Technological Forecasting & Social Change 224 (2026) 124495

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

journal homepage: www.elsevier.com/locate/techfore

# Restoring consumer trust in e-commerce: The role of blockchain technology and its behavioral implications

Louisa Uchikoshi[a], Björn Frank[a,*]

[a] *Faculty of Commerce, Waseda University, 1-6-1 Nishi-Waseda, Shinjuku-ku, Tokyo, 169-8050, Japan*

ARTICLE INFO

*Keywords:*
Blockchain
Consumer behavior
Online retail
Trust formation

ABSTRACT

Blockchain technology has unique technological features that could help e-commerce firms regain consumer trust lost due to widespread online fraud. However, their effectiveness and underlying mechanisms remain unknown. Drawing on trust formation theory, this article examines the effectiveness of these blockchain technology features and its variation across consumer needs. A multi-method approach combines a randomized between-subjects experiment (Study 1: 727 consumers; pretest: 45) and a multi-wave survey of actual experiences of tech-savvy consumers (Study 2: 563 consumers; pretest: 30) in the U.S. Consistent statistically significant results show that the blockchain technology features of privacy ownership, privacy monetization, and metadata transparency increase consumer trust in e-commerce platforms. The openness of a blockchain platform to criminal sellers, which allows consumers to access illicit products, increases trust only for consumers with illicit purchase needs, while decreasing trust for consumers without such needs. Trust mediates the effects of these blockchain technology features on consumers' willingness to pay additional fees and retail use intentions, which in turn mediate the effects on actual future retail use behavior. These findings extend trust formation theory to the context of blockchain technology and inform retail practitioners of a powerful new technology for increasing consumer purchases in their online stores.

## 1. Introduction

Trust is a key building block of society because all human interactions rely on it (Mazzella et al., 2016). Trust also has significant economic consequences (Sucher and Gupta, 2019). For example, firms involved in business scandals that violate stakeholder trust have experienced declining valuations (Herbas Torrico et al., 2018; Schumpeter, 2018). Many of these scandals involve breaches of consumer data on centralized online platforms, such as Amazon, Google, and Facebook. These breaches are facilitated by technological weaknesses, such as a lack of transparency regarding consumers' own data online, as well as by failures in centralized governance exercised by firms that have absolute control over consumer data (Garaus and Treiblmaier, 2021; Gefen et al., 2003).

Limited trust can create challenges for firms, such as consumers avoiding e-services that rely on trust. New technologies, such as blockchain and machine intelligence (Frank et al., 2021; Frank, 2024; Garaus and Treiblmaier, 2021; Shi et al., 2025; Wissawaswaengsuk et al., 2025), may be able to rebuild trust by empowering consumers and creating a better online user experience (Epstein, 2017). In particular, blockchain as a decentralized and secure technology may rebuild consumer trust (Ali et al., 2023; Gan and Lau, 2024; Zhong et al., 2020), as opposed to centralized institutions (e.g., banks, email service providers, and e-commerce platforms), which are vulnerable to hacking and manipulation (Crosby et al., 2016; Karamchandani et al., 2020). Blockchain technology is a distributed ledger or database that stores a large number of transactions in a chain structure. These transactions are highly secure due to the cryptographic capabilities of the blockchain (Gan and Lau, 2024; Völter et al., 2023). We posit that the blockchain has unique features that help firms using blockchain applications increase their consumers' trust. Our contribution to the literature is to identify these unique features and compare the effectiveness of consumer beliefs about these features, known as blockchain trusting beliefs, in building consumer trust in real-world blockchain technology applications. This would, in turn, provide firms with information on how to leverage the technology to increase their consumers' trust and purchases.

Most related research in the literature focuses on blockchain technology use cases, is conceptual, or uses a small set of interviews to draw

[*] Corresponding author.
*E-mail address:* frank@waseda.jp (B. Frank).

https://doi.org/10.1016/j.techfore.2025.124495
Received 10 December 2024; Received in revised form 17 November 2025; Accepted 9 December 2025
Available online 26 December 2025

conclusions (e.g., Ali et al., 2023; Kowalski et al., 2021). Meanwhile, robust empirical evidence of the mechanisms behind trust formation in a blockchain context is scarce (Marella et al., 2020; Völter et al., 2023). Furthermore, except for Garaus and Treiblmaier (2021), most related research focuses on main effects and neglects contingency factors (i.e., moderating effects) of trust formation in a blockchain context. In addition, previous literature on trust formation in blockchain contexts touts the positive effects of the privacy and transparency benefits of the technology on trust without addressing the possible contradictions of ensuring that data are private yet transparent. These contradictions need to be addressed and resolved.

To address these gaps in the literature, we apply trust formation theory (Mayer et al., 1995) to the novel context of blockchain technology. In this context, algorithms, rather than humans or human-supervised technology, autonomously manage processes. We decompose blockchain technology into its unique technological characteristics (specifically, privacy ownership, privacy monetization, metadata transparency, and illicit access) and highlight the role of consumer beliefs about these characteristics in trust formation. In doing so, we avoid overlap between the constructs of privacy and transparency. We also examine how the effects of these blockchain characteristics depend on consumers' personal values, an unexplored contingency factor. In addition, we link consumer trust in blockchain-based e-commerce (i.e., online retail platforms using blockchain) to consumer behavior. We empirically examine these effects using 1393 U.S. consumers' responses in two studies. Study 1 is an experiment, and Study 2 is a multi-wave survey of consumers' real-world experiences with such platforms.

## 2. Theoretical background

### 2.1. Definition and types of blockchain technology

From a functional perspective, the blockchain combines a database with a protocol (Casino et al., 2019). This type of database allows users to add information but not modify previous entries (Yang et al., 2020). Thus, if a user tries to modify information stored in the blockchain, which is difficult due to robust cryptographic algorithms, the integrity of the database will change, and all participating users will be aware of it (Yang et al., 2020). This makes blockchain technology a powerful tool for transparency (Ali et al., 2023; Roggeveen and Sethuraman, 2020).

### 2.2. The potential role of blockchain technology in building consumer trust in e-commerce

A lack of trust is the most significant barrier to e-commerce adoption (Hoffman et al., 1999; Wissawaswaengsuk et al., 2025). Current e-commerce business models rely on intermediaries (e.g., Amazon or E-Bay) to build consumer trust (Salam et al., 2003) by providing security. Consumers pay (sometimes hidden) transaction fees for this security (Marella et al., 2020). However, these intermediaries act as monopolies (West, 2022) and can undermine consumer trust through actions such as asking consumers to accept intensive data surveillance and promoting it as essential to personalized recommendations (West, 2022). This surveillance helps intermediaries like Amazon increase their market value at the expense of consumers' privacy and financial interests (Tangalakis-Lippert, 2022). In addition, a lack of transparency regarding how platforms like Amazon operate, how they use and profit from consumer data, and how they support regulatory efforts facilitates the manipulation of information (West, 2022). For example, centralized intermediaries can alter information in their online systems and create inauthentic electronic files without users' knowledge (Dai et al., 2017). Moreover, these centralized intermediaries are vulnerable to hacking (Crosby et al., 2016; Odiete et al., 2018) due to the existence of a single point of failure (Singh and Sharma, 2022). Consequently, centralized platforms amass data in massive repositories and fail to adequately protect users' personal data.

Blockchain could alleviate these problems by increasing transparency and eliminating the need for a centralized intermediary (Kamble et al., 2021; Wan et al., 2022; Wang et al., 2023). This would address consumer distrust of centralized intermediaries (Nakamoto, 2008). The blockchain keeps a record of every transaction or transfer. As a result, any expropriation or fraud can be detected by tracing it through the blockchain (Ali et al., 2023; Dai et al., 2017). The blockchain can offer solutions to consumers and firms, such as fraud prevention, supply chain transparency, payment transparency, consumer rewards, and data privacy (Gan and Lau, 2024; Garaus and Treiblmaier, 2021; Harvey et al., 2018). Thus, by increasing transparency, rewarding consumers, promoting data privacy, and eliminating fraud, the blockchain has the potential to change the nature of digital trust (Shin, 2019) (see Table 1). Our article is the first major empirical investigation of consumer beliefs about blockchain characteristics that influence trust formation in e-commerce (see Table 1).

### 2.3. The role of blockchain technology in building consumer trust: Theoretical underpinnings

In our article, we examine the role of blockchain technology in building consumer trust in an online retail context. Since consumers do not use the blockchain directly, but rather platforms powered by the blockchain, we focus on the context of blockchain-based e-commerce platforms, that is, retail marketplaces built on blockchain technology. In this context, we examine how specific of blockchain technology characteristics contribute to consumer trust formation. Although blockchain is a highly secure and transparent technology (Ali et al., 2023), online shopping always involves risk, particularly for consumers who lack experience with the online platform (Schlosser et al., 2006; Shi et al., 2025). Thus, to some extent, consumers may still perceive e-commerce platforms as risky, even if they use blockchain technology. However, we argue that blockchain reduces the perceived risk.

In consumer-seller relationships, trust can be defined as one party's (the consumer's) confidence in the reliability and integrity of the exchange partner (the seller, i.e., the blockchain-based e-commerce platform) (Cho, 2006). To explain trust formation in the context of blockchain-based e-commerce, we draw on Mayer et al.'s (1995) trust formation theory (also called the integrative model of trust) for two reasons. First, it is one of the most cited and well-established theories of trust formation (Shi et al., 2025). Second, unlike alternative theories, which are limited to technology as the object of trust, Mayer et al.'s (1995) trust formation theory places fewer restrictions on the object of trust. Thus, it fits the context of blockchain-based e-commerce, where consumers need to trust both the platform technology and the human sellers on the platform who interact with them within the platform's constraints and capabilities.

According to this theory, trust is determined by specific trusting beliefs regarding ability, benevolence, and integrity (Gefen et al., 2003; McKnight et al., 2002; Völter et al., 2023). Ability is defined as the skills and attributes that enable an entity (e.g., a person, firm, or technology) to have influence within a given area. Benevolence is when an entity is believed to be doing a favor for another party (e.g., a consumer) through services provided beyond an egocentric financial motive. Finally, the integrity of an entity is when another party (e.g., a consumer) perceives that entity as having a set of acceptable morals and standards (Mayer et al., 1995). In this article, we posit that the characteristics (privacy ownership, privacy monetization, and metadata transparency, as well as illicit access for consumers with illicit purchase needs but not for those without such needs) of blockchain-based e-commerce platforms can enhance consumer trust by conveying ability, benevolence, and integrity (see the conceptual model in Fig. 1). In addition to extending trust formation theory to the blockchain context, we offer new insights into the boundary conditions of this theory by integrating consumers' personal needs as a moderator. Based on Mayer et al.'s (1995) trust formation theory, and following past research on the trust-behavior relationship in

**Table 1**
Positioning in the empirical literature on trust formation in blockchain contexts.

| Year | Authors | Theory to explain trust formation | Method | Type of blockchain | Country | Sample size | Dependent variable | Effects of predictor variables | Moderators of these effects |
|---|---|---|---|---|---|---|---|---|---|
| 2019 | Shin | – | Survey (single data source, no time-lag) | Blockchain | n/a | 363 | Trust | Privacy (+), security (+) | – |
| 2020 | Marella et al. | Text content model (doc2vec model of discussion posts) | Semantic | Cryptocurrency technologies (i.e., the blockchain, cryptocurrency wallet, and exchanges) | n/a | 850 discussion posts related to Bitcoin | Trust in technology | Functionality (+), reliability (+), helpfulness (+) | – |
| 2020 | Shin & Bianco | – | Survey (single data source, no time-lag) | Blockchain media | n/a | 283 | Trust | Privacy (+), security (+) (mediated by confirmation of expectations) | – |
| 2021 | Garaus & Treiblmaier (Studies 2 and 3) | Integrative model of trust | Experiments | Blockchain-based food traceability system | Austria | 150 students (Study 2), 439 (Study 3) | Trust in the food retailer | Studies 2 and 3: blockchain-based (vs. non-blockchain, firm-owned) food traceability system (+) | Study 3: retailer familiarity (−), blockchain benefit disclosure (+) |
| 2021 | Joo & Han | – | Survey (single data source, no time-lag) | Blockchain-based food supply chain | China | 318 | Trust | Transparency (+), traceability (+), security (+) | – |
| 2021 | Kowalski et al. | – | In-depth interviews | Blockchain technology in trade finance | n/a | 7 | Trust | No statistical tests: security, benevolence, efficiency/quality of communication, predictability of trade partners | – |
| 2022 | Koroma et al. | Trust transfer theory | Survey (single data source, no time-lag) | Blockchain cryptocurrency | Mano river union states (MRU) | 421 | Trust in cryptocurrency | Technology attachment (+), blockchain transparency (+) | – |
| 2022 | Shao et al. | Trust transfer theory | Survey (single data source, no time-lag) and interviews | Blockchain-enabled healthcare mutual aid platform | China | 213 students | Trust transfer (trust in members, trust in technology, trust in platform) | Platform mechanisms: member credibility (+), blockchain certificate (+), structural assurance (+) | – |
| 2023 | Ali et al. | – | Semi-structured interviews | Blockchain | n/a | 14 | Trust | No statistical tests: reliability, integrity, tamper-proofing, immutability, versatility, transparency, privacy | – |
| 2023 | Liu et al. | Signal theory, trust transfer theory | Survey (single data source, no time-lag) | Blockchain | China | 474 | Digital trust, swift trust | Blockchain experience (+), environmental information transparency perceived (+) | – |
| 2023 | Völter et al. | Trust signals | Between-groups experiment and interviews | Inter-organizational private blockchain | U.K. | 80 students | Trust in blockchain implementations | Familiarity (n.s.), complete transparency of information (+), interaction history and network effects (+) | – |
| 2025 | This article | Integrative model of trust | Study 1: experiment; Study 2: survey (multiple data sources, time-lag) | Blockchain-based e-commerce (public blockchains) | USA | 1393 | Technology trust: competence, benevolence and integrity | Trust-building technology: privacy ownership (+), privacy monetization (+), metadata transparency (+), illicit access (+/−) | Illicit purchase needs (+) |

Notes: (+) / (−) / (n.s.): positive / negative / non-significant effect. n/a: information not available in article.

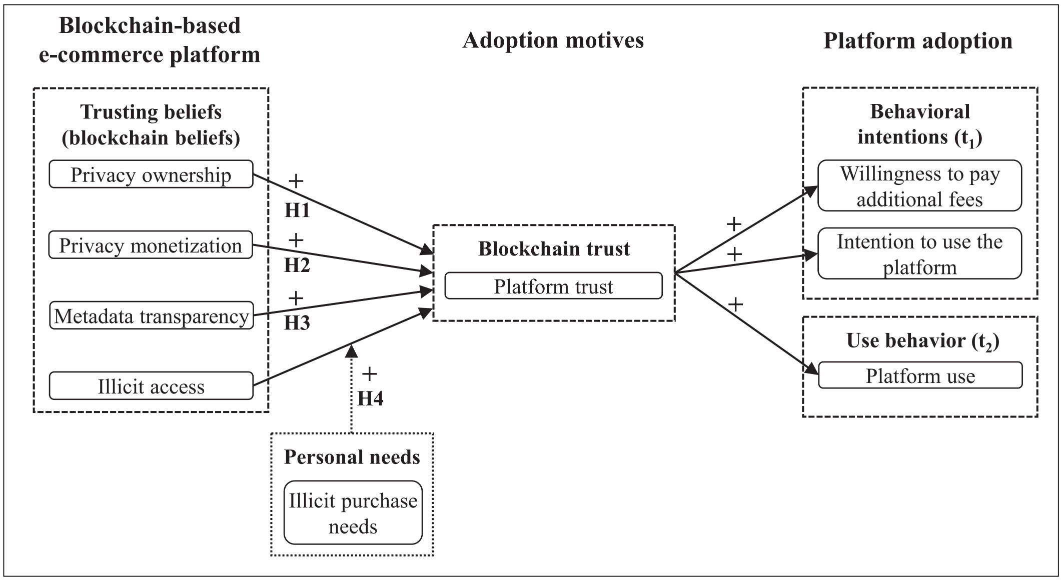

**Fig. 1.** Conceptual model and hypotheses.

general (Shi et al., 2025) and in other blockchain contexts (Gan and Lau, 2024; Garaus and Treiblmaier, 2021), we demonstrate that trust positively influences consumers' intentions and behavior in the context of blockchain-based e-commerce.

## 3. Development of hypotheses

*Trust in blockchain-based e-commerce*. According to trust formation theory (Mayer et al., 1995), trust is one party's willingness to expose itself to (i.e., allow itself to be vulnerable to) the actions of another party, despite an inability to monitor or control the latter, based on the expectation that the latter will perform an important action. We assume the same principle applies in a blockchain context because blockchain functions similarly to an organization where people are replaced by consensus algorithms and nodes that agree on transactions within a shared infrastructure. Therefore, trust is placed in the technology itself (i.e., the algorithms) (Odiete et al., 2018), which is operated by people (i.e., the nodes). According to trust formation theory, an entity's ability, integrity, and benevolence drive trust in that entity (e.g., a platform using blockchain technology). Thus, we examine how consumers' beliefs about blockchain characteristics, including privacy ownership, privacy monetization, metadata transparency, and illicit access, affect their trust by reflecting the perceived ability, integrity, and benevolence of the blockchain.

*Privacy ownership*. Privacy ownership is the right to possess and control (e.g., encrypt) one's personal data. However, individual data ownership rights are not yet recognized in any jurisdiction (Hummel et al., 2021). In the absence of legal protection and enforcement, blockchain technology, with its decentralized structure and cryptography-based security (Rejeb et al., 2020), can provide a technical means of protecting and enforcing privacy ownership. It can do this better than centralized technologies (Ziccardi, 2012). Using the terminology of trust formation theory (Mayer et al., 1995), this represents an ability that a blockchain-based platform provides to its users. An ability is the possession of skills and attributes that enable a technology to have influence within a certain area (Mayer et al., 1995). In this sense, blockchain has an ability that allows users to own and control their data (Casino et al., 2019). In addition, users believe they have a moral right to own (i.e., possess and control) their data (Hummel et al., 2021). Therefore, users may view the role of the blockchain in selflessly protecting and enforcing this right to privacy ownership without any financial motive as both an act of integrity reflecting acceptable morals and standards and an act of benevolence or favor without selfish (e.g., financial) motives (Mayer et al., 1995). Since trust formation theory considers an entity's ability, benevolence, and integrity to be key drivers of trust in that entity (Mayer et al., 1995), we posit that privacy ownership will increase consumer trust in blockchain-based e-commerce platforms.

**H1**. Privacy ownership has a positive effect on platform trust.

*Privacy monetization*. Privacy monetization is the ability of users to sell access to their private data to another party, such as a store or third party on an e-commerce platform. Blockchain platforms tend to offer users the option to monetize their privacy. In contrast, centralized platforms (e.g., Amazon) do not offer this option, preferring instead to pocket a (mostly hidden) profit margin from store owners and third parties for access to the platform and user data (Odiete et al., 2018; Rejeb et al., 2020). Specifically, blockchain platforms protect user data and allow users to monetize these by sharing them with parties selected by the user (Harris, 2020). In other words, blockchain platforms enable users to capture the value of their participation (Casino et al., 2019). Using the terminology of trust formation theory (Mayer et al., 1995), users perceive the privacy monetization feature as a platform ability and a benevolent act reflecting integrity. This is because centralized platforms selfishly profit from user data instead of doing the ethically right thing and letting users profit from their own data. Benevolence involves caring for another party (e.g., a consumer), not having self-interest, and not benefiting from the relationship, while integrity reflects a set of acceptable morals and standards (Mayer et al., 1995). Since consumers are likely to view the presence of data monetization functionality as an ability and an expression of benevolence and integrity, all of which trust formation theory posits influence trust (Mayer et al., 1995), we predict that privacy monetization will increase consumer trust in blockchain-based e-commerce platforms.

**H2**. Privacy monetization has a positive effect on platform trust.

*Metadata transparency*. Metadata are data that describe other data. In a blockchain, metadata convey important information about a transaction, such as the anonymous IDs of the users involved, without revealing their identities or personal data, such as purchase history or home address (Benisi et al., 2020), which are the only data worth monetizing. Transparency is the presentation of detailed data. Transparency enables accountability and enhances the legitimacy of a given entity by showing how and why decisions are made and by which actors

(Gillman, 2023). Metadata transparency means that metadata are publicly available (i.e., not hidden or restricted to involved parties), making them transparent. Unlike centralized platforms (e.g., Amazon), blockchain platforms tend to provide metadata transparency. Transparent metadata can provide insight into anonymous transaction aspects (e.g., anonymous user IDs), and changes to metadata (e.g., user IDs) and publicly available data (e.g., edited product reviews). Using the terminology of trust formation theory (Mayer et al., 1995), users may perceive transaction tracking and real-time access to changes to metadata (e.g., user IDs) and publicly published data (e.g., online reviews) (Odiete et al., 2018) as an indication of both the ability and benevolence of an e-commerce platform. This is because public visibility of such information may help users make purchase decisions (i.e., an ability) without requiring compensation in return (i.e., benevolence) (Mende and Noble, 2019). Users may also perceive metadata transparency, which provides public access to metadata rather than hiding it, as an act of honesty and sincerity and, thus, integrity. Since users are thus likely to perceive metadata transparency as an ability, benevolence, and integrity, which trust formation theory posits influence trust (Mayer et al., 1995), we predict a positive effect of metadata transparency on consumer trust in blockchain-based e-commerce platforms.

**H3.** Metadata transparency has a positive effect on platform trust.

*The moderating effect of illicit purchase needs on the effect of illicit access on trust.* Illicit access is unrestricted access for consumers to use a platform to obtain illicit products from criminal sellers. In contrast, restricted access, such as on Amazon or Google Play, allow access only to approved sellers and aims to prevent illicit products and criminal sellers. Open blockchains, the technological basis for illicit access, allow unrestricted access for developers, sellers, and consumers (Eisenmann et al., 2009; Kwon and Shao, 2021). This unrestricted access allows sellers of illicit products to join the platform and hide their identity, facilitating consumers' access to illicit product offerings (Marella et al., 2020).

We argue that a consumer's illicit purchase needs (i.e., need for illicit products: Kim et al., 2009) moderates the extent to which illicit access contributes to consumer trust in a platform. Using the terminology of trust formation theory (Mayer et al., 1995), consumers with illicit purchase needs may interpret illicit access as an indication of the blockchain platform's ability to provide access to necessary illicit products, its benevolence in selflessly respecting consumers' needs without profiting itself, and its integrity in defending consumers' moral right to access needed products. According to trust formation theory (Mayer et al., 1995), the perception of higher ability, benevolence, and integrity increases trust. In contrast, people without illicit purchase needs may perceive illicit access as the blockchain platform's lack of ability to block criminals, its lack of benevolence in selfishly attracting traffic to the platform by facilitating criminal activity, and its lack of integrity in failing to defend consumers' moral right to have criminals blocked. Based on trust formation theory (Mayer et al., 1995), the perception of lower ability, benevolence, and integrity would reduce such consumers' trust in the platform.

**H4.** Illicit purchase needs positively moderate the positive effect of illicit access on platform trust, such that illicit access has a positive effect on platform trust for consumers with illicit purchase needs, while it has a negative effect on platform trust for consumers without illicit purchase needs.

## 4. Study 1: experiment

### 4.1. Method: experimental design

*Design.* Study 1 has a 2 (privacy ownership: low vs. high) × 2 (privacy monetization: low vs. high) × 2 (metadata transparency: low vs. high) × 2 (illicit access: low vs. high) between-subjects design. We conducted an experiment to test our hypotheses and establish the causal nature of our proposed effects.

*Manipulation of blockchain technology features.* We randomly assigned participants to one of sixteen scenarios (privacy ownership × privacy monetization × metadata transparency × illicit access, each high or low). Each scenario contained the same general description of OpenCommerce, a peer-to-peer e-commerce site that uses blockchain technology and, unlike Amazon, is not operated by a single firm that mediates transactions between consumers and sellers. We then described the characteristics of OpenCommerce, manipulating the level of blockchain technology features. Appendix 1 includes these descriptions and manipulations. Appendix 2 includes our measures of demographics, personal needs, trust, use intentions, and intentions to pay additional fees to use blockchain-based e-commerce.

### 4.2. Data collection and sample

We targeted consumers in the U.S. because it has the largest economy and individualistic consumers may care more about privacy ownership (H1) and act more in accordance with their personal needs (H4) than collectivist consumers, who may prioritize group needs.

First, we conducted a pretest using data collected from 45 consumers on MTurk, a well-established U.S. crowdsourcing platform operated by Amazon that is frequently used for consumer research. After ensuring the validity of our measures, we recruited respondents from MTurk for our actual experiment in March 2021 using random sampling. The literature suggests that MTurk participants are highly diverse, more so than a sample of university students (Buhrmester et al., 2011). Furthermore, MTurk data are of equal or better quality than data collected in a laboratory setting, from professional online panels, and using marketing research firms (Buhrmester et al., 2011; Kees et al., 2017). These data are representative of our target population: regular U. S. consumers who are web-savvy and likely to shop online. To rule out data generated by bots or respondents faking a U.S. location with a spoofed IP address, we included attention checks (approved by our university prior to data collection) that verified correct identification of image content, comprehension of text, and roughly correct English in open-ended responses. Our data collection was anonymous and met institutional requirements for informed consent and ethics.

There were 727 responses. 84 % of the respondents were full-time employees, distinguishing our sample from pure student samples. This demonstrates the respondents' financial ability to make purchases on e-commerce platforms, which aligns with our study objectives. Just over half of the respondents were male, most were relatively young, and most had at least a bachelor's degree. These characteristics align with the growing popularity of cutting-edge technologies such as blockchain among male, young, and well-educated consumers, matching the profile of early technology adopters (Frank et al., 2015). Therefore, the sample is consistent with our study objectives.

### 4.3. Data validity

*Convergent and discriminant validity.* The results of a confirmatory factor analysis (CFA) ($\chi^2$/df = 3.99, CFI = 0.95, RMSEA = 0.06, upper limit (UL) of 90 % RMSEA confidence interval (CI) = 0.07) meet the criteria for a high goodness-of-fit of the model ($\chi^2$/df < 5, CFI ≥ 0.95, RMSEA ≤0.07, UL of 90 % RMSEA CI ≤ 0.1) (Hair et al., 2010). Moreover, as shown in Table 2, all values of average variance extracted (AVE), Cronbach's α, and composite reliability (CR) meet the convergent validity criteria (AVE > 0.5, α > 0.7, CR > 0.7). All items loaded significantly on their respective constructs with a loading of 0.7 or higher. Moreover, the AVE for each construct was greater than the squared correlations with all other constructs, demonstrating discriminant validity (Hair et al., 2010). To further evaluate discriminant validity, we used the method proposed by Rönkkö and Cho (2022). We compared the UL of the 95 % CI of all factor correlations in the CFA model with threshold values: severe (UL ≥ 1), moderate (0.9 ≤ UL < 1),

**Table 2**
Correlations and descriptive statistics of multi-item constructs (Study 1 and Study 2).

| | Correlations | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Variables | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Platform trust | | 0.71 *** | 0.30 *** | 0.34 *** | 0.03 | −0.06 | 0.56 *** | 0.38 *** |
| Privacy ownership | 0.24 *** | | 0.36 *** | 0.37 *** | 0.09 * | 0.04 | 0.57 *** | 0.37 *** |
| Privacy monetization | 0.10 ** | 0.02 | | 0.63 *** | 0.49 *** | 0.34 *** | 0.17 *** | 0.28 *** |
| Metadata transparency | 0.10 ** | −0.02 | 0.00 | | 0.42 *** | 0.28 *** | 0.26 *** | 0.28 *** |
| Illicit access | −0.04 | −0.03 | −0.02 | 0.03 | | 0.59 *** | 0.01 | 0.21 *** |
| Illicit purchase needs | 0.40 *** | 0.05 | 0.07 * | 0.07 | 0.03 | | −0.06 | 0.22 *** |
| Intention to use the platform | 0.64 *** | 0.10 ** | 0.10 ** | 0.08 * | −0.04 | 0.50 *** | | 0.31 *** |
| Willingness to pay additional fees | 0.60 *** | 0.07 | 0.08 * | 0.08 * | −0.03 | 0.65 *** | 0.76 *** | |
| *Descriptive statistics (Study 1)* | | | | | | | | |
| Cronbach's α | 0.85 | 0.93 | 0.92 | 0.94 | 0.94 | 0.95 | 0.92 | 0.92 |
| Average variance extracted (AVE) | 0.59 | 0.73 | 0.80 | 0.77 | 0.80 | 0.87 | 0.80 | 0.86 |
| r (highest (positive or negative) correlation) | 0.64 | 0.24 | 0.10 | 0.10 | 0.04 | 0.65 | 0.76 | 0.65 |
| $r^2$ (highest squared correlation) | 0.41 | 0.06 | 0.01 | 0.01 | 0.00 | 0.42 | 0.58 | 0.42 |
| Convergent validity (α > 0.7 and AVE > 0.5) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Discriminant validity (AVE > $r^2$) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Number of measurement items | 4 | 5 | 3 | 5 | 4 | 3 | 3 | 2 |
| *Descriptive statistics (Study 2: first wave only)* | | | | | | | | |
| Cronbach's α | 0.88 | 0.91 | 0.95 | 0.93 | 0.97 | 0.96 | 0.88 | 0.91 |
| Average variance extracted (AVE) | 0.65 | 0.64 | 0.82 | 0.73 | 0.88 | 0.88 | 0.70 | 0.84 |
| r (highest (positive or negative) correlation) | 0.71 | 0.71 | 0.63 | 0.63 | 0.59 | 0.59 | 0.57 | 0.38 |
| $r^2$ (highest squared correlation) | 0.50 | 0.50 | 0.40 | 0.40 | 0.35 | 0.35 | 0.32 | 0.14 |
| Convergent validity (α > 0.7 and AVE > 0.5) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Discriminant validity (AVE > $r^2$) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Number of measurement items | 4 | 6 | 4 | 5 | 4 | 3 | 3 | 2 |

Notes: *$p < .05$; **$p < .01$; ***$p < .001$ (two-sided $p$-values). The correlations of Study 1 (sample size: 727) are below the diagonal, and those of Study 2 (sample size: 563) are above the diagonal.

marginal (0.8 ≤ UL < 0.9), and no problem (UL < 0.8). Our results indicate no problem (UL < 0.8) for nearly all factor correlations, and two marginal (i.e., insignificant) discriminant validity issues, where the interpretation as distinct constructs is "probably safe" (Rönkkö and Cho, 2022). These issues include a manipulation check measure not used in hypothesis testing (UL = 0.84 < 0.9) and the distinction between our two alternative measures of behavioral intention (i.e., the same construct) (UL = 0.86 < 0.9). Neither issue compromises the validity of the measures used to test our hypotheses.

*Manipulation checks*. We ran a one-way ANOVA for each manipulated variable, using the standardized values of the perceptual measures reported in Appendix 2. All results showed a significant effect in the expected direction, confirming the success of manipulating privacy ownership ($F(1, 725) = 134.70$, $p < .001$, $\eta_p^2 = 0.16$, $M_{low} = -0.40$, $M_{high} = 0.39$), privacy monetization ($F(1, 725) = 157.90$, $p < .001$, $\eta_p^2 = 0.18$, $M_{low} = -0.43$, $M_{high} = 0.42$), metadata transparency ($F(1, 725) = 158.33$, $p < .001$, $\eta_p^2 = 0.18$, $M_{low} = -0.40$, $M_{high} = 0.43$), and illicit access ($F(1, 725) = 167.54$, $p < .001$, $\eta_p^2 = 0.19$, $M_{low} = -0.49$, $M_{high} = 0.41$).

*Common method bias (CMB)*. Our experimental method avoids CMB when testing our hypotheses. To test for CMB in the remaining variables, we used the marker variable technique (Podsakoff et al., 2003) with a three-item community ethics scale (see Appendix 2) as a marker of method variance. This scale measures the extent to which an individual's community expects him or her to behave ethically (Shafer, 2002). Using the method by Podsakoff et al. (2003) and Williams et al. (2010), we tested for CMB by comparing CFA models with marker variables. Since there is no statistically significant difference between model-u and model-r (df = 28, $p > .1$), any potential CMB would not bias the results regarding the relationships between constructs in our model.

### 4.4. Hypothesis tests

*Type of analysis*. To test our hypotheses, we performed a 2 × 2 × 2 × 2 analysis of covariance (ANCOVA) and a corresponding regression. We used trust as the dependent variable, dummy variables for the four manipulated variables and their interaction effects as well as illicit purchase needs and their interaction with illicit access as the independent variables, and the consumer's gender and education level as the control variables. We standardized all variables before calculating the interaction effects. Since all variance inflation factors are below 1.1, multicollinearity is not a concern (Mason and Perreault, 1991).

*Antecedents of trust*. Table 3 shows the results of our regression analysis after eliminating (through the backward selection method) all the higher-order interactions between the blockchain technology features, all of which were insignificant. This suggests that the different blockchain technology features act independently in building trust. Based on the adjusted $R^2$, the model explains 22.9 % of the variance in trust. This suggests that blockchain features affect trust, yet they do not fully account for the remaining variance. Thus, e-commerce platforms require supplementary trust-building measures alongside blockchain technology. Our hypothesis tests confirm that privacy ownership, privacy monetization, and metadata transparency positively affect trust, supporting H1-H3. Illicit access positively affects trust for consumers with illicit purchase needs (i.e., one standard deviation above the mean) and negatively affects trust for consumers without such needs (i.e., one standard deviation below the mean), supporting H4. Regarding the control variables, education and illicit purchase needs positively affect trust, but gender does not. The left side of Fig. 2 visualizes this interaction effect. An ANCOVA leads to the same conclusions as our regression analysis.

*Consequences of trust*. Table 4 presents the results of multiple regression analyses about the consequences of trust, as predicted by our conceptual model (see Fig. 1). They show positive effects of consumers'

**Table 3**
The mechanisms of consumer trust formation in blockchain-based e-commerce.

| | Study 1: Experiment | | Study 2: Survey | |
|---|---|---|---|---|
| Dependent variable: | Platform trust | | Platform trust | |
| Independent variables | β | | β | |
| *Control variables* | | | | |
| Intercept | −0.002 | | −0.075 | * |
| Female (1; male: 0) gender | −0.023 | | −0.021 | |
| Education | 0.112 | *** | 0.015 | |
| Illicit purchase needs | 0.352 | *** | −0.161 | *** |
| Illicit access | −0.037 | | −0.031 | |
| *Main effects of technology characteristics* | | | | |
| Privacy ownership (H1: +) | 0.227 | *** | 0.639 | *** |
| Privacy monetization (H2: +) | 0.065 | * | 0.081 | * |
| Metadata transparency (H3: +) | 0.088 | ** | 0.095 | * |
| *Moderating effect* | | | | |
| Illicit purchase needs × Illicit access (H4: +) | 0.066 | * | 0.127 | *** |
| *Fit statistics* | | | | |
| Adjusted $R^2$ | 0.229 | | 0.528 | |
| Sample size | 727 | | 563 | |

Notes: Regression analysis. *$p$ < .05; **$p$ < .01; ***$p$ < .001 (two-sided). All variables standardized before calculating interaction terms. Effects of standardized variables and their interaction terms. Technology characteristics coded as 1/0 (high/low) in Study 1 (experiment) and as a perceptual score in Study 2 (survey).

trust in e-commerce platforms on their intention to use the platforms (explaining 41 % of the variance) and their willingness to pay additional fees if the platforms were not free (explaining 37.7 % of the variance). Among the control variables, education positively affects both dependent variables, while female gender positively affects only the willingness to pay additional fees.

*Mediation analysis.* Using bootstrapping tests, we confirmed that platform trust significantly ($p$ < .05) mediates the effects of privacy ownership (H1), privacy monetization (H2), and metadata transparency (H3) on platform usage intentions and willingness to pay additional fees. Therefore, blockchain technology features affect behavioral intentions through the hypothesized trust mechanisms.

### *4.5. Robustness tests*

We conducted a robustness test using formative rather than reflective measures. Instead of using factor analysis, we calculated the mean across the items of each construct and included these variables in the regression models. This yielded very similar results, which further validated the hypotheses. For an additional robustness test, we included additional control variables, namely age, occupation, income, and blockchain knowledge, and ran the same regression to test our hypotheses. The results were very similar, confirming our main findings. In another robustness test, instead of testing our hypothesis with dummy variables, we ran a regression using the standardized extracted factors of our perceptual measures (see Appendix 2) of the independent variables that we originally measured for the manipulation checks. All the results remained consistent in terms of significance and direction.

### *4.6. Discussion*

Study 1 confirms that privacy ownership, privacy monetization, metadata transparency, and the interaction effect of illicit access and consumers' illicit purchase needs collectively explain ordinary, not necessarily blockchain-savvy consumers' trust in blockchain-based e-commerce platforms. This trust, in turn, mediates the effects on consumers' intention to use the platform and their willingness to pay additional fees if the platform were not free. In Study 1, the controlled experimental design with random assignment of participants eliminated potential biases and provided evidence for the causal nature of the hypothesized effects. However, Study 1 does not reflect consumers' actual experiences, since most ordinary consumers have not yet used blockchain platforms. To address this, we conducted Study 2, which included a multi-wave survey of consumers' actual experiences with blockchain-based e-commerce platforms. Study 2 also tested whether the hypothesized mechanisms affect not only consumers' behavioral intentions, but also their actual future behavior.

## 5. Study 2: multi-wave survey

### *5.1. Method: multi-wave survey*

To test our hypotheses, we designed a survey for consumers who had used a blockchain-based e-commerce platform at least once. A qualifying question ensured that respondents without such experience were excluded from the survey. We asked all respondents to rate a specific blockchain-based e-commerce platform, using the same measures as in Study 1 (see Appendix 2). Since different platforms exhibit significant differences in the intensity of the four blockchain technology features, such as the privacy monetization opportunities offered and the degree of illicit access, and since consumer trust is influenced by how consumers subjectively perceive a platform, we measured the blockchain technology features (H1-H4) through the perceptual measures used in Study 1 for the manipulation checks.

To test the power of our theoretical mechanisms to predict actual consumer behavior, we conducted a second survey wave ($t_2$) eight months after the first wave, asking participants about their use of the platform since the first wave ($t_1$). This lag allows time for psychological processes to translate into action, for product-related needs to emerge, and for consumers to seek ways to address and satisfy those needs. Our measures can be found at the end of Appendix 2.

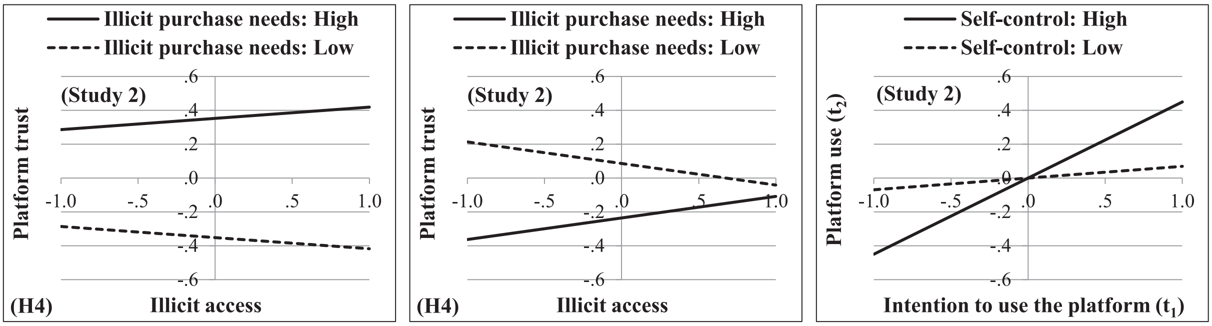

**Fig. 2.** Visualized moderating effects.

**Table 4**
The effect of consumers' platform trust on their platform adoption.

| | | Study 1: Experiment | | Study 2: Survey ($t_1$) | | Study 2: Follow-up survey ($t_2$) | |
|---|---|---|---|---|---|---|---|
| | Dependent variables: | Willingness to pay additional fees | Intention to use the platform | Willingness to pay additional fees | Intention to use the platform | Platform use ($t_2$) | Platform use ($t_2$) |
| Independent variables | | β | β | β | β | β | β |
| *Control variables* | | | | | | | |
| Intercept | | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | −0.007 |
| Female (1; male: 0) gender | | −0.059* | −0.044 | −0.040 | −0.019 | −0.035 | −0.083 |
| Education | | 0.152*** | 0.061* | 0.069 | −0.026 | −0.002 | 0.034 |
| Low self-control | | | | | | | 0.197 |
| *Main effects* | | | | | | | |
| Platform trust | | 0.565*** | 0.625*** | 0.374*** | 0.558*** | 0.224* | |
| Intention to use the platform | | | | | | | 0.259* |
| *Moderating effect* | | | | | | | |
| Low self-control × Intention to use the platform | | | | | | | −0.190* |
| *Fit statistics* | | | | | | | |
| Adjusted $R^2$ | | 0.377 | 0.410 | 0.148 | 0.308 | 0.022 | 0.086 |
| Sample size | | 727 | 727 | 563 | 563 | 103 | 103 |

Notes: Regression analysis. *$p < .05$; **$p < .01$; ***$p < .001$ (two-sided). All variables standardized before calculating interaction terms. Effects of standardized variables and their interaction terms.

### 5.2. Data collection and sample

First, we collected data from 30 consumers for a pretest through Measure Protocol, a market research firm that uses and promotes blockchain technology (Dynata, 2020). It distributed our survey via random sampling, providing us with access to consumers experienced in blockchain-based e-commerce who are representative of our target population. The test survey included several attention controls (e.g., reverse-coded items, open-ended questions, time spent on the survey, and details about experience with blockchain-based e-commerce) and varied the question order. We then improved the survey to focus respondents' attention on the most critical variables of our research model.

Afterwards, from April to May 2021, we collected data for the first wave of our survey ($t_1$) from various blockchain user/developer-related social media groups (Facebook, LinkedIn, Twitter, Instagram, Telegram, Reddit, and Discord) and, using random distribution, from Measure Protocol. This approach provided access to a wide range of actual blockchain users. Our data collection resulted in a sample of 563 observations. Eight months later, in December 2021, we collected data for the second wave of our survey ($t_2$) by re-contacting respondents, resulting in a sample of 103 observations. The sample profile is very similar to that of Study 1 and consistent with our study objectives. Most respondents were full-time employees, just over half were male, most were relatively young, and the majority had at least a bachelor's degree. This is consistent with the expected profile of early adopters of a technology like blockchain (Frank et al., 2015). The demographic distribution of both waves of Study 2 was similar, suggesting that attrition in the second wave was not biased toward any particular demographic.

### 5.3. Data validity

*Convergent and discriminant validity*. As shown in Tables 2 (first wave) and Table 5 (second wave), all values of AVE, Cronbach's α, and CR meet the convergent validity criteria (AVE > 0.5, α > 0.7, CR > 0.7). Moreover, the AVE values of all constructs surpass the squared correlations with all other constructs, which confirms the discriminant validity of all constructs (Hair et al., 2010). In addition, the results of a CFA ($\chi^2$/df = 2.36, CFI = 0.97, RMSEA = 0.05, UL of the 90 % RMSEA CI = 0.05) meet the criteria for a high goodness-of-fit of the model ($\chi^2$/df < 5, CFI ≥ 0.95, RMSEA ≤0.07, upper bound of the 90 % RMSEA confidence interval ≤ 0.1) (Hair et al., 2010). As an additional test of discriminant validity (Rönkkö and Cho, 2022), we compared the UL of the 95 % CI of all factor correlations in the CFA model with threshold values: severe (UL ≥ 1), moderate (0.9 ≤ UL < 1), marginal (0.8 ≤ UL < 0.9), and no problem (UL < 0.8). The results indicate no problem for any of the factor correlations except for one marginal (i.e., non-significant) discriminant validity issue (UL = 0.86 < 0.9). Regarding this marginal issue, interpreting privacy concern and trust as distinct constructs is "probably safe" (Rönkkö and Cho, 2022). Moreover, H1 provides theoretical support for a very strong effect, rather than a measurement problem.

**Table 5**
Correlations and descriptive statistics of multi-item constructs (Study 2: wave 2 and related variables measured in wave 1).

| | Correlations | | | |
|---|---|---|---|---|
| Variables | 1 | 2 | 3 | 4 |
| 1 Platform trust ($t_1$) | | | | |
| 2 Intention to use the platform ($t_1$) | 0.58*** | | | |
| 3 Platform use ($t_2$) | 0.22* | 0.26** | | |
| 4 Low self-control ($t_1$) | 0.04 | −0.04 | 0.12 | |
| *Descriptive statistics* | | | | |
| Cronbach's α | 0.88 | 0.88 | 0.78 | 0.86 |
| Average variance extracted (AVE) | 0.65 | 0.70 | 0.64 | 0.68 |
| r (highest (positive or negative) correlation) | 0.58 | 0.58 | 0.26 | 0.12 |
| $r^2$ (highest squared correlation) | 0.34 | 0.34 | 0.07 | 0.01 |
| Convergent validity (α > 0.7 and AVE > 0.5) | Yes | Yes | Yes | Yes |
| Discriminant validity (AVE > $r^2$) | Yes | Yes | Yes | Yes |
| Number of measurement items | 4 | 3 | 2 | 3 |

Notes: *$p < .05$; **$p < .01$; ***$p < .001$ (two-sided $p$-values). Sample size: 103.

*CMB*. We collected data from the same respondents with an eight-month interval, which significantly reduces or even eliminates CMB. To test for CMB in the first wave, we compared CFA models with marker variables (Podsakoff et al., 2003; Williams et al., 2010), using the same marker variable as in Study 1. Since there is no statistically significant difference between model-u and model-r (df = 28, $p > .1$), any potential CMB would not bias the results regarding construct relations.

### 5.4. Hypothesis tests

*First survey wave: Antecedents of trust*. We used the same regression analysis as in Study 1, but with perceptual measures of blockchain features rather than dummy variables. Table 3 presents the results. The variance inflation factors are all less than two, indicating that multicollinearity is not a concern (Mason and Perreault, 1991). Once again, the blockchain features have no significant interactions with each other in influencing trust. As in Study 1, privacy ownership, privacy monetization, and metadata transparency positively affect platform trust, thus supporting H1-H3. Illicit access has a positive effect for consumers with illicit purchase needs and a negative effect for consumers without such needs, as shown in Fig. 2, thus supporting H4. Based on a nominal comparison of standardized effects, privacy ownership has the strongest effect among the independent variables, followed by metadata transparency and privacy monetization. This relative strength is consistent with the results of Study 1. Our model explains 52.8 % of the variation in trust, which is much higher than in Study 1, suggesting that the trust-building mechanisms of blockchain technology work better in practice for experienced consumers (Study 2) than in theory for ordinary, not necessarily technical consumers (Study 1). Furthermore, illicit purchase needs have a positive effect on trust in Study 1 but a negative effect in Study 2. This may indicate that the idealized notion of purchase-related freedom among inexperienced consumers (Study 1) is shattered when consumers are confronted with the reality of criminal activity (Study 2).

*First survey wave: Consequences of trust*. As shown in Table 4, platform trust positively affects consumers' intention to use the platform (explaining 30.8 % of the variance) and their willingness to pay additional fees if the platform were not free (explaining 14.8 % of the variance).

*First survey wave: Mediation analysis*. Similar to Study 1, bootstrapping tests confirmed that trust significantly ($p < .05$) mediates the effects of privacy ownership (H1), privacy monetization (H2), and metadata transparency (H3) on platform usage intentions and willingness to pay additional fees.

*Second survey wave: Effects on actual consumer behavior.* As shown in Table 4, platform trust ($t_1$) and intention to use the platform ($t_1$) influence actual platform use ($t_2$). Moreover, we observed a negative interaction effect between the intention to use the platform and low self-control ($t_1$, see Appendix 2 for the measure) on platform use ($t_2$). This suggests that consumers with higher self-control are more likely to follow through on their initial intentions, while other consumers are more easily distracted. None of the control variables (i.e., education and gender) have statistically significant effects on platform use ($t_2$).

*First and second survey waves: Mediation analysis*. Bootstrapping tests confirmed that the intention to use the platform ($t_1$) significantly ($p <$ .05) mediated the effect of trust ($t_1$) on actual platform use ($t_2$).

### 5.5. Robustness tests

*Measures*. We conducted a robustness test using formative rather than reflective measures. We operationalized each construct as an index using the mean of its items instead of factor analysis. This produced very similar results, which further validated our hypotheses.

*Additional effects included*. We used additional squared terms for all non-binary independent variables. Our conclusions remained consistent (significance, direction). Furthermore, we ran a regression analysis with two additional control variables: income and occupation. Our conclusions remained consistent.

*Endogeneity*. Our hypothesis tests are unlikely to suffer from endogeneity problems because the blockchain technology characteristics that serve as our independent variables (see Fig. 1) are inherent properties of the technology and platform design, are relatively stable during our short window of observation, and are unlikely to depend on external variables that would simultaneously influence both the independent and dependent variables. In addition, blockchain technology and trust are unlikely to affect each other because trust does not affect the inherent properties of blockchain technology, at least during our short observation period. Despite this low probability of endogeneity problems, if we speculate that privacy monetization could be more attractive to some consumers than to others and that these consumer groups differ in their trust levels, then privacy monetization could potentially be endogenous under this speculative assumption. To test the robustness of our results under this assumption, we conducted an endogeneity test using an instrumental variable. We identified a consumer's income as an appropriate instrumental variable that influences privacy monetization (b = 0.136, $p < .001$). This is likely because wealthier consumers are more financially attractive to online stores, which may offer them more privacy monetization opportunities. In addition, income affects trust only through privacy monetization and not separately (b = 0.02, $p = .53$) because trust in a technology platform has little to do with salary level otherwise (Dutton and Shepherd, 2006).

As a slight adaptation of the model used for our hypothesis testing, we ran an instrumental variable regression on trust, using income in USD as the instrument and privacy monetization as the potentially endogenous regressor. The results are consistent with our hypothesis tests, including the effect of privacy monetization ($p = .04$), which suggests that our findings are robust. Afterwards, we tested for endogeneity using the Durbin and Wu-Hausman tests. Both tests were statistically insignificant (both $p = .06$), indicating that there is no endogeneity problem in the model (Ullah et al., 2021).

### 5.6. Discussion

The results of Study 2, which measured consumers' real-world experiences with blockchain-based e-commerce, were consistent with those of Study 1, which established the causal nature of the mechanisms under study. Together, this helps generalize the results and limits the possibility of sample bias. Study 2 shows that the mechanisms under study indeed influence consumers' actual use of the platform.

## 6. Discussion

### 6.1. Summary of research

To help shape the future of online shopping, our research builds theoretical and practical knowledge about the characteristics of blockchain technology that drive consumer trust and technology adoption (Kamolsook et al., 2019) in the context of blockchain-based e-commerce, which uses novel technology to replace the intermediation mechanisms of centralized platforms (e.g., Amazon) (Kamble et al., 2021; Rejeb et al., 2020; Wan et al., 2022; Wang et al., 2023). Thus, we extend trust formation theory (Mayer et al., 1995) to explain consumer trust in these platforms. Specifically, we developed hypotheses about the effects of the blockchain technology features of privacy ownership (H1), privacy monetization (H2), metadata transparency (H3), and illicit access (H4: moderated by illicit purchase needs) on trust. We tested these hypotheses and the mediating role of trust in technology adoption using an experiment with 16 scenarios (727 consumers) and a multi-wave survey of consumer experiences (666 consumers). The results consistently support the effects of blockchain technology features (i.e., trusting beliefs) on consumer trust (H1-H4) and the mediating role of trust in promoting technology adoption. We also show that trust mediates the effect of consumers' blockchain beliefs on their actual use of blockchain-based platforms. These findings provide retailers with guidance on rebuilding consumer trust in e-commerce, which has been eroded by data breaches and online fraud (Marella et al., 2020; Zhong et al., 2020).

### 6.2. Theoretical implications

Our first theoretical contribution is to provide evidence of how unique blockchain features, as seen by a consumer, can increase the adoption of e-commerce services by fostering consumer trust. This extends the empirical literature on the trust-building capacity of blockchains in different contexts, such as blockchain-based food traceability (Garaus and Treiblmaier, 2021; Joo and Han, 2021), media (Shin and Bianco, 2020), healthcare systems (Shao et al., 2022), and cryptocurrencies (Koroma et al., 2022; Marella et al., 2020). We demonstrate that the blockchain features of privacy ownership, privacy monetization, and metadata transparency enhance consumer trust in e-commerce platforms, thereby promoting e-commerce adoption. These effects occur through specific mechanisms predicted by trust formation theory (Mayer et al., 1995). Privacy ownership signals the platform's ability to protect consumer data, its benevolence in safeguarding users' rights without exploitation, and its integrity in upholding moral standards. Privacy monetization demonstrates the platform's ability to create value for consumers, its benevolence in allowing them to profit from their own data, and its integrity in acting fairly compared to centralized intermediaries. Metadata transparency conveys the ability to provide reliable, verifiable transaction information, benevolence in aiding consumer decision-making without self-serving motives, and integrity through openness and honesty. Furthermore, illicit access functions as a conditional mechanism. For consumers with illicit purchase needs, it enhances trust by reflecting the platform's ability, benevolence, and integrity in meeting their unique demands, while for consumers without such needs, it undermines trust by signaling deficiencies in these same attributes. Notably, these features, although enabled by blockchain, are not its core technical attributes such as immutability, decentralization, or tamper-proofing (Crosby et al., 2016; Nakamoto, 2008). Our findings suggest that non-blockchain-specific, user-facing trust features may be more effective in building consumer trust than these core technical qualities, which often remain invisible to lay users (Alshamsi and Andras, 2019; Shin, 2019). This represents a major theoretical insight: consumer trust in blockchain-based platforms may hinge less on the intrinsic cryptographic or structural guarantees of the technology, and more on perceivable, experience-oriented features that map directly onto the determinants of trust: ability, benevolence, and integrity (Mayer et al., 1995).

By demonstrating these mechanisms, we confirm the results of studies on the role of privacy (Shin, 2019; Shin and Bianco, 2020) and transparency (Garaus and Treiblmaier, 2021; Joo and Han, 2021; Liu et al., 2023; Völter et al., 2023) in different blockchain contexts. Since data that are kept private cannot also be transparent to everyone else, our article extends this work by more clearly specifying different data levels for these constructs. We theorize and empirically test the separate roles and differential effects of transparent, publicly visible metadata and of private data that is securely protected, owned by the consumer, and can be monetized in blockchain-based e-commerce systems. While intermediary entities (e.g., Amazon) own private data in traditional e-commerce platforms with a central intermediary, the ability of consumers to own their data and choose whether to monetize them in a blockchain-based e-commerce platform can empower consumers, increase their revenues, and build their trust in the platform.

Our second contribution is to extend the scope of trust formation theory (Mayer et al., 1995) from one that describes trust in humans and organizations to one that can also describe consumer trust in inanimate online platforms powered by inanimate technology. This aligns with Tan and Saraniemi's (2023) assertion that the object of trust in a blockchain exchange context is less the human actors in a traditional exchange context, but rather the exchange actors (in our research, cryptographically assured privacy ownership), exchange actions (in our research, metadata transparency), and exchange assets (in our research, privacy monetization). Thus, in our research, trust in the blockchain platform, rather than interpersonal trust in transaction partners, emerges as a critical mediator driving consumer behavior. Our research confirms the applicability of a traditional trust theory, namely Mayer et al.'s (1995) trust formation theory, to a blockchain contexts. We do so by drawing an analogy between the technological characteristics of the blockchain, as perceived by consumers, and traditional trust determinants (i.e., ability, integrity, and benevolence). In other words, an inanimate and technology-based e-commerce platform with a defined organizational structure can trigger the same trust formation mechanisms with an analogous set of trust determinants as an interpersonal setting.

As a third contribution, we identify a striking and counterintuitive boundary condition for trust formation theory. Our findings reveal that openness to criminal sellers, and thus access to illicit products, enhances trust only among consumers with illicit purchase needs, while reducing trust among those without such needs (H4; see also Foley et al., 2019; Lusthaus, 2012). This result underscores a darker side of technological trust formation: the same feature that signals ability, benevolence, and integrity to one consumer segment may signal incompetence, self-interest, and moral laxity to another (Mayer et al., 1995; Schoorman et al., 2007). Theoretically, this mechanism highlights how emerging technologies, by removing traditional gatekeepers, can foster trust through enabling autonomy and access, yet simultaneously erode trust when such autonomy facilitates harmful or unethical behavior (De Filippi and Wright, 2018; Kwon and Shao, 2021). This phenomenon extends beyond blockchain to other emerging technologies such as artificial intelligence, decentralized social networks, and generative platforms, which may engender trust among certain users precisely because they circumvent regulation or oversight, while undermining trust among others who value control and safeguards (Shin, 2019; Tan and Saraniemi, 2023). By demonstrating how trust formation can hinge on the morally ambivalent affordances of technology, we expand the scope of trust formation theory to account for the dual potential, both constructive and corrosive, of advanced, autonomous systems. We extend the previous literature on trust formation that focuses only on the trust-building benefits of blockchain applications (Ali et al., 2023; Garaus and Treiblmaier, 2021; Joo and Han, 2021; Shao et al., 2022; Völter et al., 2023), but we emphasize that the absence of an intermediary may also reduce trust in blockchain applications for some consumers.

### 6.3. Practical implications for e-commerce practitioners, policymakers, and consumers

*E-commerce store managers*. In addition to combating fraud and rebuilding consumer trust, blockchain-based e-commerce can give online store managers a competitive advantage by offering consumers features enabled by blockchain technology. The intensity of these features, namely privacy ownership, privacy monetization, metadata transparency, and illicit access, can vary (see Study 2), resulting in different blockchain-based e-commerce platform designs. We recommend that store managers switch to platforms that offer high levels of these features. However, we recommend that store managers only switch to platforms that offer illicit access if their target customers have illicit purchase needs that align with the products offered. Otherwise, they should switch to platforms offering a low level of illicit access. Specifically, we encourage managers to adopt a blockchain platform with a high level of privacy ownership for customers. This feature increases consumer trust the most and is a prerequisite for offering feasible privacy monetization solutions (Harvey et al., 2018). Regarding privacy monetization, we advise store managers to create innovative offers (Frank et al., 2015) to compensate consumers for sharing their personal data. Blockchain-based e-commerce platforms do not offer any other way to collect individual consumer data (e.g., purchase preferences, past purchase details, web browsing history, and daily shopping receipts). Privacy monetization solutions also enhance direct contact between sellers and consumers by providing direct lines of communication that allow for better customer understanding. Moreover, these solutions can be tailored to each consumer's characteristics. Compensation may include monetary incentives (e.g., cryptocurrency, fiat money), reward points, discounts, and free products. Furthermore, we encourage managers to inform potential customers about the types of metadata that are transparent on their blockchain platform and the coexistence of privacy ownership (hidden private data) and metadata transparency (publicly available metadata). Ultimately, practitioners must pursue a hybrid trust model, integrating these powerful blockchain features with robust, traditional mechanisms of accountability (e.g., clear dispute resolution) to ensure consumer trust is grounded in both code and conduct. This approach recognizes that like stablecoins (Manley, 2025), which often require one-to-one backing by real-world assets and regulatory compliance (e.g., as formalized in recent legislation such as the U.S. GENIUS Act: U.S. Congress, 2025), the algorithmic trust of a decentralized platform must be collateralized by tangible legal and physical safeguards.

*E-commerce platform operators*. In addition to benefiting online sellers, blockchain technology can help centralized platforms, such as Amazon, improve their services. These platforms could offer two types of services: the current free services that do not allow consumers to benefit from blockchain features, and new, blockchain-based services that would require a fee. Our results suggest that blockchain features increase consumers' trust, thereby triggering their willingness to pay additional fees. These fees could serve as an additional source of profit. Offering these services could also help centralized platforms become more consumer-centric because blockchain-based e-commerce services address consumers' needs for privacy ownership and monetization, transparency, and access to a wide range of products. Furthermore, our findings demonstrate that human proximity is unnecessary for building trust in and driving adoption of blockchain-based e-commerce platforms. This could reduce costs associated with hiring people to assist consumers, such as Amazon's hiring of customer service representatives.

*Policymakers*. We recommend that policymakers encourage the adoption of blockchain technology by promoting its use by the government and its societal benefits. They can also support blockchain innovation and adoption by creating a flexible regulatory environment that allows experimentation with this technology. By doing so, policymakers can achieve policy goals such as reducing scandals like data breaches and online fraud, addressing the lack of trust in e-commerce, and breaking up online monopolies. Furthermore, the necessity for a hybrid trust model, where algorithmic security is balanced with tangible, real-world accountability, carries specific and timely implications for policymakers. This is highly relevant given recent regulatory attention to decentralized finance, such as the focus on the asset-backing and stable values of stablecoins (Manley, 2025) under frameworks like the U.S. GENIUS Act (U.S. Congress, 2025). The emergence of hybrid trust systems demands the swift creation of a hybrid legislative environment that governs both the decentralized code and the real-world conduct of blockchain-based commerce. Our findings, validating the power of features like privacy monetization and metadata transparency, imply that regulators must develop frameworks that ensure these digital entitlements translate into real-world financial and legal obligations. Specifically, policymakers should mandate mechanisms that legally bind platform operators and users to the inherent promises of blockchain algorithms, such as clear liability for the misuse of transparent data or the failure to uphold privacy ownership rights. By ensuring that the trust-building benefits of blockchain technology are accompanied by mandated and enforceable accountability, policymakers can prevent the decentralized system from becoming a regulatory void, thereby accelerating the ethical and legitimate adoption of this commerce infrastructure.

*Consumers*. We advise consumers to embrace blockchain-based e-commerce because it enables them to protect their online privacy, take ownership of their personal data, and receive compensation for sharing it. Blockchain technology also provides transparency, offering authentic information about products and online stores, as well as access to a wide range of content, including illicit products.

### 6.4. Limitations and directions for future research

Since our research is limited to U.S. data and blockchain-based e-commerce, we encourage scholars to expand upon our research using data from other countries and other blockchain applications, such as social networking, advertising, and gaming, to generalize the findings. Although we used a causal method in Study 1 (experiment) and addressed possible endogeneity issues arising from a limited number of control variables through a robustness test in Study 2 (multi-wave survey), we encourage future research to replicate our findings using alternative methods based on panel data, which can more robustly address endogeneity in similar observations of actual consumer behavior. In addition, future research could extend our findings by comparing blockchain-based trust formation in individualistic versus collectivist cultures. Consumers in individualistic countries may be more concerned about their privacy ownership, whereas consumers in collectivist countries may be more accustomed to sharing information within groups and collectives (e.g., platforms). Future research could also examine other advantages and disadvantages of blockchain applications besides our focal mechanism of increased trust. Most research has focused on the positive aspects of blockchain applications (see Table 1). However, future research could focus more on the negative aspects, similar to our supported hypothesis about a negative effect of illicit access on trust for some consumers. Furthermore, while our research and that of others has examined the main effects of blockchain features on trust formation (see Table 1), only limited research has examined their moderators. These moderators include illicit purchase needs (our research), retailer familiarity, and blockchain benefit disclosure (Study 3 in Garaus and Treiblmaier, 2021). Thus, future research may expand the list of moderators of these main effects to enhance scholars' understanding of the boundary conditions of trust formation theory in blockchain contexts.

## CRediT authorship contribution statement

**Louisa Uchikoshi:** Writing – original draft, Visualization, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Björn Frank:** Writing – review & editing, Writing – original draft, Visualization, Supervision, Project administration, Methodology, Funding acquisition, Conceptualization.

## Declaration of competing interest

The authors have no conflicts of interest.

## Acknowledgments

The authors extend their gratitude to the participants of the studies and the review team. Björn Frank gratefully acknowledges financial support from Waseda University (grant no. 2022R-055).

## Appendix 1. Experimental stimuli

OpenCommerce is a peer-to-peer e-commerce website that uses the blockchain technology and gives you access to a web interface and product range very similar to Amazon or eBay. However, OpenCommerce is not run by one company (such as Amazon) that mediates transactions between you and online vendors/shops, has access to your personal data, and takes a share of the profit for its use. Rather, due to advanced technology, you would purchase directly from online vendors/shops on OpenCommerce. Moreover, you must take full responsibility for controlling your transactions and privacy settings.

Below are additional characteristics of OpenCommerce. Please read them VERY CAREFULLY and REMEMBER them during the entire rest of this questionnaire. Otherwise, all of your responses will be meaningless. We will verify your memory later.

1. **Privacy ownership:**

*Privacy ownership: high.* Due to perfectly secure technology (e.g., encryption), your personal data on OpenCommerce cannot be hacked and leaked to third parties (e.g., criminals). Moreover, you have total control over which personal data you wish to share with online vendors/ shops or keep private.

*Privacy ownership: low.* Due to imperfections in secure technology (e.g., encryption), your personal data on OpenCommerce might be hacked and leaked to third parties (e.g., criminals). Moreover, you have some control over which personal data you wish to share with online vendors/ shops or keep private. However, during online purchases, some of your basic personal data (payment, delivery address) is automatically shared with vendors/shops to facilitate these transactions.

2. **Privacy monetization:**

*Privacy monetization: high.* On OpenCommerce, you can earn money by selling your personal data (e.g., details of your past purchases, Internet browsing history, and daily shop receipts) to online vendors/ shops of your choice.

*Privacy monetization: low.* On OpenCommerce, you cannot earn money by selling your personal data (e.g., details of your past purchases, Internet browsing history, and daily shop receipts) to online vendors/ shops of your choice.

3. **Metadata transparency:**

*Metadata transparency: high.* On OpenCommerce, the anonymous metadata of all users and online shops (e.g., anonymous user ID, purchase transaction details) is publicly visible to anyone else, but not their personal data (e.g., address, age, email/phone) unless voluntarily published (e.g., online reviews). Any modification of visible data (e.g., past reviews, transaction history) is also publicly visible to anyone.

*Metadata transparency: low.* On OpenCommerce, the data of all users and online shops (e.g., user ID, purchase transaction details, address, age, email/phone) is not publicly visible to anyone else unless voluntarily published (e.g., online reviews). Modifications of visible data (e.g., past reviews) is also not publicly visible to anyone.

4. **Illicit access:**

*Illicit access: high.* On OpenCommerce, you can buy illegal products (e.g., fake passports, illegal narcotics, weapons, hacking software, dangerous chemicals, counterfeits, and illegal sexual products) from anonymous sellers that are difficult to catch (e.g., criminals laundering money or financing terrorism).

*Illicit access: low.* On OpenCommerce, you cannot buy illegal products (e.g., fake passports, illegal narcotics, weapons, hacking software, dangerous chemicals, counterfeits, and illegal sexual products) from anonymous sellers that are difficult to catch (e.g., criminals laundering money or financing terrorism).

## Appendix 2. Measures

**MEASURES FOR STUDIES 1 AND 2** ($t_1$; 7-point scales: absolutely disagree/agree):

**TRUST-BUILDING TECHNOLOGY** ($t_1$; 7-point scales: absolutely disagree/agree)

**Perceived privacy ownership** (Adapted from Dinev and Hart, 2005; Gefen, 2002; Hossain and Prybutok, 2008; Mayer et al., 1995; McKnight et al., 2002)

This platform …

1) … perfectly protects my personal data from being hacked and leaked.
2) … has perfectly secure technology (e.g., encryption) that protects my private data.
3) … perfectly protects my privacy.
4) … does not own my personal data, but rather lets me own my personal data.
5) … gives me total control over what personal data I share with online shops.
6) … lets me perfectly control what personal data to share or keep private.

**Perceived privacy monetization** (Adapted from Gefen, 2002; Hsiao and Chen, 2016; Mayer et al., 1995)

By using this platform, …

1) … I can sell my personal data (e.g., details of my past purchases, internet browsing history, and daily shop receipts) to online vendors/shops of my choice.
2) … I can choose personal data that I wish to sell to online vendors/ shops of my choice.
3) … I, rather than a mediating entity (similar to Amazon), can profit financially from my personal data.
4) … I can earn money by selling my private data.

**Perceived metadata transparency** (Adapted from Mayer et al., 1995; Zhou et al., 2018)

On this platform, …

1) … I can view the anonymous metadata of all users and online shops (e.g., anonymous user ID, and purchase transaction details).
2) … the anonymous metadata of all users and online shops (e.g., anonymous user ID, and purchase transaction details) is publicly visible to anyone.
3) … non-personal information of all users and online shops (e.g., anonymous user ID, and purchase transaction details) is publicly visible to anyone.
4) … any modification of visible data (e.g., online reviews) is publicly visible to anyone.
5) … any modification of openly published data (e.g., online reviews) is publicly visible to anyone.

**Perceived illicit access** (Developed based on Coyle et al., 2009; Foley et al., 2019; Lusthaus, 2012; Wang et al., 2005)

This platform…

1) … enables users to buy illegal products (e.g., fake passports, illegal narcotics, weapons, hacking software, dangerous chemicals, and illegal sexual products).
2) … gives access to many illegal products from anonymous sellers, who are difficult to catch.
3) … gives access to low-priced, illegal (e.g., counterfeit) products.
4) … gives access to illegal products sold by criminals for illegal purposes (e.g., laundering money, financing terrorism).

**TECHNOLOGY TRUST** ($t_1$; 7-point scales: absolutely disagree/ agree)

**Platform trust** (Adapted from Alshamsi and Andras, 2019; Mayer et al., 1995; McKnight et al., 2002; Teo and Liu, 2007)

1) This platform is trustworthy.
2) This platform keeps my best interests in mind.
3) I trust the security of this platform.
4) On this platform, I trust that companies cannot make money by using my personal data without my consent.

**PERSONAL TRAITS/VALUES** ($t_1$; 7-point scales: absolutely disagree/agree)

**Illicit purchase needs** (Adapted from Wang and McClung, 2011)

1) I like buying illegal products (e.g., fake passports, illegal narcotics, weapons, hacking software, dangerous chemicals, illegal sexual products, counterfeits).
2) Buying illegal products is important for me.
3) I like the idea of making a good deal in buying illegal products.

**Low self-control** (Choi and Kruis, 2021)

1) I often behave impulsively.
2) I usually behave without planning ahead.
3) I often suddenly engage in unplanned behavior.

**Community ethics** (Adapted from Shafer, 2002)

My community (family, friends, local community) strongly demands that …

1) … I should never do anything unethical.
2) … I should never psychologically or physically harm myself or another person.
3) … I should not perform an action which might threaten the dignity and welfare of myself or of another individual.

**BEHAVIORAL INTENTIONS** ($t_1$; 7-point scales: absolutely disagree/agree)

**Intention to use the platform** (Adapted from Venkatesh et al., 2012)

In the next three months, …

1) … I intend to use this platform.
2) … I predict I will use this platform.
3) … I plan to use this platform.

**Willingness to pay additional fees** (Adapted from McKnight et al., 2002)

Suppose this platform were not free but charged for its use.

1) I would be willing to pay a fee for using this platform.
2) I would be willing to pay for the use of this platform.
3) I am not willing to pay anything for the use of this platform. (reverse)

**ADDITIONAL MEASURES FOR THE SECOND WAVE OF STUDY 2** ($t_2$; 7-point scales: absolutely disagree/agree):

**CONSUMER BEHAVIOR** ($t_2$; 7-point scales: absolutely disagree/agree)

**Technology use** (Lin and Huang, 2008)

In the past six months, I …

1) … have used this platform a lot.
2) … have frequently used this platform.

## Data availability

During data collection, respondents were assured that their answers would not be shared with third parties. However, the research materials will be made available to the editor for verification purposes in accordance with research ethics.

## References

Ali, V., Norman, A.A., Azzuhri, S.R.B., 2023. Characteristics of blockchain and its relationship with trust. IEEE Access 11, 15364–15374.

Alshamsi, A., Andras, P., 2019. User perception of bitcoin usability and security across novice users. Int. J. Hum. Comput. Stud. 126, 94–110.

Benisi, N.Z., Aminian, M., Javadi, B., 2020. Blockchain-based decentralized storage networks: a survey. J. Netw. Comput. Appl. 162, 102656.

Buhrmester, M., Kwang, T., Gosling, S.D., 2011. Amazon's mechanical Turk: a new source of inexpensive, yet high quality data? Perspect. Psychol. Sci. 6 (1), 133–139.

Casino, F., Dasaklis, T.K., Patsakis, C., 2019. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Inform. 36, 55–81.

Cho, J., 2006. The mechanism of trust and distrust formation and their relational outcomes. J. Retail. 82 (1), 25–35.

Choi, J., Kruis, N.E., 2021. Low self-control, substance-using peers and intimate partners, pro-drug use definitions, and inhalant use among convicted offenders in South Korea. J. Drug Issues 51 (1), 128–142.

Coyle, J.R., Gould, S.J., Gupta, P., Gupta, R., 2009. "To buy or to pirate": the matrix of music consumers' acquisition-mode decision-making. J. Bus. Res. 62 (10), 1031–1037.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., 2016. Blockchain technology: beyond bitcoin. Appl. Innov. Rev. 2, 6–19. https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf.

Dai, J., Wang, Y., Vasarhelyi, M.A., 2017. Blockchain: an emerging solution for fraud prevention. CPA J. 87 (6), 12–14. https://www.proquest.com/openview/37d6f16662e21feea20dacfd6664287a/1?pq-origsite=gscholar&cbl=41798.

De Filippi, P., Wright, A., 2018. Blockchain and the Law: The Rule of Code. Harvard University Press.

Dinev, T., Hart, P., 2005. Internet privacy concerns and social awareness as determinants of intention to transact. Int. J. Electron. Commer. 10 (2), 7–29.

Dutton, W.H., Shepherd, A., 2006. Trust in the Internet as an experience technology. Inf. Commun. Soc. 9 (4), 433–451.

Dynata, 2020, January 7. Measure Protocol announces new funding to advance its blockchain-powered marketplace for person-based data. https://www.dynata.com/press/measure-protocol-announces-new-funding-to-advance-its-blockchain-powered-marketplace-for-person-based-data/.

Eisenmann, T.R., Parker, G., Van Alstyne, M., 2009. Opening platforms: how, when and why. Platforms Mark. Innov. 6, 131–162.

Epstein, J., 2017. The CMO Primer for the Blockchain World. Never Stop Marketing. https://assets.ctfassets.net/sdlntm3tthp6/resource-asset-r307/197e57c5f006c9c7a7d7b6ff6819ab70/b12c97b1-3dae-4159-93a2-42f4cbe984ac.pdf.

Foley, S., Karlsen, J.R., Putniņš, T.J., 2019. Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? Rev. Financ. Stud. 32 (5), 1798–1853.

Frank, B., 2024. Consumer preferences for artificial intelligence-enhanced products: differences across consumer segments, product types, and countries. Technol. Forecast. Soc. Chang. 209, 123774.

Frank, B., Enkawa, T., Schvaneveldt, S.J., Torrico, B.H., 2015. Antecedents and consequences of innate willingness to pay for innovations: understanding motivations and consumer preferences of prospective early adopters. Technol. Forecast. Soc. Chang. 99, 252–266.

Frank, B., Herbas-Torrico, B., Schvaneveldt, S.J., 2021. The AI-extended consumer: technology, consumer, country differences in the formation of demand for AI-empowered consumer products. Technol. Forecast. Soc. Change 172, 121018.

Gan, Q., Lau, R.Y.K., 2024. Trust in a 'trust-free' system: Blockchain acceptance in the banking and finance sector. Technol. Forecast. Soc. Change 199, 123050.

Garaus, M., Treiblmaier, H., 2021. The influence of blockchain-based food traceability on retailer choice: the mediating role of trust. Food Control 129, 108082.

Gefen, D., 2002. Reflections on the dimensions of trust and trustworthiness among online consumers. ACM SIGMIS Database DATABASE Adv. Inform. Syst. 33 (3), 38–53.

Gefen, D., Karahanna, E., Straub, D.W., 2003. Trust and TAM in online shopping: an integrated model. MIS Q. 27 (1), 51–90.

Gillman, D., 2023. Achieving transparency: a metadata perspective. Data Intell. 5 (1), 261–274.

Hair, J. F. Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis (7th ed.). Prentice Hall.

Harris, R., 2020. Forging a path towards meaningful digital privacy: data monetization and the CCPA. Loyola Los Angeles Law Rev. 54 (1), 197–234.

Harvey, C.R., Moorman, C., Toledo, M., 2018, October 1. How blockchain can help marketers build better relationships with their customers. Harvard Business School Publishing. https://hbr.org/2018/10/how-blockchain-can-help-marketers-build-better-relationships-with-their-customers.

Herbas Torrico, B., Frank, B., Arandia Tavera, C., 2018. Corporate social responsibility in Bolivia: meanings and consequences. Int. J. Corp. Soc. Responsib. 3 (7), 1–13. https://doi.org/10.1186/s40991-018-0029-0.

Hoffman, D.L., Novak, T.P., Peralta, M., 1999. Building consumer trust online. Commun. ACM 42 (4), 80–85.

Hossain, M.M., Prybutok, V.R., 2008. Consumer acceptance of RFID technology: an exploratory study. IEEE Trans. Eng. Manag. 55 (2), 316–328.

Hsiao, K.L., Chen, C.C., 2016. What drives in-app purchase intention for mobile games? An examination of perceived values and loyalty. Electron. Commer. Res. Appl. 16, 18–29.

Hummel, P., Braun, M., Dabrock, P., 2021. Own data? Ethical reflections on data ownership. Philos. Technol. 34 (3), 545–572.

Joo, J., Han, Y., 2021. An evidence of distributed trust in blockchain-based sustainable food supply chain. Sustainability 13 (19), 10980.

Kamble, S.S., Gunasekaran, A., Kumar, V., Belhadi, A., Foropon, C., 2021. A machine learning based approach for predicting blockchain adoption in supply chain. Technol. Forecast. Soc. Change 163, 120465.

Kamolsook, A., Badir, Y.F., Frank, B., 2019. Consumers' switching to disruptive technology products: the roles of comparative economic value and technology type. Technol. Forecast. Soc. Chang. 140, 328–340.

Karamchandani, A., Srivastava, S.K., Srivastava, R.K., 2020. Perception-based model for analyzing the impact of enterprise blockchain adoption on SCM in the Indian service industry. Int. J. Inf. Manag. 52, 102019.

Kees, J., Berry, C., Burton, S., Sheehan, K., 2017. An analysis of data quality: professional panels, student subject pools, and Amazon's mechanical Turk. J. Advert. 46 (1), 141–155.

Kim, J., Jin, B., Swinney, J.L., 2009. The role of retail quality, e-satisfaction and e-trust in online loyalty development process. J. Retail. Consum. Serv. 16 (4), 239–247.

Koroma, J., Rongting, Z., Muhideen, S., Akintunde, T.Y., Amosun, T.S., Dauda, S.J., Sawaneh, I.A., 2022. Assessing citizens' behavior towards blockchain cryptocurrency adoption in the Mano River Union states: mediation, moderation role of trust and ethical issues. Technol. Soc. 68, 101885.

Kowalski, M., Lee, Z.W., Chan, T.K., 2021. Blockchain technology and trust relationships in trade finance. Technol. Forecast. Soc. Change 166, 120641.

Kwon, K.H., Shao, C., 2021. Dark knowledge and platform governance: a case of an illicit e-commerce community in reddit. Am. Behav. Sci. 65 (6), 779–799.

Lin, T.C., Huang, C.C., 2008. Understanding knowledge management system usage antecedents: an integration of social cognitive theory and task technology fit. Inf. Manag. 45 (6), 410–417.

Liu, H., Ma, R., He, G., Lamrabet, A., Fu, S., 2023. The impact of blockchain technology on the online purchase behavior of green agricultural products. J. Retail. Consum. Serv. 74, 103387.

Lusthaus, J., 2012. Trust in the world of cybercrime. Global Crime 13 (2), 71–94.

Manley, J., 2025, July 9. What is a stablecoin? J.P. Morgan. https://am.jpmorgan.com/us/en/asset-management/adv/insights/market-insights/market-updates/on-the-minds-of-investors/what-is-a-stablecoin/.

Marella, V., Upreti, B., Merikivi, J., Tuunainen, V.K., 2020. Understanding the creation of trust in cryptocurrencies: the case of bitcoin. Electron. Mark. 30 (2), 259–271.

Mason, C.H., Perreault, W.D., 1991. Collinearity, power, and interpretation of multiple regression analysis. J. Market. Res. 28 (3), 268–280.

Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995. An integrative model of organizational trust. Acad. Manage. Rev. 20 (3), 709–734.

Mazzella, F., Sundararajan, A., d'Espous, V.B., Möhlmann, M., 2016. How digital trust powers the sharing economy. IESE Insight Rev. 30, 24–30.

McKnight, D.H., Choudhury, V., Kacmar, C., 2002. Developing and validating trust measures for e-commerce: an integrative typology. Inf. Syst. Res. 13 (3), 334–359.

Mende, M., Noble, S.M., 2019. Retail apocalypse or golden opportunity for retail frontline management? J. Retail. 95 (2), 84–89.

Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system. Decentralized Bus. Rev., 21260 https://doi.org/10.2139/ssrn.3440802.

Odiete, O., Lomotey, R.K., Deters, R., 2018. Using blockchain to support data and service management in IoV/IoT. In: Security with Intelligent Computing and Big-data Services, vol. 733. Springer, pp. 344–362.

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. J. Appl. Psychol. 88 (5), 879–903.

Rejeb, A., Keogh, J.G., Treiblmaier, H., 2020. How blockchain technology can benefit marketing: six pending research areas. Front. Blockchain 3 (3), 1–12.

Roggeveen, A.L., Sethuraman, R., 2020. Customer-interfacing retail technologies in 2020 & beyond: an integrative framework and research directions. J. Retail. 96 (3), 299–309.

Rönkkö, M., Cho, E., 2022. An updated guideline for assessing discriminant validity. Organ. Res. Methods 25 (1), 6–14.

Salam, A.F., Rao, H.R., Pegels, C.C., 2003. Consumer-perceived risk in e-commerce transactions. Commun. ACM 46 (12), 325–331.

Schlosser, A.E., White, T.B., Lloyd, S.M., 2006. Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions. J. Mark. 70 (2), 133–148.

Schoorman, F.D., Mayer, R.C., Davis, J.H., 2007. An integrative model of organizational trust: past, present, and future. Acad. Manage. Rev. 32 (2), 344–354.

Schumpeter, 2018, March 28. Getting a handle on a scandal. https://www.economist.com/business/2018/03/28/getting-a-handle-on-a-scandal.

Shafer, W.E., 2002. Ethical pressure, organizational-professional conflict, and related work outcomes among management accountants. J. Bus. Ethics 38 (3), 261–273.

Shao, Z., Zhang, L., Brown, S.A., Zhao, T., 2022. Understanding users' trust transfer mechanism in a blockchain-enabled platform: a mixed methods study. Decis. Support. Syst. 155, 113716.

Shi, W., Rumokoy, F.S., Frank, B., 2025. Customer loyalty through augmented reality apps: quality attributes, market differences, and trust as a mediator. Total Qual. Manag. Bus. Excell. 36 (7–8), 759–787.

Shin, D.D., 2019. Blockchain: the emerging technology of digital trust. Telematics Inform. 45, 101278.

Shin, D., Bianco, W.T., 2020. In blockchain we trust: does blockchain itself generate trust? Soc. Sci. Q. 101 (7), 2522–2538.

Singh, V., Sharma, S.K., 2022. Application of blockchain technology in shaping the future of food industry based on transparency and consumer trust. J. Food Sci. Technol. 60 (4), 1237–1254.

Sucher, S.J., Gupta, S., 2019, July 16. The trust crisis. Harvard Business School Publishing. https://hbr.org/2019/07/the-trust-crisis.

Tan, T.M., Saraniemi, S., 2023. Trust in blockchain-enabled exchanges: future directions in blockchain marketing. J. Acad. Mark. Sci. 51 (4), 914–939.

Tangalakis-Lippert, K., 2022, August 28. Amazon's empire of surveillance: through recent billion-dollar acquisitions of health care services and smart home devices, the tech giant is leveraging its monopoly power to track every aspect of our lives. Bus. Insid. https://www.businessinsider.com/amazon-empire-of-surveillance-leveraging-monopoly-power-tracking-purchases-2022-8.

Teo, T.S., Liu, J., 2007. Consumer trust in e-commerce in the United States, Singapore and China. Omega 35 (1), 22–38.

U.S. Congress, 2025. GENIUS Act. https://www.congress.gov/bill/119th-congress/senate-bill/1582/text.

Ullah, S., Zaefarian, G., Ullah, F., 2021. How to use instrumental variables in addressing endogeneity? A step-by-step procedure for non-specialists. Ind. Mark. Manag. 96, A1–A6.

Venkatesh, V., Thong, J.Y., Xu, X., 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Q. 36 (1), 157–178.

Völter, F., Urbach, N., Padget, J., 2023. Trusting the trust machine: evaluating trust signals of blockchain applications. Int. J. Inf. Manage. 68, 102429.

Wan, Y., Gao, Y., Hu, Y., 2022. Blockchain application and collaborative innovation in the manufacturing industry: based on the perspective of social trust. Technol. Forecast. Soc. Change 177, 121540.

Wang, X., McClung, S.R., 2011. Toward a detailed understanding of illegal digital downloading intentions: an extended theory of planned behavior approach. New Media Soc. 13 (4), 663–677.

Wang, F., Zhang, H., Zang, H., Ouyang, M., 2005. Purchasing pirated software: an initial examination of Chinese consumers. J. Consum. Mark. 22 (6), 340–351.

Wang, Z., Zhang, S., Zhao, Y., Chen, C., Dong, X., 2023. Risk prediction and credibility detection of network public opinion using blockchain technology. Technol. Forecast. Soc. Change 187, 122177.

West, E., 2022, June 13. How Amazon branded convenience and normalized monopoly. https://thereader.mitpress.mit.edu/how-amazon-branded-convenience-and-normalized-monopoly/.

Williams, L.J., Hartman, N., Cavazotte, F., 2010. Method variance and marker variables: a review and comprehensive CFA marker technique. Organ. Res. Methods 13 (3), 477–514.

Wissawaswaengsuk, P., Kumar, P., Frank, B., Badir, Y.F., 2025. The role of trust as the facilitator and contingency factor in the adoption of digital healthcare services: a telemedicine context. Comput. Hum. Behav. 172, 108722.

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G., Chen, S., 2020. Public and private blockchain in construction business process and information integration. Autom. Constr. 118, 103276.

Zhong, B., Wu, H., Ding, L., Luo, H., Luo, Y., Pan, X., 2020. Hyperledger fabric-based consortium blockchain for construction quality information management. Front. Eng. Manag. 7 (4), 512–527.

Zhou, L., Wang, W., Xu, J.D., Liu, T., Gu, J., 2018. Perceived information transparency in B2C e-commerce: an empirical investigation. Inf. Manag. 55 (7), 912–927.

Ziccardi, G., 2012. Resistance, Liberation Technology and Human Rights in the Digital Age, vol. 7. Springer.

**Louisa Uchikoshi** conducted research at Waseda University (Japan). Previously, she graduated from Paris-Saclay University (France) and the Algiers School of Higher Commercial Studies (Algeria). Her research interests are in the areas of blockchain, marketing, and innovation.

**Björn Frank** is Professor at Waseda University in Tokyo, Japan. Previously, he was Associate Professor at Sophia University and Assistant Professor at the Tokyo Institute of Technology. He holds a doctoral degree from Tokyo Institute of Technology and master's degrees from Ecole Centrale de Lyon and Technische Universität Darmstadt. His research interests are in the areas of marketing, innovation, and sustainable business.