

Exploring Determinants of Metaverse E-Commerce Purchase Intention Among Albanian University Students

Research Paper

Kreshnik Vukatana¹, Anxhela Ferhataj^{2,*}

¹University of Tirana, Tirana, Albania, kreshnik.vukatana@unitir.edu.al, ORCID: <https://orcid.org/0000-0002-8779-0767>

²University of Tirana, Tirana, Albania, anxhela_ferhataj.feutdr@unitir.edu.al, ORCID: <https://orcid.org/0000-0002-1054-2351>

Received 13 November 2025; Accepted 04 June 2026

Abstract: **Research purpose.** This study investigates how metaverse knowledge, perceived value and perceived security risk relate to university students' intention to engage in metaverse e-commerce in a developing-economy context. Focusing on Albanian students as an early-adopter cohort, it examines whether knowledge and value act as enablers and perceived security risk as a barrier to metaverse-based shopping.

Design / Methodology / Approach. A quantitative, cross-sectional online survey was conducted with 221 undergraduate and graduate students from universities in Albania. Knowledge of the metaverse, along with its perceived value, perceived security risk, and metaverse e-commerce purchase intention, were evaluated using multi-item five-point Likert scales based on privacy-calculus and technology-acceptance research. Descriptive statistics profiled respondents' perceptions. Bivariate associations were examined using Spearman correlations, and hypotheses were evaluated using hierarchical regression (controls: gender, age) and PLS-SEM with bias-corrected bootstrapping (5,000 resamples). Programme-group differences were explored using Mann-Whitney U tests. Reliability was excellent (Cronbach's $\alpha = 0.911$).

Findings. Students reported moderate but uneven metaverse knowledge, with greater familiarity with basic concepts and commercial applications and lower familiarity with VR/AR/XR technologies and ethics or privacy issues. Bivariate results supported both hypotheses: metaverse knowledge ($\rho = .249, p < .001$) and perceived value ($\rho = .400, p < .001$) were positively associated with metaverse e-commerce purchase intention, whereas perceived security risk was negatively associated ($\rho = -.118, p = .040$). Hierarchical regression showed a significant improvement from the control model to the full model ($\Delta R^2 = .128, p < .001$), and PLS-SEM showed comparable explanatory power ($R^2 = .177$).

Originality / Value / Practical implications. The study adds evidence from a developing-economy setting by jointly examining knowledge, value, and security risk as determinants of metaverse e-commerce intention. The results show a clear benefit-risk balance: knowledge and perceived value encourage intention, but high security concerns continue to hold students back, even among tech-savvy users. For universities and policymakers, this points to the need for metaverse-focused literacy on VR/AR/XR, data protection and digital rights, not just technical pilots. For firms and platform providers, the findings underline that successful metaverse offers must pair personalisation and rewards with transparent information, visible security-by-design measures, and real control over how students' identities and avatars are used.

Keywords: *metaverse e-commerce • metaverse knowledge • perceived value of metaverse e-commerce • perceived security risk • metaverse e-commerce purchase intention*

JEL codes: I23; L81; O33

* Email: anxhela_ferhataj.feutdr@unitir.edu.al

Introduction

The metaverse is rapidly emerging as a commercial interface that allows consumers to browse, try, and purchase products in immersive environments. Prior research suggests that telepresence, flow, and related experiential cues can enhance shopping attitudes and purchase intention because richer interaction and a stronger sense of “being there” make products feel more knowable and trustworthy (Jafar et al., 2023; Jafar et al., 2024; Zhong & Hamouda, 2024). Drawing on a systematic review of virtual commerce research, Shen et al. (2021) show that most studies explain purchase intention primarily through experiential and design-related drivers such as presence, enjoyment, engagement, trust, and satisfaction, whereas user knowledge, perceived value, and security-related risk receive comparatively less attention as explicit determinants. Recent empirical work in avatar-based settings points in the same direction. Noor et al. (2025) report that social presence and flow consciousness increase users’ likelihood of buying online and co-creating content and value, with e-trust and affinity for technology interaction moderating these relationships. Prior research highlights the potential of metaverse-based commerce, yet translating interest into transactions remains challenging amid persistent concerns about cost, privacy, and security. This motivates the question of which factors convert initial interest into metaverse e-commerce purchase intention.

Decades of e-commerce research identify risk as a central barrier. Meta-analytic evidence links trust, perceived risk, and perceived security to online purchasing behaviour, while validated scales show that fear of online identity theft suppresses willingness to transact (Handoyo, 2024; Hille et al., 2015). Cost is another practical constraint: when expected benefits do not outweigh monetary and non-monetary costs, purchase intention declines. In consumer-technology contexts, perceived value is a direct antecedent of behavioural intention, and VR/AR hardware requirements can amplify perceived costs, especially for first-time users (Pillai et al., 2024; Venkatesh et al., 2012). A third determinant in this context is knowledge. Basic awareness and literacy reduce uncertainty and help consumers assess both value and risk. In virtual store environments, metaverse features can improve product knowledge and, in turn, increase purchase intention (Jafar et al., 2023). Privacy concerns are also consistent with the privacy-calculus perspective, in which individuals weigh expected benefits against security and data-protection risks (Dinev & Hart, 2006).

Despite growing interest in the metaverse, there is limited empirical evidence on how knowledge, perceived security risk, and perceived value jointly influence purchase intention, and evidence from developing economies is particularly sparse. To address this gap, we analyse survey data from Albanian university students, an early-adopter cohort of immersive and social technologies that participates actively in digital commerce. In this context, we examine metaverse knowledge and perceived value as enablers, and perceived security risk as a barrier, to metaverse e-commerce purchase intention.

To strengthen the theoretical grounding, this study integrates UTAUT2 and privacy calculus by mapping each construct to core theory components. Perceived value is specified as the benefit appraisal in metaverse retail, capturing functional utility, experiential and social value, and “worth it” evaluations consistent with price value (Venkatesh et al., 2012). Metaverse knowledge is conceptualised as domain-specific literacy that reduces uncertainty and supports more informed benefit-cost evaluation. Complementing this, perceived security risk is positioned as the privacy-calculus cost component, reflecting concerns about account compromise, data misuse, payment security, and avatar-based identity threats (Dinev & Hart, 2006; Laiz-Ibanez et al., 2025). Although related, trust and risk are conceptually distinct: trust reflects positive expectations regarding platform integrity, whereas perceived risk captures anticipated harm from privacy and security threats (Pavlou, 2003). Accordingly, perceived security risk is specified as the main inhibiting belief in the proposed framework. Figure 1 presents the conceptual model linking metaverse knowledge, perceived value, and perceived security risk to metaverse e-commerce purchase intention.

This study addresses two research questions:

- RQ1. What are Albanian university students’ perceptions of their metaverse knowledge and of the value of metaverse e-commerce?
- RQ2. How do Albanian university students perceive security risk in metaverse e-commerce?

Accordingly, we test the following hypotheses:

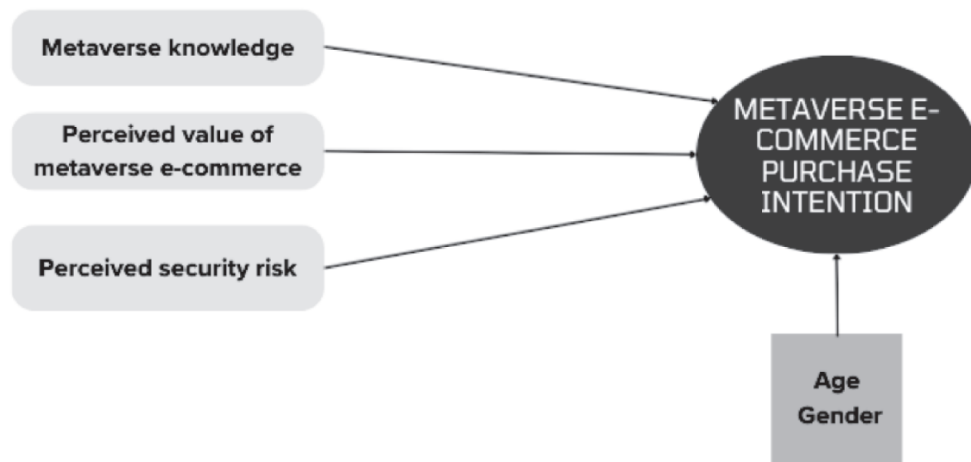


Figure 1. Conceptual Model (Source: Created by the authors).

- H1. Metaverse knowledge and perceived value are positively associated with metaverse e-commerce purchase intention. ($\alpha = 0.05$)
- H2. Perceived security risk is negatively associated with metaverse e-commerce purchase intention. ($\alpha = 0.05$)

Literature review

Early e-commerce research suggests that consumers evaluate online transactions through a benefit-risk calculus. The privacy-calculus framework captures this trade-off by showing that privacy and security risk beliefs reduce willingness to disclose data or transact, while perceived benefits and safeguards can partly offset these concerns (Dinev & Hart, 2006). Perceived risk has been conceptualised as a distinct inhibitor of online purchasing, including identity-theft related fears that can suppress intention even when attitudes are favourable (Hille et al., 2015; Pavlou, 2003). In consumer technology contexts, UTAUT2 positions price value as a direct antecedent of intention, which is particularly relevant when adoption involves device, time, or learning costs (Venkatesh et al., 2012). Consistent evidence in metaverse-retail settings also links value-related beliefs to intention (Pillai et al., 2024). Although UTAUT2 is not metaverse-specific, it is directly relevant where access involves device, time, or learning costs. Meta-analytic evidence further supports these relationships by linking security and trust to higher purchasing and perceived risk to lower purchasing (Handoyo, 2024). Overall, prior e-commerce research suggests that adoption is shaped by users' value assessments, security risk perceptions, and the knowledge that supports benefit-risk evaluation.

With the shift to persistent, social, 3D environments, metaverse studies have examined how immersive cues translate into shopping outcomes. A consistent pattern is that immersive design cues, such as vividness, interactivity, and social presence, strengthen experiential states like telepresence and flow, which in turn are associated with more favourable attitudes and stronger purchase intentions (Ahn et al., 2024; Jafar et al., 2023; Jafar et al., 2024; Zhong & Hamouda, 2024). Evidence also suggests that excitement generated by immersion coexists with practical barriers, implying that experiential appeal must be matched with clear value delivery to translate engagement into purchase intention (Soni et al., 2025). Despite progress on experiential mechanisms, direct comparative tests of metaverse knowledge, perceived value, and perceived security risk as determinants of purchase intention remain limited.

Alongside experiential drivers, recent research has increasingly focused on adoption-critical determinants in metaverse retail. Applying UTAUT2 to this context, Pillai et al. (2024) show that performance expectancy, hedonic motivation, and price value are positively associated with intention to shop in metaverse environments, whereas security and privacy concerns are negatively associated. At the same time, recent research highlights privacy and safety concerns as key barriers to metaverse adoption intention (Kirmani et al., 2025). Together, this evidence

supports a parsimonious framing in which knowledge and perceived value function as enabling factors, while perceived security risk functions as an inhibiting factor for metaverse e-commerce purchase intention. These dynamics may be especially salient in developing economies, where affordability, infrastructure, and payment security constraints can intensify risk perceptions and heighten the role of value in adoption decisions (Hendricks & Mwapwele, 2024). Because evidence from developing-economy contexts remains limited, examining these determinants among Albanian university students provides underrepresented, contextually relevant insight.

The importance of the metaverse is visible in two external signals: rising EU financing for deployment and a recent wave of patenting (Eulaerts et al., 2025; European Commission, 2025). Patents mark intense invention, while EU-funded projects channel resources into pilots, standards, training, and industry and university partnerships (Fig. 2). This European momentum now reaches Albania through initiatives involving local universities and firms, such as Erasmus+ VALEU-X and COWEB, together with vocational and regional pilots that use VR and metaverse tools in teaching and skills development (VALEU-X, 2022; COWEB, 2025). These projects spread metaverse-related knowledge through curricula and faculty training, promote clearer security and privacy practices, and allow value propositions to be tested with real users. Against this backdrop, our focus on knowledge, perceived value, and perceived security risk speaks directly to the adoption frictions faced by Albanian students as early participants in metaverse e-commerce. The initiatives signal growing institutional support but do not, by themselves, remove individual-level barriers, reinforcing the need to measure knowledge, perceived value, and perceived security risk as immediate drivers of purchase intention.

The regulation of intellectual property rights (IPR) in the metaverse remains unsettled. EU policy documents emphasise that user-generated content and virtual assets complicate ownership, licensing, and enforcement, and call for coherent rules that protect rights without stifling innovation (European Parliament, 2024; European Union Intellectual Property Office, 2024). Recent developments also signal that existing doctrines are being tested in adjacent digital markets, including disputes involving NFTs and platform liability for third-party listings (Hermès International v. Rothschild, 2023; Atari Interactive, Inc. v. Redbubble, Inc., 2021). For metaverse e-commerce, such uncertainty can heighten perceived security risk, while clearer protection can strengthen perceived value by signalling that virtual purchases carry enforceable and durable rights. At the same time, the complexity of IP rules increases what users need to know: they must be able to understand what exactly they are buying and which rights are attached to that purchase.

Research methodology

This study employed a quantitative research design to examine how metaverse knowledge, perceived value and perceived security risk relate to university students' intention to engage in metaverse e-commerce in Albania.

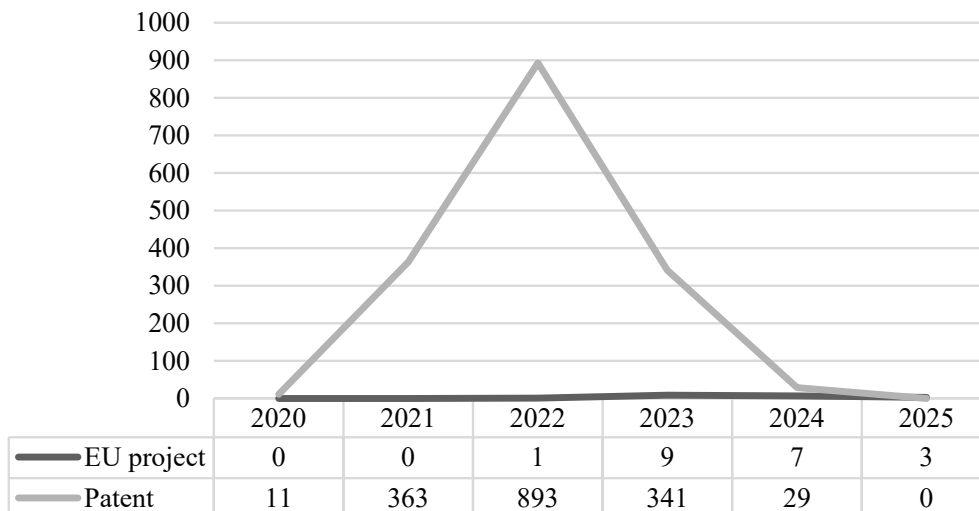


Figure 2. Patents and EU-funded projects in metaverse technologies (Source: European Commission, 2025).

University students form a salient early-adopter group: they are frequent online shoppers and confident users of digital technologies, yet they still face considerable uncertainty about the benefits, costs, and security risks of metaverse e-commerce.

Sample and data collection

The sample for this research consisted of undergraduate and graduate students enrolled in universities in Albania. Data were collected between June and September 2025 using an online questionnaire disseminated via university mailing lists and student social media groups. The study involved an anonymous, voluntary online survey and did not collect personally identifying or sensitive data. In line with institutional guidance for minimal-risk research, formal ethics committee review was not required for this study design. Participants were first shown an information page covering the essential points, such as the study's aim, estimated duration, confidentiality and anonymity of responses, and the right to withdraw at any moment before completion. Clicking through to the first question was treated as providing informed consent. Data handling complied with GDPR (European Parliament & Council of the European Union, 2016) and Albania's Law No. 124/2024 (Parliament of Albania, 2024).

In total, 255 questionnaires were submitted; after quality screening, 221 valid responses were retained for analysis. This represents an 86.7% response rate. The final sample comprised 221 students (90 female; 131 male), predominantly aged 18-22 ($n=175$), followed by 23-27 ($n=34$), 28-32 ($n=10$), and >32 ($n=2$). Around 64% of respondents were Bachelor students, 30% were enrolled in Master of Science programs, and 6% in Professional Master programs. With respect to field of study, approximately 71.5% were enrolled in STEM programs (Information Technology, Computer Engineering, Applied Informatics) and 28.5% in business and economics (Business Management, Finance).

The sample is concentrated in a narrow age range and a single national context, so the findings are most directly generalisable to comparable student populations. Focusing on university students is appropriate at this stage because they constitute a plausible early-adopter cohort in which value appraisals and security concerns can be observed before wider market diffusion. Although recruitment channels may underrepresent less digitally engaged users, the sample is well aligned with the study's target segment and therefore fits the study's aims. This approach is consistent with prior research on nascent digital innovations that deliberately examines tech-savvy young users as early adopters.

Survey instrument

The questionnaire had six sections: (1) study information and consent, (2) metaverse knowledge, (3) perceived value of metaverse e-commerce, (4) perceived security risk, (5) metaverse e-commerce purchase intention, and (6) demographic and contextual questions. All construct items were answered on a five-point Likert scale from 1 ("strongly disagree") to 5 ("strongly agree"). Demographic and contextual questions were included as multiple-choice or Likert-type items to describe the sample and its metaverse-related attitudes.

Guided by prior e-commerce, technology-acceptance and metaverse research, four core constructs were conceptualised and measured as follows.

- Metaverse knowledge captures students' self-assessed understanding of metaverse-related technologies and issues. Drawing on work linking digital literacy and domain knowledge to reduced uncertainty and technology adoption (Dinev & Hart, 2006; Jafar et al., 2023), it is measured with four items on familiarity with basic metaverse concepts, VR/AR/XR technologies, commercial applications, and ethics/privacy.
- Perceived value of metaverse e-commerce reflects students' overall judgement of whether metaverse shopping is "worth it" given the balance of benefits and costs. Following the price-value logic in UTAUT2 and metaverse adoption studies (Pillai et al., 2024; Venkatesh et al., 2012), it is measured with nine items capturing functional, social, and experiential/personalisation value in a metaverse store.
- Perceived security risk captures concerns about privacy, data protection and potential harm when transacting in metaverse environments. Based on the privacy-calculus framework and research on perceived risk and online identity theft (Dinev & Hart, 2006; Hille et al., 2015; Pavlou, 2003), it is measured with six items on identity theft, misuse or sale of personal data, device and account compromise, payment misuse, and avatar-related identity threats.
- Metaverse e-commerce purchase intention represents students' willingness to engage in metaverse-based shopping. Consistent with technology-acceptance models that treat behavioural intention as a proximal predictor

of use (Pillai et al., 2024; Venkatesh et al., 2012), it is measured with four items asking how likely respondents are to use metaverse environments to browse, try and buy products once such options become available.

To contextualise these constructs, additional Likert-scale and multiple-choice items covered avatar design, preferred basis for personalisation, devices, data sharing, payment methods, perceived excitement, usefulness and hardware costs, and comfort with metaverse influencers or other “non-real” agents.

Data analysis

Data were analysed using JASP version 0.95.0 (JASP, 2025), an open-source statistical environment. Descriptive statistics were computed for all variables, and scale reliability was assessed; the overall instrument showed excellent internal consistency (Cronbach's $\alpha = 0.911$). Bivariate associations were examined using Spearman's rank-order correlations. To test the hypothesised relationships in a multivariate setting, we estimated hierarchical regression models with gender and age entered as control variables in Model 0 and metaverse knowledge, perceived value, and perceived security risk added in Model 1. As a robustness check, the same structural relationships were estimated using PLS-SEM. Statistical inference for both regression coefficients and PLS-SEM paths relied on bias-corrected bootstrapping (5,000 resamples). Programme-group differences were explored using Mann–Whitney U tests. A conventional significance level of $\alpha = 0.05$ and 95% confidence intervals were used for all inferential analyses.

Research results

Before examining metaverse knowledge and perceived value, it is useful to consider how students imagine representing themselves in metaverse environments and how they would prefer brands to address them. When asked how they would design an avatar, about half of the respondents (49.8%) would create an avatar that closely resembles their real self. The remaining students would use the avatar to experiment with or protect their identity: 18.1% would rather “be who I want to be” in a virtual world, 10.4% seek to avoid stereotypes, 9.5% are uncomfortable sharing their real identity, 8.1% would choose an avatar that does not resemble them at all, and 4.1% would emphasise traits that others may not notice. This pattern suggests that avatar design is not only an aesthetic choice, but also a practical way of managing authenticity and identity exposure in metaverse commerce.

Preferences for personalisation reveal a similar split. About one third of students (34.9%) wanted experiences personalised to them as real persons, 30.3% preferred personalisation around their avatar, and 34.8% were not yet sure which “persona” they would want brands to recognise. Students were moderately open to engaging with metaverse influencers ($M = 3.31$), yet they reported higher discomfort with sharing information with a “non-real person” ($M = 3.68$). Together, these results imply that personalisation can be attractive, but it must be paired with clear boundaries, transparency, and user control over identity and data.

Price and payment-related perceptions provide further context. Students reported a generally positive stance toward metaverse experiences ($M = 3.62$) and expected the metaverse's technical features to have a meaningful impact ($M = 3.51$). They were also relatively open to using cryptocurrencies for payments ($M = 3.56$). At the same time, hardware costs were perceived as high ($M = 3.44$). Overall, the profile is consistent with an early-adopter cohort that is curious and optimistic, but whose readiness to transact is tempered by affordability concerns and persistent doubts about identity and payment security.

RQ1. What are Albanian university students' perceptions of their metaverse knowledge and of the value of metaverse e-commerce?

According to Figure 3, the metaverse knowledge of Albanian students is at a moderate level but with different areas showing varying degrees of knowledge. On a five-point scale, the students represented by the mean score of 3.91 found it easiest to understand the basic concepts associated with the metaverse and its commercial usage (mean = 3.588). The least of all was the knowledge of the underlying VR/AR/XR technologies (mean = 3.299), and awareness & understanding of ethics and privacy issues were the weakest (mean = 3.222). This pattern parallels Jafar et al.'s (2023) observation that perceived knowledge serves as a mediator between telepresence and purchase intention; users need to be familiar with the environment before immersive cues convert into assurance and purchase intentions.

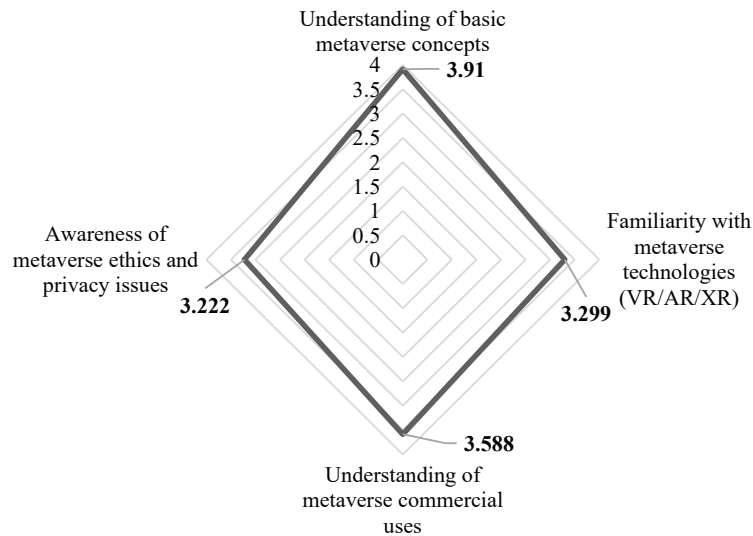


Figure 3. Metaverse knowledge (Source: Created by the authors).

The data in Table 1 show broadly similar value perceptions across programmes, with mean ratings ranging from 3.254 to 3.794 among Business and Economics students ($n = 63$) and from 3.266 to 3.639 among STEM students ($n = 158$). However, Mann-Whitney U tests indicate statistically significant programme differences for five of the nine items. Compared with STEM students, Business and Economics students rated “receiving attractive benefits or rewards” higher ($M = 3.698$ vs. 3.557 ; $U = 7362$; $p < .001$) and also rated “having options that are tailored to me” higher ($M = 3.794$ vs. 3.639 ; $U = 4775$; $p = .005$). By contrast, STEM students gave higher ratings to “clear and easy-to-understand product information” ($M = 3.551$ vs. 3.524 ; $U = 7170$; $p = .004$), “feeling that I belong and am welcome in a metaverse store” ($M = 3.494$ vs. 3.429 ; $U = 5147$; $p = .045$), and “being able to speak with a similar customer-support agent or brand representative” ($M = 3.449$ vs. 3.254 ; $U = 4799$; $p = .006$). The remaining items did not differ significantly by programme, including anonymous shopping ($p = .382$), familiarity with home shopping routines ($p = .324$), opportunities for interaction with similar others ($p = .187$), and exploring a different way of shopping ($p = .468$). Importantly, even where differences are statistically significant, the mean gaps are small, suggesting that the overall value profile is largely shared across disciplines.

RQ2. How do Albanian university students perceive security risk in metaverse e-commerce?

As shown in Table 2, students perceive metaverse e-commerce as high-risk across all six indicators, with mean ratings close to or above 4.0 in both programme groups. The strongest concerns relate to account and device security, including the possibility that the device could be hacked when accessing metaverse platforms (Business and Economics: $M = 4.19$; STEM: $M = 4.171$; $U = 7070$; $p = .008$) and that network or account credentials could be compromised ($M = 4.143$ vs. 4.101 ; $U = 6863$; $p = .030$). Concerns about data exploitation were also pronounced, particularly the possibility that personal data could be collected and sold to third parties ($M = 4.127$ vs. 3.943 ; $U = 6919$; $p = .023$). Students also reported strong concern about avatar-related identity threats ($M = 4.048$ vs. 4.013 ; $U = 6826$; $p = .040$), showing that perceived risk extends beyond conventional e-commerce issues to metaverse-specific identity exposure. Payment-related risk was slightly lower but still above the midpoint, including fear that payment or banking information could be misused ($M = 3.794$ vs. 3.835 ; $U = 7090$; $p = .008$). Concern about real-world online identity theft was similarly high ($M = 3.905$ vs. 3.918 ; $U = 6796$; $p = .048$). Across items, programme differences are statistically detectable but small in magnitude, which suggests that elevated security risk perceptions are broadly shared across disciplines rather than concentrated in one field.

Spearman correlations were used to describe bivariate associations (Table 4). The hypothesised relationships were then examined using two complementary multivariate approaches: hierarchical regression, with gender and age entered as controls, and PLS-SEM as a robustness check. In the hierarchical regression, Model 0 included gender and age, and Model 1 added metaverse knowledge, perceived value, and perceived security risk. Model 1 provided a significant improvement over Model 0 ($R^2 = .146$ vs. $.018$; $\Delta R^2 = .128$, $p < .001$), and the control variables

Table 1. Perceived value of metaverse e-commerce (Source: Created by the authors).

Statement	Mann-Whitney U test		Mean	
	U	p	Business and Economics programs (63)	STEM programs (158)
Clear and easy-to-understand product information in a metaverse store would make me more willing to shop there.	7170	0.004	3.524	3.551
Receiving attractive benefits or rewards would make metaverse shopping worthwhile for me.	7362	< .001	3.698	3.557
Having the option to shop anonymously in the metaverse would be an important advantage for me.	5642	0.382	3.54	3.544
Feeling that I belong and am welcome in a metaverse store would improve my overall shopping experience.	5147	0.045	3.429	3.494
Having options that are tailored to me would increase the benefit I get from metaverse shopping.	4775	0.005	3.794	3.639
Being able to speak with a customer-support agent or brand representative similar to me would make metaverse shopping more appealing.	4799	0.006	3.254	3.449
If metaverse shopping felt familiar and similar to what I am used to at home, I would be more inclined to use it.	5606	0.324	3.333	3.291
Opportunities to interact with others who share my interests would make metaverse shopping more attractive to me.	5445	0.187	3.429	3.5
Having the chance to explore a different way of shopping in the metaverse would be a meaningful benefit for me.	5714	0.468	3.302	3.266

Table 2. Perceived security risk (Source: Created by the authors).

Statement	Mann-Whitney U test		Mean	
	U	p	Business and Economics programs (63)	STEM programs (158)
I am concerned that my real-world online identity could be stolen if I shop in the metaverse.	6796	0.048	3.905	3.918
I am concerned that my personal data could be collected and sold to third parties when I use metaverse stores.	6919	0.023	4.127	3.943
I am concerned that my device could be hacked when I access metaverse platforms.	7070	0.008	4.19	4.171
I am concerned that my network or account credentials could be compromised when I use the metaverse.	6863	0.03	4.143	4.101
I am concerned that my payment or banking information could be misused when I pay in the metaverse.	7090	0.008	3.794	3.835
I am concerned that my metaverse avatar could be hacked or used to steal my identity.	6826	0.04	4.048	4.013

Table 3. Model Summary - Metaverse e-commerce purchase intention (Source: Created by the authors).

Model	R ²	R ² Change	F Change	p
M ₀	0.018	0.018	0.993	0.412
M ₁	0.146	0.128	10.639	< .001

Note. M₀: Gender, Age. M₁: Gender, Age + Metaverse knowledge, Perceived value, Perceived security risk.

were not statistically meaningful and did not alter the focal estimates. The PLS-SEM model showed comparable explanatory power ($R^2 = .177$; adjusted $R^2 = .166$). Statistical inference was strengthened using bias-corrected bootstrapping (5,000 resamples) for both the regression coefficients and the PLS-SEM paths, and Table 5 reports the standardised coefficients side-by-side.

– H1. Metaverse knowledge and perceived value are positively associated with metaverse e-commerce purchase intention. ($\alpha = 0.05$)

Table 4 shows that metaverse knowledge is positively associated with metaverse e-commerce purchase intention ($p = .249, p < .001$), indicating that students with a stronger understanding of the metaverse report higher intention to shop in immersive environments. This finding is consistent with prior work suggesting that knowledge reduces uncertainty and supports more confident evaluation of emerging digital contexts (Jafar et al., 2023). Perceived value exhibits an even stronger positive association with purchase intention ($p = .400, p < .001$), implying that students who perceive clearer benefits are substantially more inclined to adopt metaverse shopping. This pattern aligns with UTAUT2 and related evidence positioning perceived benefits and value as proximal determinants of behavioural intention in consumer technology settings (Pillai et al., 2024; Venkatesh et al., 2012).

The multivariate results reinforce these bivariate patterns (Table 5). In the hierarchical regression model controlling for gender and age, metaverse knowledge remains a significant predictor ($\beta = .21, p < .01$) and perceived value remains the strongest positive predictor ($\beta = .278, p < .001$). The PLS-SEM estimates show the same ordering ($\beta = .26$ and $\beta = .318$), supporting the stability of the effects across analytical approaches. Overall, the evidence supports H1, with perceived value emerging as the stronger enabling factor.

– H2. *Perceived security risk is negatively associated with metaverse e-commerce purchase intention. ($\alpha = 0.05$)*

Table 4 indicates a negative association between perceived security risk and metaverse e-commerce purchase intention ($p = -0.118, p = .040$). This bivariate association is statistically significant but small in magnitude, suggesting that perceived security risk plays a modest constraining role rather than being a central determinant of purchase intention. In the hierarchical regression model, perceived security risk remains a significant negative predictor after controlling for gender and age ($\beta = -0.154, p < .05$; Table 5). The PLS-SEM results show the same directional relationship ($\beta = -0.176$), providing convergent support across analytical approaches.

This pattern is consistent with privacy-calculus accounts, which argue that perceived losses and uncertainty can suppress willingness to transact in data-intensive environments even when benefits are recognised (Dinev & Hart, 2006; Pavlou, 2003). It also aligns with e-commerce evidence that privacy and security concerns, including fears of identity or credential misuse, reduce purchase intention (Handoyo, 2024; Hille et al., 2015). In metaverse commerce, where identity, behavioural traces, and transactions may be tightly linked, such concerns can remain salient adoption constraints (Kirmani et al., 2025; Laiz-Ibanez et al., 2025). Substantively, the results support H2, but they also indicate that security risk operates as a secondary constraint rather than a primary driver.

Table 4. Spearman's Correlations (Source: Created by the authors).

Independent Variable	Dependent Variable	Spearman's rho	p
Metaverse knowledge	- Metaverse e-commerce purchase intention	0.249***	< .001
Perceived value of metaverse e-commerce	- Metaverse e-commerce purchase intention	0.4***	< .001
Perceived security risk	- Metaverse e-commerce purchase intention	-0.118*	0.04

* $p < .05$, ** $p < .01$, *** $p < .001$.

Table 5. Predictors of metaverse e-commerce purchase intention (Source: Created by the authors).

Predictors	Hierarchical regression (β)	PLS-SEM (β)
Metaverse knowledge	0.21**	0.26
Perceived value of metaverse e-commerce	0.278***	0.318
Perceived security risk	-0.154*	-0.176
Model statistics		
R ²	0.146	0.177
Adjusted R ²	0.118	0.166

Conclusions

This study examined how metaverse knowledge, perceived value and perceived security risk relate to Albanian university students' intention to engage in metaverse e-commerce. Grounded in the privacy-calculus perspective (Dinev & Hart, 2006), technology-acceptance models such as UTAUT2 (Venkatesh et al., 2012) and recent metaverse research (Jafar et al., 2023; Kirmani et al., 2025; Pillai et al., 2024), the results portray an early-adopter cohort that is curious about metaverse shopping but remains cautious.

Two substantive patterns emerge. First, students' metaverse knowledge is moderate but uneven: familiarity is higher for basic concepts and commercial applications, and lower for VR/AR/XR technologies as well as ethics and privacy issues. Second, perceived value is moderately positive, with the strongest endorsements for personalisation, rewards, information clarity, and social or experiential benefits. Consistent with these descriptive patterns, the bivariate results show that metaverse knowledge ($p = .249$, $p < .001$) and perceived value ($p = .4$, $p < .001$) are positively associated with purchase intention, whereas perceived security risk is negatively associated ($p = -.118$, $p = .040$). While statistically detectable, the security-risk association is modest in magnitude, suggesting a constraining influence rather than a dominant driver of intention. The multivariate evidence converges across modelling approaches: the hierarchical regression indicates a meaningful improvement from the control model to the full model ($\Delta R^2 = .128$, $p < .001$; $R^2 = .146$), and the PLS-SEM model shows comparable explanatory power ($R^2 = .177$; adjusted $R^2 = .166$). Overall, the findings support a benefit-risk account of metaverse e-commerce intention, with perceived value emerging as the strongest enabling factor.

The findings imply actionable priorities for stakeholders. For universities and policymakers, metaverse initiatives should be accompanied by targeted literacy programmes that explicitly address VR/AR/XR foundations, data protection, and digital rights, enabling more informed benefit-risk judgments. For firms and platform providers, effective metaverse retail offerings should combine value delivery with visible security-by-design. Priority safeguards include multi-factor authentication and step-up verification for sensitive actions (payments, wallet linking, privacy-setting changes), secure account recovery, anomaly detection and user alerts, and identity governance to reduce avatar impersonation and strengthen reporting and remediation pathways. Transparency dashboards should communicate what data are collected and why, disclose relevant recipients, and enable users to adjust sharing, limit personalisation, and access, export, or delete their data.

For practical uptake, the findings can be translated into a staged implementation scenario. First, institutions and providers can run baseline assessments of metaverse literacy and perceived risk to identify the most sensitive points. Second, pilot metaverse stores should combine clear value cues with visible safeguards. Third, pilots should be evaluated using intention and behavioural proxies to refine forecasts of adoption as safeguards and user knowledge mature.

Future research should employ longitudinal and cross-country designs and complement self-reported intentions with behavioural evidence from VR shopping environments, including interaction logs, dwell time, and, where feasible, eye-tracking, to test whether intentions translate into purchasing behaviour. By linking the benefit-risk structure to scenario-based adoption conditions and evidence-supported mitigations, the study increases the developmental output value of its findings for future pilots and forecasting. Changes in perceived security risk and metaverse literacy may serve as leading indicators of whether intention is likely to convert into metaverse purchasing behaviour as safeguards and user knowledge mature (Dinev & Hart, 2006; Handoyo, 2024).

References

- Ahn, S., Jin, B. E., & Seo, H. (2024). Why do people interact and buy in the Metaverse? Self-Expansion perspectives and the impact of hedonic adaptation. *Journal of Business Research*, 175, 114557. <https://doi.org/10.1016/j.jbusres.2024.114557>
- Atari Interactive, Inc. v. Redbubble, Inc. (2021). 515 F. Supp. 3d 1089 (N.D. Cal. 2021). <https://case-law.vlex.com/vid/atari-interactive-inc-v-886135366>
- COWEB. (2025). *Project results: COWEB*. <https://www.cowebproject.eu/>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Eulaerts, O., Grabowska, M., & Bergamini, M. (2025). *Weak signals in science and technologies 2024*:

- Technologies at an early stage of development that could impact our future*. Publications Office of the European Union. <https://doi.org/10.2760/6571994>
- European Commission. (2025). *TIM analytics: Tools for innovation monitoring (TIM)*. European Commission, Joint Research Center. <https://www.timanalytics.eu/>
- European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Official Journal of the European Union, L119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Parliament. (2024). *Virtual worlds – opportunities, risks and policy implications for the single market*. European Parliament. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0032_EN.html
- European Union Intellectual Property Office. (2024). *Impact of the metaverse on infringement and enforcement of intellectual property: Impact of technology deep dive report II*. European Union Intellectual Property Office. <https://doi.org/10.2814/4732968>
- Handoyo, S. (2024). *Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce*. *Heliyon*, 10(8), e29714. <https://doi.org/10.1016/j.heliyon.2024.e29714>
- Hendricks, S., & Mwapwele, S. D. (2024). A systematic literature review on the factors influencing e-commerce adoption in developing countries. *Data and Information Management*, 8(1), 100045. <https://doi.org/10.1016/j.dim.2023.100045>
- Hermès International v. Rothschild. (2023). *WL 1458126 (S.D.N.Y. Feb. 2, 2023)*. <https://www.wipo.int/wipolex/en/judgments/details/1841>
- Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, 30, 1–19. <https://doi.org/10.1016/j.intmar.2014.10.001>
- Jafar, R. M., Ahmad, W., & Sun, Y. (2023). Unfolding the impacts of metaverse aspects on telepresence, product knowledge, and purchase intentions in the metaverse stores. *Technology in Society*, 74, 102265. <https://doi.org/10.1016/j.techsoc.2023.102265>
- Jafar, R. M., Ahmad, W., & Chen, Y. (2024). Metaverse in human behavior: The role of telepresence and flow experience on consumers' shopping behavior in the metaverse. *SAGE Open*, 14(2). <https://doi.org/10.1177/21582440241261256>
- JASP (2025). *JASP (Version 0.95.0)*[Computer software]. <https://jasp-stats.org/>
- Kirmani, M. D., Sadiq, M. A., Uddin, S. M., Adil, M., Ahmad, A., Asadul Haque, M., & Thaichon, P. (2025). Negative perceptions, attitudes, and adoption intentions: Unravelling metaverse adoption challenges. *Journal of Consumer Behaviour*, 24(6), 2872–2896. <https://doi.org/10.1002/cb.70036>
- Laiz-Ibanez, H., Mendaña-Cuervo, C., & Carus Candas, J. L. (2025). The metaverse: Privacy and information security risks. *International Journal of Information Management Data Insights*, 5(2), 100373. <https://doi.org/10.1016/j.jjime.2025.100373>
- Noor, U., Mansoor, M., Khan, T. I., & Khattak, M. N. (2025). The zenith of flow consciousness in metaverse: Glancing the consumer behavior in the future. *International Journal of Consumer Studies*, 49(5), e70120. <https://doi.org/10.1111/ijcs.70120>
- Parliament of Albania. (2024). *Law No. 124/2024 on Personal Data Protection*. <https://qbz.gov.al/eli/ligj/2024/12/19/124>
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- Pillai, R., Sivathanu, B., Rana, N. P., & Struweg, I. (2024). Assessing the determinants of metaverse adoption for e-commerce retailing. *Journal of Computer Information Systems*, 1–20. <https://doi.org/10.1080/08874417.2024.2416452>
- Shen, B., Tan, W., Guo, J., Zhao, L., & Qin, P. (2021). How to promote user purchase in metaverse? A systematic literature review on consumer behavior research and virtual commerce application design. *Applied Sciences*, 11(23), 11087. <https://doi.org/10.3390/app112311087>
- Soni, S., Arora, P., Kasilingam, D., & Jain, V. (2025). Digital daydreams: Exploring consumer motivations for engaging with the metaverse. *Journal of Retailing and Consumer Services*, 85, 104294. <https://doi.org/10.1016/j.jretconser.2025.104294>
- VALEU-X. (2022). *Results: VALEU-X*. <https://valeu-x.eu/>
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157–178. <https://doi.org/10.2307/41410412>
- Zhong, Z., & Hamouda, M. (2024). The impact of immersive and flow experiences on consumer participation in hyper-connected shopping platforms: A metaverse perspective. *Journal of Consumer Behaviour*, 23(6), 2826–2845. <https://doi.org/10.1002/cb.2377>