107	0.157	0.192	0.041	0.076	0.053	0.094	0.074	N/A	
	16.UE	1.746	0.660	0.191	0.073	0.086	0.079	0.136	0.221	0.410	0.472	0.531	0.186	0.045	0.189	0.032	0.017	0.165	N/A

Appendix K: Validation of Blockchain-Enabled Technology Assurance as a Second-order Formative Construct

Table K1. Path Weights and VIF for Formative Indicators

Formative indicators relationships	Path weights	VIF
Transparency → Blockchain-enabled technology assurance	0.340^{***}	2.280
Anonymity → Blockchain-enabled technology assurance	0.288^{***}	1.509
Immutability → Blockchain-enabled technology assurance	0.297^{***}	1.550
Disintermediation → Blockchain-enabled technology assurance	0.318^{***}	1.876
Note: t-tests are significant at: $^{***}p$ < 0.001		

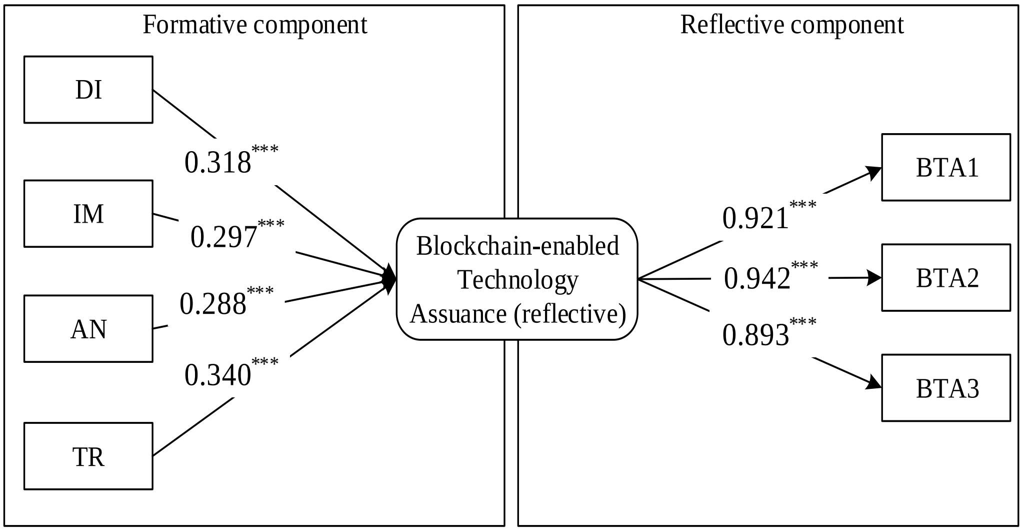


Figure K1. MIMIC Analysis

Note: t-tests are significant at: $^{***}p$ < 0.001; for formative items, the number represents path weight; for reflective items, the number represents the factor loading; DI represents disintermediation; IM represents immutability; AN represents anonymity; TR represents transparency.

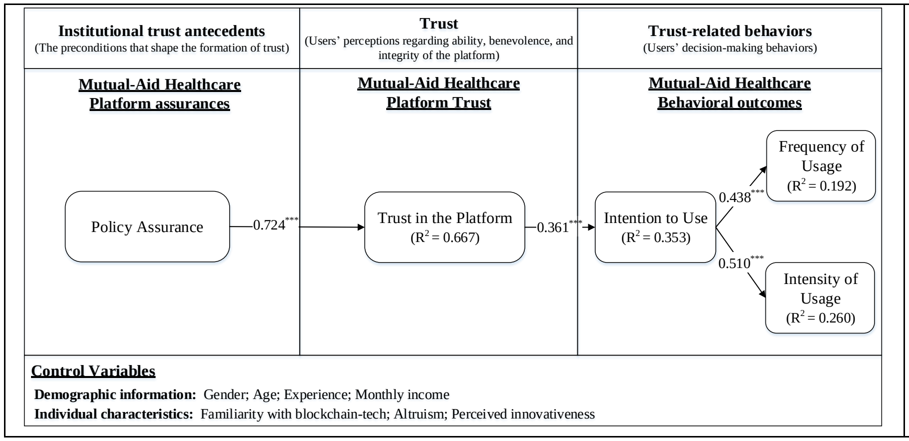
Table K2. Descriptive Statistics and Correlational Analysis of the Internal MIMIC Structure

Construct	*M*	*SD*	CR(AVE)	(1)	(2)	(3)	(4)	(5)	(6)
1.Overal BTA_reflective component	5.420	1.007	0.910(0.771)	N/A					
2.Overal BTA_formative component	5.613	0.674	N/A	0.593***	N/A				
3.DI	5.610	0.910	N/A	0.422***	0.657***	N/A			
4.IM	5.602	0.990	N/A	0.474***	0.719***	0.496***	N/A		
5.AN	5.280	1.171	N/A	0.535***	0.527***	0.434***	0.406***	N/A	
6.TR	5.717	0.845	N/A	0.571***	0.833***	0.655***	0.548***	0.570***	N/A
Note: M represents mean; *SD* represents standard deviation. *** represents *p* <0.001; CR represents composite reliability, and the number in the parentheses represents AVE; BTA represents blockchain-enabled technology assurance; DI represents disintermediation; IM represents immutability; AN represents anonymity; TR represents transparency.									

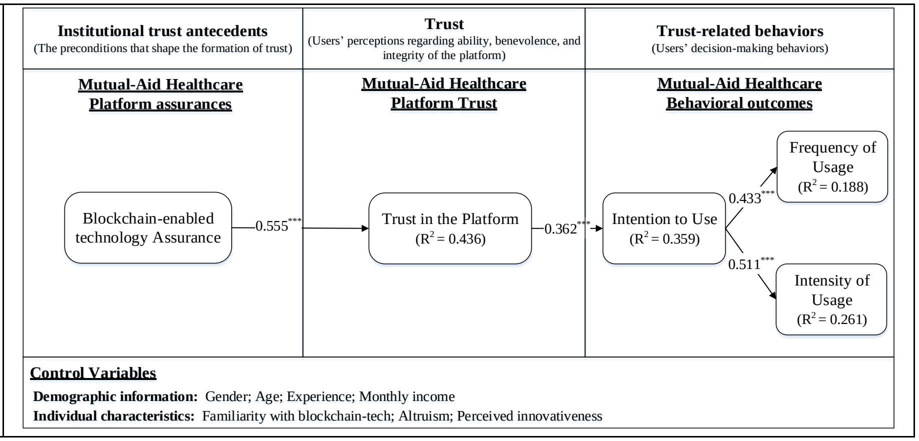
Appendix L: Testing of Alternative Models

We conducted a thorough analysis to assess the separate and combined effects of policy assurance and technology assurance on users' intention and use. Specifically, we tested three alternative models: *(a)* a model with only the antecedent of policy assurance and the mediator (i.e., trust), *(b)* a model with only the antecedent of blockchain-enabled technology assurance and the mediator (i.e., trust), and *(c)* a model with the antecedents of policy and blockchain-enabled technology assurances. Our proposed model *(d)* includes the antecedents of policy and blockchain-enabled technology assurances and the mediator (i.e., trust). The analysis results are presented below. We can see that model *(d)* explains more variance in endogenous variables compared to other models. Specifically, concerning the endogenous variable of trust in the platform, there is a statistically significant increase in the incremental R^2 of 0.231 (F- value = 83.143, $p < 0.001$) observed from model (*a*) to model (*b*). This implies that policy assurance explains more variance in trust in the platform compared to blockchain-enabled technology assurance. Meanwhile, we found that the incremental R^2 is 0.041 (F-value = 28.223, $p < 0.001$) when transitioning from model (*a*) to model (*d*), and a substantial increase of R^2 is 0.272 (F-value = 187.233, $p < 0.001$) when progressing from model (*b*) to model (*d*). These findings suggest that incorporating both types of assurances in the model together explains the most variance in trust in the platform. Additionally, for the endogenous variable of intention to use, there was a significant incremental R^2 increase of 0.027 (F-value = 8.506, $p < 0.001$) after incorporating the mediating variable of trust in the platform in the shift from model (*c*) to model (*d*). Therefore, the comparison between the four models further demonstrates the validity and superiority of our proposed research model.

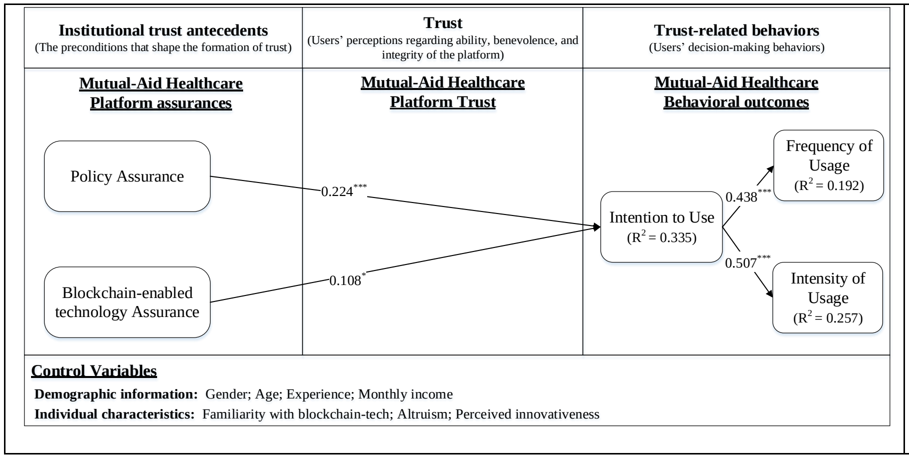
Model (a): Testing a Model With the Antecedent of Policy Assurance (With Mediators)


Institutional trust antecedents
(The preconditions that shape the formation of trust)
Trust
(Users' perceptions regarding ability, benevolence, and integrity of the platform)
Trust-related behaviors
(Users' decision-making behaviors)
Mutual-Aid Healthcare Platform assurances
Mutual-Aid Healthcare Platform Trust
Mutual-Aid Healthcare Behavioral outcomes
Policy Assurance
0.724***
Trust in the Platform ($R^2 = 0.667$)
0.361***
Intention to Use ($R^2 = 0.353$)
0.438***
0.510***
Frequency of Usage ($R^2 = 0.192$)
Intensity of Usage ($R^2 = 0.260$)
Control Variables
Demographic information: Gender; Age; Experience; Monthly income
Individual characteristics: Familiarity with blockchain-tech; Altruism; Perceived innovativeness

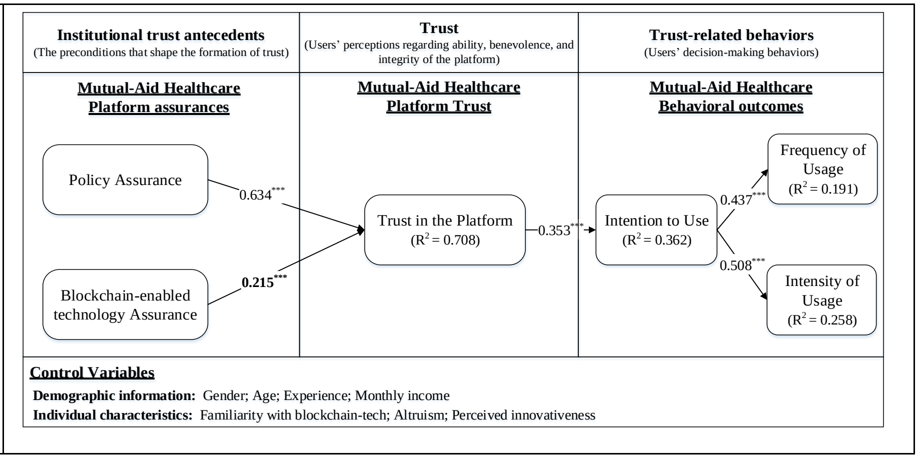
Model (b): Testing a Model With the Antecedent of Blockchain-Enabled Technology Assurance (With Mediators)


Institutional trust antecedents
(The preconditions that shape the formation of trust)
Trust
(Users' perceptions regarding ability, benevolence, and integrity of the platform)
Trust-related behaviors
(Users' decision-making behaviors)
Mutual-Aid Healthcare Platform assurances
Mutual-Aid Healthcare Platform Trust
Mutual-Aid Healthcare Behavioral outcomes
Blockchain-enabled technology Assurance
0.555***
Trust in the Platform ($R^2 = 0.436$)
0.362***
Intention to Use ($R^2 = 0.359$)
0.433***
0.511***
Frequency of Usage ($R^2 = 0.188$)
Intensity of Usage ($R^2 = 0.261$)
Control Variables
Demographic information: Gender; Age; Experience; Monthly income
Individual characteristics: Familiarity with blockchain-tech; Altruism; Perceived innovativeness

Model (c): Testing a Model With the Antecedents of Two Types of Assurances (Without Mediators)


Institutional trust antecedents
(The preconditions that shape the formation of trust)
Trust
(Users' perceptions regarding ability, benevolence, and integrity of the platform)
Trust-related behaviors
(Users' decision-making behaviors)
Mutual-Aid Healthcare Platform assurances
Mutual-Aid Healthcare Platform Trust
Mutual-Aid Healthcare Behavioral outcomes
Policy Assurance
0.224***
Blockchain-enabled technology Assurance
0.108*
Intention to Use ($R^2 = 0.335$)
0.438***
0.507***
Frequency of Usage ($R^2 = 0.192$)
Intensity of Usage ($R^2 = 0.257$)
Control Variables
Demographic information: Gender; Age; Experience; Monthly income
Individual characteristics: Familiarity with blockchain-tech; Altruism; Perceived innovativeness

Model (d): Testing a Model With the Antecedents of Two Types of Assurances (With Mediators)


Institutional trust antecedents
(The preconditions that shape the formation of trust)
Trust
(Users' perceptions regarding ability, benevolence, and integrity of the platform)
Trust-related behaviors
(Users' decision-making behaviors)
Mutual-Aid Healthcare Platform assurances
Mutual-Aid Healthcare Platform Trust
Mutual-Aid Healthcare Behavioral outcomes
Policy Assurance
0.634***
Blockchain-enabled technology Assurance
0.215***
Trust in the Platform ($R^2 = 0.708$)
0.353***
Intention to Use ($R^2 = 0.362$)
0.437***
0.508***
Frequency of Usage ($R^2 = 0.191$)
Intensity of Usage ($R^2 = 0.258$)
Control Variables
Demographic information: Gender; Age; Experience; Monthly income
Individual characteristics: Familiarity with blockchain-tech; Altruism; Perceived innovativeness

Appendix M: CMB Test

We conducted multiple tests to test the CMB issue, including the Harman one-factor test, the marker variable technique, and the full collinearity variance inflation factors (FCVIFs) (Kock & Lynn, 2012; Podsakoff et al., 2003; Williams et al., 2010). All criteria were satisfied, indicating that CMB is not a serious concern in the data, as shown below. First, we ran a Harman one-factor test (Podsakoff et al., 2003; Venkatesh et al., 2020) with unrotated factor analysis. The first factor extracted only 28.02% of the variance, thus reducing the concern about CMB in this study. Second, a marker variable technique was used (Williams et al., 2010). Specifically, we selected self-management of learning as a marker variable, referring to the extent to which an individual perceives he/she is self-disciplined and can engage in autonomous learning (Shao et al., 2022a). This marker variable is theoretically unrelated to the constructs in our research model (see Appendix G for detailed measurement items) (Lindell & Whitney, 2001; Venkatesh et al., 2020). The correlations between the marker variable and other constructs varied from -0.046 to 0.359, with an average correlation value of 1.320. We then added the marker variable to the research model and established its path relationship with each endogenous construct. A comparison analysis was conducted between the baseline model and the CMB test model after incorporating the marker variable. As noted in Table M1, the path coefficients do not differ significantly between the baseline model (without marker variable) and the CMB test model (with marker variable), and the marker variable has no significant influence on the endogenous variables (i.e., trust in the platform, intention to use, and actual usage behavior). Third, we assessed CMB using the full collinearity variance inflation factors (FCVIFs) (Kock & Lynn, 2012). The results show that FCVIFs vary from 1.045 to 2.922, which are lower than the threshold of 3.3. Overall, the above analysis demonstrates that CMB was not a serious concern in our study.

Table M1. PLS Marker Variable Approach

Path coefficients	Baseline model without marker variable	CMB test model with marker variable
PA→TP	0.634^{***}	0.641^{***}
BTA→TP	0.215^{***}	0.216^{***}
TP→IU	0.353^{***}	0.360^{***}
IU→USF	0.437^{***}	0.441^{***}
IU→USI	0.508^{***}	0.511^{***}
Control variables		
Gender→TP	0.010^{NS}	0.008^{NS}
Gender→IU	0.020^{NS}	0.019^{NS}
Age→TP	0.023^{NS}	0.021^{NS}
Age→IU	-0.013^{NS}	-0.013^{NS}
Income→TP	0.071^{NS}	0.075^{NS}
Income→IU	-0.025^{NS}	-0.023^{NS}
Experience→TP	0.109^{NS}	0.108^{NS}
Experience→IU	0.308^{***}	0.316^{***}
FBT→TP	0.016^{NS}	0.010^{NS}
FBT→IU	-0.024^{NS}	-0.028^{NS}
AL→TP	0.079^{NS}	0.077^{NS}
AL→IU	0.064^{NS}	0.060^{NS}
PI→TP	0.048^{NS}	0.046^{NS}
PI→IU	0.146^{*}	0.128^{*}
Marker variable		
Marker variable→TP	N/A	0.023^{NS}
Marker variable→IU	N/A	0.064^{NS}
Marker variable→USF	N/A	-0.033^{NS}
Marker variable→USI	N/A	-0.028^{NS}

Note: *** represents p <0.001; ** represents p <0.01; * represents p <0.05; NS represents not significant; PA represents policy assurance; BTA represents blockchain-enabled technology assurance; TP represents trust in the platform; IU represents intention to use; USF represents frequency of usage; USI represents intensity of usage; FBT represents familiarity with blockchain technology; AL represents altruism; PI represents perceived innovativeness.

Appendix N: Endogeneity Test

Specifically, Park and Gupta's (2012) Gaussian copula approach (Park & Gupta, 2012) controls for endogeneity by directly modeling the correlation between the potential endogenous variables (i.e., two structural assurances) and the error term by means of a copula. We first ran the Kolmogorov-Smirnov test with Lilliefors correction and confirmed that the two structural assurances are non-normally distributed (Sarstedt et al., 2020). Then we proceeded with the Gaussian copula approach and found that the Gaussian copulas included in our research model are nonsignificant on the relationships between two structural assurances, trust, and dependent variable (i.e., intention to use). Moreover, following Kock's (2022) guidelines, we created instrumental variables by incorporating the variation of policy and technology assurances as predictors of intention to use. These results yield small and non-significant coefficients, that is, -0.069 for the variation of policy assurance and -0.034 for the variation of technology assurance with $p > 0.1$. We thus conclude that endogeneity was not a serious issue in our study, providing support for the robustness of our structural model analysis (Hult et al., 2018).

Table N1. Results of the Gaussian Copula Approach

Relationship	**Original model**	**Gaussian Copula Model 1**	**Gaussian Copula Model 2**	**Gaussian Copula Model 3**	**Gaussian Copula Model 4**	**Gaussian Copula Model 5**	**Gaussian Copula Model 6**	**Gaussian Copula Model 7**
PA → TP	0.634 $(p < 0.001)$	0.568 $(p < 0.001)$	0.568 $(p < 0.001)$	0.568 $(p < 0.001)$	0.568 $(p < 0.001)$	0.568 $(p < 0.001)$	0.568 $(p < 0.001)$	0.568 $(p < 0.001)$
BTA → TP	0.215 $(p < 0.001)$	0.204 $(p < 0.001)$	0.204 $(p < 0.001)$	0.204 $(p < 0.001)$	0.204 $(p < 0.001)$	0.204 $(p < 0.001)$	0.204 $(p < 0.001)$	0.204 $(p < 0.01)$
TP → IU	0.353 $(p < 0.001)$	0.248 $(p < 0.01)$	0.256 $(p < 0.01)$	0.851 $(p < 0.05)$	0.266 $(p < 0.01)$	0.770 $(p < 0.05)$	0.883 $(p < 0.05)$	0.796 $(p < 0.05)$
GC (PA) → IU		-0.314 (p > 0.05)			-0.330 (p > 0.05)	-0.169 (p > 0.05)		-0.183 (p > 0.05)
GC (BTA) → IU			-0.471 (p > 0.05)		-0.493 (p > 0.05)		-0.491 (p > 0.05)	-0.500 (p > 0.05)
GC (TP) → IU				0.009 (p > 0.05)		-0.526 (p > 0.05)	-0.627 (p > 0.05)	-0.534 (p > 0.05)

Note: PA represents policy assurance; BTA represents blockchain-enabled technology assurance; TP represents trust in the platform; IU represents intention to use; GC represents Gaussian copula. The parentheses represent the *p*-value.

Appendix O: Mediation Test Results

Path			Direct effect	Confidence interval (95%)	Effect size	Indirect effect	Confidence interval (95%)	Effect size	Results
IV	Mediator	DV							
Indirect effects for paths with 2 segments									
PA	TP	IU	0.017	[-0.119, 0.154]	0.035	0.199^{***}	[0.026, 0.215]	0.077	Full mediation
BTA			0.048	[-0.088, 0.183]	0.024	0.067^{*}	[0.011, 0.114]	0.022	Full mediation
Indirect effects for paths with 3 segments									
PA	TP → IU	USF	0.008	[-0.104, 0.120]	0.001	0.143^{***}	[0.217, 0.367]	0.016	Full mediation
BTA		USF	-0.028	[-0.138, 0.082]	0.004	0.063^{*}	[0.001, 0.125]	0.007	Full mediation
PA		USI	-0.031	[-0.141, 0.079]	0.004	0.178^{***}	[0.116, 0.240]	0.017	Full mediation
BTA		USI	-0.083	[-0.193, 0.027]	0.007	0.077^{*}	[0.013, 0.141]	0.005	Full mediation

Note: PA represents policy assurance; BTA represents blockchain-enabled technology assurance; TP represents trust in the platform; IU represents intention to use; USF represents frequency of usage; USI represents intensity of usage. The significant value is confirmed with a 95% confidence interval excluding zero. $^{*}p < 0.05$; $^{***}p < 0.001$.

About the Authors

Zhen Shao is an associate professor of IS in the School of Economics and Management at Harbin Institute of Technology, Harbin, China. She previously worked as a visiting scholar in the Eller College of Management at the University of Arizona, USA. Her research primarily focuses on enterprise information systems assimilation, digital innovation, sharing economy, and digital trust. Her work has been published in academic journals, including *Production and Operations Management*, *European Journal of Information Systems*, *Information Systems Journal*, *Information & Management*, *Decision Support Systems*, *International Journal of Information Management*, *Journal of Enterprise Information Management*, *Electronic Commerce and Research Application*, *Internet Research*, *Behaviour & Information Technology*, *Computers in Human Behavior*, and *Industrial Management & Data Systems*, and has been presented at conferences including the INFORMS Annual Conference, International Conference on Information Systems, Americas Conference on Information Systems, the Hawaii International Conference on System Sciences, and the Pacific Asia Conference on Information Systems.

Lin Zhang is an associate professor of IS in the School of Management at Northwestern Polytechnical University, Xi'an, China. His research focuses on gamification in the electronic and mobile business, trust in the sharing economy, and IT adoption. He has published articles in journals such as *Production and Operations Management*, *European Journal of Information Systems*, *Decision Support Systems*, *Information & Management*, *Internet Research*, *Electronic Commerce Research and Applications*, and *Industrial Management & Data Systems*.

Susan A. Brown is the Stevie Eller Professor and department head of Management Information Systems at the University of Arizona's Eller College of Management, USA. She received her PhD from the University of Minnesota and an MBA from Syracuse University, USA. Her research interests focus on the antecedents and consequences of IT use by organizations and individuals. Her research has been published in top journals including *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Communications of the ACM*, *Journal of the Association for Information Systems*, and *Decision Support Systems*. She has served on the editorial boards of *MIS Quarterly*, *Information Systems Research*, *Journal of the Association for Information Systems*, and *Decision Sciences*. Susan was named an Association for Information Systems Fellow in 2017 and in 2024 became the editor-in-chief for *MIS Quarterly*.

Jose Benitez is a professor of IS, department chair of IS and Business Analytics, and the Bridgestone Endowed Chair in International Business at the Ambassador Crawford College of Business and Entrepreneurship, Kent State University, Kent, Ohio, USA. His research interests cover the impact of digital technologies and digitalization on companies and individuals and the development of theory and quantitative research methods in IS research. His research has been published in leading journals including *MIS Quarterly*, *Information Systems Research*, *Journal of Operations Management*, *Production and Operations Management*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, and *Decision Support Systems*. Jose was recognized as an Association for Information Systems (AIS) Distinguished Member Cum Laude in July 2021 and received the AIS Sandra Slaughter Service Award in December 2022. He is a senior editor of *European Journal of Information Systems*, *Information & Management*, and *Decision Support Systems* and an associate editor of *Journal of the Association for Information Systems*. He also serves as an editorial review board member for *Information Systems Research*.