Journal of Theoretical and Applied Information Technology
15th September 2019. Vol.97. No 17
© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A QUANTITATIVE MODEL OF DETERMINANTS OF USE BEBAVIOR FOR THE CRYPTOCURRENCY SYSTEM IN TERMS OF SECURITY CONCERNS AND RISKS

[1]YOUNG-HO HWANG, [2]YOO-JIN MOON

[1]First Author: Kunsan National University, Gunsan, Republic of Korea

[2]Corresponding Author: Hankuk University of Foreign Studies, Seoul, Republic of Korea

E-mail: [1]yhwang@kunsan.ac.kr, [2]yjmoonmis@naver.com

ABSTRACT

The paper performs quantitative analysis of moderating effects of security concerns and risks for management of cryptocurrency systems and proposes solutions for security concerns and risks. The results show some important implications for the management of cryptocurrency systems. Particularly, performance expectancy can be headed for management and system design strategies of cryptocurrency service providers, and the cryptocurrency systems should be elaborated in the pleasant and beneficial way. This paper also illustrates that perceived security concerns and perceived risks might negatively affect cryptocurrency use and trading. Based on the research results, security concerns and risks prove that they are very important interaction variables as a great interest for cryptocurrency users. For the safe transmission of cryptocurrency in the financial industries, the paper suggests that Korean Article 49 of the Enforcement Decree of Information and Communication Network Act should require higher standards to the cryptocurrency exchange markets. For the safe transactions of cryptocurrency, the paper suggests three solutions for security concerns and risks relevant to the cryptocurrency exchange markets.

Keywords: *Cryptocurrency, Use Behavior, Performance Expectancy, Social Influence, Hedonic Motivation, Security Concerns, Risks*

1. INTRODUCTION

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, to control the creation of additional units, and to verify the transfer of assets [1, 2, 3]. A cryptocurrency aspires to be a new form of currency and promises to maintain trust in the stability of its value through use of technology. It consists of three elements. First, a set of rules (the ‘’protocol’’), computer code specifying how participants can transact. Second, a ledger storing the history of transactions. Third, a decentralized network of participants that update, store and read the ledger of transactions following the protocol [4]. With these elements, advocates claim, a cryptocurrency is not subject to the potentially misguided incentives of banks and sovereigns. A cryptocurrency is a kind of digital currency, virtual currency and alternative currency. Cryptocurrencies utilize decentralized control as opposed to centralized E-money and central banking systems [5, 6]. While all cryptocurrencies rely on a distributed ledger, they differ in terms of how the ledger is updated [7, 8, 9].

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined, when the system is created, and which is publicly known. More important use cases are likely to combine crypto-payments with sophisticated self-executing codes and data permission systems. Some decentralized cryptocurrency protocols such as Ethereum already allow for smart contracts that self-execute the payment flows for derivatives. At present, the efficacy of these products is limited by the low liquidity and intrinsic inefficiencies of permission less cryptocurrencies [4]. In case of decentralized cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which hold asset value measured in it. The underlying technical system on which decentralized cryptocurrencies are based, was created by the group or individual known as Satoshi Nakamoto [10].

As of May 2018, over 1,800 cryptocurrency specifications existed [11]. With the growing popularity of the crypto market, the large number of unregulated cryptocurrencies (several hundreds), greater attention is now being paid by governments and other stakeholders around the world. Illustrative is that the total market capitalization of the 100 largest cryptocurrencies is reported to exceed the equivalent of EUR 330 billion globally by early 2018 [12]. Regulators are looking at whether — and how — to regulate cryptocurrencies. Until now there is no univocal view on how to do that. In any event, there are compelling reasons why cryptocurrencies should be under more scrutiny by regulators and supervisors. The threat of price volatility, speculative trading, hack attacks, money laundering and terrorist financing all call for stricter regulation [13]. Within the cryptocurrency system the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: who use their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a certain timestamping scheme [14].

A good many of cryptocurrencies are designed to gradually reduce production of that currency, placing a cap on the total amount of that currency that will ever be in circulation [15]. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement [1]. This difficulty derived from leveraging cryptographic technologies.

The purpose of this research is to address empirical analysis of effects of revised UTAUT factors on use behavior of cryptocurrency and moderating effects between the factors. For the safe transactions of cryptocurrency, the paper suggests three solutions for security concerns and risks in the aspect of law relevant to the cryptocurrency exchange markets. Based on the research it could be found how cryptocurrency's users (including potential users) behave, regarding use and trading of cryptocurrency.

2. THEORETICAL BACKGROUND: CRYTOCURRENCY

Due to the anonymity in the night market, the exchange of goods necessitates a means of payment which we assume is a cryptocurrency. A cryptocurrency is a digital record-keeping device that uses balances to keep track of the obligations from trading and that is publicly known to all traders. A cryptocurrency system is defined by two parameters: money growth rate $\mu \geq 0$ and transaction fee charge at a rate $\tau \geq 0$. As discussed, the digital nature of these balances results in the double-spending problem. In what follows, we describe the features of a ledger that records the transfers of these balances [16].

2.1 Aggregate State

Each trader is entitled to a balance. *Let* $m_t^D(i) \geq 0$ denote the balance associated with agent i in the period t day market. We then use $S_t^D = \{m_t^D(i)\}$ to denote the entire public record of these balances, called the *(aggregate)* state. Similarly, $m^N_{t,n}(i) \geq 0$ and $S^N_{t,n}$ denote the balances and the state at the beginning of the nth trading session of the period t night market. The economy starts with a given initial state S^D_0.

2.2 Payments

We use $\Delta^D_t(i,j)$ and $\Delta^N_{t,n}(i,j)$ to denote respectively day and night transfers of balances from agent i to agent j and call these transfers payments. A day payment is feasible if

$$\Delta^D_t(i,j) \geq 0, \quad (1)$$

$$m_t^D(i) \geq \sum \Delta^D_t(i,j). \quad (2)$$

Similarly, a night payment is feasible if

$$\Delta^N_{t,n}(i,j) \geq 0, \quad (3)$$

$$m^N_{t,n}(i) \geq \sum \Delta^N_{t,n}(i,j). \quad (4)$$

A trader can pay positive amounts to others and the total payments are bounded by the balances one has accumulated.8 Given any payments the state is then updated in the two markets according to

$$m^N_{t,0}(i) = m_t^D(i) + \sum_j \Delta^D_t(j,i) - \Delta^D_t(i,j) + T_t(i), \quad (5)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$m^{N}_{t,n}(i) = m_{t,n-1}{}^{D}(i) + \sum_{j} \Delta^{N}{}_{t,n-1}(j, i) - \Delta^{N}_{t,n-1}(i, j),$$

for n = 1, ….. $\overline{N}$ (6)

$$m_{t+1}{}^{D}(i) = m^{N}_{t,\tilde{N}}(i) + \sum_{j} \Delta^{N}{}_{t,\tilde{N}}(j, i) - \Delta^{N}_{t,\tilde{N}}(i,j) \quad (7)$$

where $T(i)$ is the transfer of new balances to agent i.

3. RESEARCH METHODOLOGY

3.1 Research Model

The objective of this research is to study, understand and identify the factors that affect the acceptance and use of cryptocurrency services by utilizing the power of revised UTAUT model. It also aims to investigate and analyze the fundamental relationships among the proposed research model constructs and moderating effects of security concerns and risks on cryptocurrency system.

The research utilizes the Venkatesh et al.'s UTAUT model as a theoretical driver for this study [17]. However, a revised version of the UTAUT will be utilized to suit the context of the study and to achieve its aim. The original UTAUT model contains four direct independents (effort expectation, performance expectation, social influence, facilitating conditions) of behavioral intention and use behavior [18]. In this research, independent variable, 'facilitating conditions', was omitted, hedonic motivation was chosen as a substitute for facilitating conditions. And additionally, two new constructs, security concerns and risks, have been added, so there are six independent variables (effort expectancy, performance expectancy, social influence, hedonic motivation, security concerns, risks) and one dependent variable (use behavior) as follows.

The independent variables in the proposed research model are presented below:

1. Effort expectancy (E-E) - the degree of ease associated with the use of the system. Effort expectancy will be measured by the perceptions of the ease of use of cryptocurrency services, as well as the ease of learning how to use these services [16].

2. Performance expectancy (P-E) – the degree to which individuals believe that using a system will help them improve their job performance. Performance expectancy will be measured by the perceptions of using cryptocurrency services in terms of benefits, such as saving time, money and effort and improving the quality of cryptocurrency services [17].

3. Social influence (S-I) – the degree of which peers and important people influence the use of the system, whether positive or negative. Social influence is a main factor in many aspects of the lives of young people and is likely to be powerful. This variable will be measured by the perception of how peers and important people affect my use of cryptocurrency services [19].

4. Hedonic motivation (H-M) – the degree of pleasure or enjoyment derived from using cryptocurrency services. Hedonic motivation will be measured by perception of how user enjoys using the cryptocurrency services [20].

5. Security concerns (S-C) – the degree to which users feel that using the cryptocurrency system will cause security concerns. Security concerns will be measured by the perception of potential loss due to fraud or hacking compromising insecurity of the cryptocurrency services [21].

6. Risks (R-S) - the degree of uncertainty using the cryptocurrency systems. Risks will be measured by the perception of the uncertainty in the cryptocurrency transaction situation [22].

7. Use behavior (U-B) – the degree of the actual use behavior and potential use behavior of the cryptocurrency systems. Use behavior will be measured by the actual use behavior that is dominated by behavioral intention. But, in this research use behavior will be measured by the intention, prediction, and planned use of cryptocurrency services [18].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

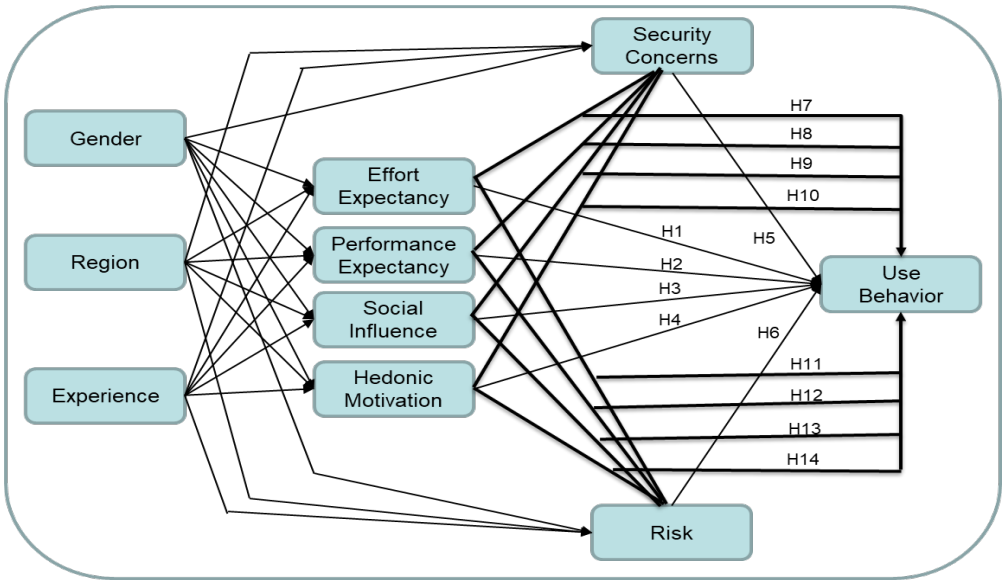

Figure 1: The Proposed Research Model

3.2 Research Hypotheses

Taking into account relationships and constructs of the revised UTAUT, we put forward the following hypotheses in respect of cryptocurrency.

3.2.1 Key Constructs Hypotheses

The key constructs hypotheses are the direct relationships between the seven constructs in the proposed research model as presented in Figure 1. This set of hypotheses addresses the relationship between six independent variables and one dependent variable.

H-1: A user's effort expectancy (E-E) would have a positive influence on use behavior of cryptocurrency.

H-2: A user's performance expectancy (P-E) would have a positive influence on use behavior of cryptocurrency.

H-3: A user's social influence (S-I) would have a positive influence on use behavior of cryptocurrency.

H-4: A user's hedonic motivation (H-M) would have a positive influence on use behavior of cryptocurrency.

H-5: A user's perceived security concerns (S-C) would have a negative influence on use behavior of cryptocurrency.

H-6: A user's perceived risks (R-S) would have a negative influence on use behavior of cryptocurrency.

3.2.2 Moderating Hypotheses

The moderating hypotheses are the set of hypotheses that will be tested for moderators. The revised research model considers the influence of two moderators which are: security concerns and risks. Therefore, this study is investigating the impact of these moderators on use behavior of cryptocurrency services.

H-7: A user's perceived security concerns (S-C) mediates the relation between his/her effort expectancy and use behavior of cryptocurrency.

H-8: A user's perceived security concerns (S-C) mediates the relation between his/her performance expectancy and use behavior of cryptocurrency.

H-9: A user's perceived security concerns (S-C) mediates the relation between his/her social influence and use behavior of cryptocurrency.

H-10: A user's perceived security concerns (S-C) mediates the relation between his/her hedonic motivation and use behavior of cryptocurrency.

H-11: A user's perceived risks (R-S) mediates the relation between his/her effort expectancy and use behavior of cryptocurrency.

H-12: A user's perceived risks (R-S) mediates the relation between his/her performance expectancy and use behavior of cryptocurrency.

H-13: A user's perceived risks (R-S) mediates the relation between his/her social influence and use behavior of cryptocurrency.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

H-14: A user's perceived risks (R-S) mediates the relation between his/her hedonic motivation and use behavior of cryptocurrency.

3.3 Data Collection Strategies

3.3.1 Questionnaires

Questionnaire are self-reported data collection instruments which are answered at a distance from the researcher. A high quality of a question and questionnaire design gives the researcher high valid and reliable measures that also will help the participants to understand the questions and answer them with the appropriate response [23]. The survey was designed to include a two-part questionnaire. The first part includes seven-point Likert scales. A Likert scale is appropriate when the research needs to measure the respondent's attitude towards constructs [24]. The survey consists of 21 items to measure the constructs. And the second part includes nominal scales using the demographic data.

Items selected of the questionnaire for measuring the constructs in our research model were adapted from prior studies. With regard with implementing the questionnaire in this study, the researcher followed Leedy's four practical guidelines to develop the questionnaire draft as follows: using clear language; meeting research aims; planning the development, sample, distribution, and collection of the questionnaire; and creating a solid cover letter [25].

3.3.2 Data Collection and Analytical Methods

Gray defines a population as the entire number of possible groups or elements that the researcher wishes to include in this study [26]. With regard with the population of this study, this researcher is targeting the undergraduate students, which are participated in this research from a public Korean university in the southwestern region and a private Korean university in the metropolitan area. To identify demographics of the respondents, frequency analysis and ANOVA were performed based on a total of 226 samples. Then, this research performed the exploratory factor analysis to ensure the content validity of the scales. This research also tested reliability. Lastly, 'multiple regression' analysis and 'Smart Partial Least Squares' analysis was conducted.

4. QUANTITATIVE ANALYSIS AND HYPOTHESIS VERIFICATION

4.1 Frequency Analysis

This study used purposive and non-probability sampling. Those who were questioned in this study were voluntary participants. A total of 230 questionnaires were distributed, of which 226 questionnaires were collected with the respondent rate 98.3%. Table 1 showed that 56.6 % of the respondents were male, and 43.4 % were female. In terms of experience, 11.1 % were cryptocurrency users. And 50 % of respondents lived in Seoul and 50 % lived in regional area. Table 2 illustrated descriptive statistics. While effort expectancy and hedonic motivation showed moderate level and risks showed fairly high level, performance expectancy, social influence and security concerns showed a little low level and use behavior showed fairly low level.

Table 1: Frequency Analysis

Item	Category (%)	
Gender	Male (56.6)	Female (43.4)
Experience	Experience (11.1)	Non-experience (88.9)
Region	Seoul (50)	Regional (50)

Table 2: Descriptive Statistics

	N	Min. Value	Max. Value	Mean	Standard Dev.	Variance
E-E.	226	1.00	7.00	4.0782	1.57238	2.472
P-E.	226	1.00	7.00	3.6445	1.58481	2.512
S-I	226	1.00	7.00	3.0531	1.46705	2.152
H-M.	226	1.00	7.00	3.9027	1.57020	2.466
S-C.	226	1.00	7.00	3.1350	1.59810	2.554
R-S	226	1.00	7.00	4.9204	1.50491	2.265
U-B	226	1.00	7.00	2.8997	1.71896	2.955
N	226					

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2 ANOVA

As illustrated in Table 3, results of ANOVA demonstrated that significant differences did exist at the level of α=.05 between effort expectancy and gender, between effort expectancy and experience, between performance expectancy and experience, between social influence and experience, between hedonic motivation and experience, between use behavior and experience, and between hedonic motivation and residency.

Table 3: Results of ANOVA

		Sum of Squares	Degree of Freedom	Mean Square	F	p-value
E-E * Gender	Between Group	16.571	1	16.571	6.877	.009
	Within Group	539.715	224	2.409		
	Total	556.286	225			
E-E * Experience	Between Group	58.446	2	29.223	13.090	.000
	Within Group	497.839	223	2.232		
	Total	556.286	225			
P-E * Experience	Between Group	47.929	2	23.965	10.333	.000
	Within Group	517.182	223	2.319		
	Total	565.112	225			
S-I * Experience	Between Group	17.336	2	8.668	4.140	.017
	Within Group	466.916	223	2.094		
	Total	484.252	225			
H-M*Experience	Between Group	21.352	2	10.676	4.463	.013
	Within Group	533.396	223	2.392		
	Total	554.747	225			
U-B* Experience	Between Group	37.744	2	18.872	6.711	.001
	Within Group	627.093	223	2.812		
	Toral	664.838	225			
P-E * Region	Between Group	10.624	1			
	Within Group	554.488	224	10.624	4.292	.039
	Total	565.112	225			
H-M * Region	Between Group	29.270	1	29.270	12.477	.001
	Within Group	525.477	224	2.346		
	Total	554.747	225			

4.3 Test of Reliability and Validity

The reliability of a measure refers to the degree to which the instrument is free of random error. It is concerned with the consistency and stability of the measurement. Hair et al. mentioned that construct reliability should be .7 or higher to indicate adequate convergence or internal consistency [27]. In this study, there were seven scales used in the survey questionnaire to measure the constructs proposed in the model. The reliability scores are highly satisfactory. In Table 4, standardized

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Cronbach's α values for each construct ranged from .927 to .946, and all values were above the recommended value of .7 [28].

Construct validity is defined as the degree to which an operational measure correlates with the theoretical concept being investigated. According to Turocy, factor analysis is most often associated with construct validity and considered one of the analytic tools to assess construct validity [29]. In this study, the validity and the unidimensional measurement scale was assessed by using exploratory factor analysis and an examination of the correlation coefficients for all of instrument scales. Generally, factor loadings below .4 are considered low, and low-loading items should be suppressed [27]. In this study, the recommended cut-off factor loading of .50 was used to ensure that all variables had practical significance [27]. Moreover, the researcher assessed sampling adequacy by examining the Kaiser-Meyer-Olkin (KMO) output provided in the factor analysis. A KMO correlation above .60 to .70 is considered adequate for analyzing the exploratory factor analysis output [29]. As Table 5 shows, the KMO statistic is .87477, which is above the minimal acceptable level. As shown in Table 5, this research verified validity of the structural model (n=226), by conducting the exploratory factor analysis based on principal components analysis and Varimax Rotation [20]. All seven factors were extracted. Each factor showed that an Eigen value was above 1.

Table 4: Results of Reliability Analysis

	Scale Mean	Scale Variance	Total Correlation Coefficient	Squared Multiple Correlation Coefficient	Cronbach Alpha
E-E1	70.7832	503.415	.584	.603	**.931**
E-E2	71.1195	491.403	.703	.690	**.929**
E-E3	71.2080	493.721	.704	.743	**.929**
P-E1	71.5575	494.879	.760	.776	**.928**
P-E2	71.3009	491.358	.727	.768	**.929**
P-E3	71.5531	489.759	.776	.828	**.928**
S-I1	71.9027	503.635	.646	.720	**.930**
S-I2	71.9956	499.311	.712	.797	**.929**
S-I3	72.2876	495.495	.765	.831	**.928**
H-M1	71.6947	493.591	.727	.655	**.929**
H-M2	70.9558	497.056	.663	.780	**.930**
H-M3	70.9867	496.938	.675	.805	**.930**
S-C1	72.1416	489.998	.760	.838	**.928**
S-C2	71.6947	497.706	.645	.758	**.930**
S-C3	71.9425	493.370	.751	.862	**.928**
S-C4	72.1416	494.060	.699	.751	**.929**
R-S1	70.3274	578.390	-.390	.784	**.946**
R-S2	70.0619	578.929	-.396	.788	**.946**
U-B1	71.8761	480.456	.812	.885	**.927**
U-B2	72.2566	483.632	.804	.915	**.927**
U-B3	72.5133	494.509	.725	.799	**.929**

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 5: Exploratory Factor Analysis

	Re-scaled component						
	1	2	3	4	5	6	7
S-C2	**.868**	.089	.196	.172	.163	.104	.104
S-C3	**.813**	.256	.205	.224	.103	.224	.168
S-C1	**.754**	.337	.172	.229	.103	.263	.195
S-C4	**.748**	.209	.218	.177	.153	.186	.278
S-I1	.222	**.840**	.106	.115	.209	.189	.063
S-I2	.186	**.796**	.188	.218	.262	.146	.208
S-I3	.316	**.748**	.167	.163	.241	.280	.198
H-M2	.207	.098	**.861**	.205	.195	.128	.041
H-M3	.245	.086	**.849**	.196	.200	.157	-.018
H-M1	.184	.324	**.687**	.173	.230	.241	.124
E-E1	.255	.026	.265	**.810**	.122	.036	-.002
E-E3	.176	.215	.180	**.805**	.240	.189	.098
E-E2	.202	.268	.120	**.727**	.303	.219	.017
P-E2	.182	.215	.239	.297	**.807**	.135	.101
P-E3	.159	.313	.279	.256	**.747**	.226	.140
P-E1	.154	.312	.264	.214	**.700**	.308	.115
U-B2	.281	.262	.262	.245	.262	**.746**	.231
U-B3	.321	.338	.158	.118	.220	**.715**	.238
U-B1	.280	.221	.356	.234	.287	**.692**	.233
R-S2	-.185	-.139	-.040	-.031	-.113	-.187	**-.908**
R-S1	-.227	-.144	-.035	-.035	-.087	-.141	**-.908**
Eigen Value	**33.538**	**5.520**	**4.218**	**3.466**	**2.692**	**2.086**	**1.803**
Explained Var. (%)	**55.020**	**9.056**	**6.920**	**5.686**	**4.416**	**3.422**	**2.958**
KMO (%)	**87.477**						

Extraction: Principal Component Analysis. Rotation: Varimax with Kaiser normalization

4.4 Multiple Regression Analysis

The results of multiple regression analysis illustrated that five of the six suggested hypotheses turned out to be significant, as shown in Table 6. This research used multiple regression analysis by setting use behavior (U-B) as a dependent variable and six variables (E-E, P-E, S-I, H-M, S-C, R-S) as independent variables.

As shown in Table 6, the results of multiple regression analysis showed the results of hypothesis verification.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

H-1 was rejected because E-E did not influence on U-B significantly at the level of α= .05 (ß= .063, $p \leq$ .240). Effort expectancy means perceived ease of use for predicting adoption of new technologies.

H-2 was accepted because U-B was significantly influenced by P-E at the level of α= .05 (ß= .231, $p \leq$ .000). Performance expectancy means the degree of perceived usefulness. This research indicated that the higher the performance expectancy was, the higher use behavior of cryptocurrency services was.

H-3 was accepted because S-I had a positive influence on U-B significantly at the level of α= .05 (ß= .195, $p \leq$ .001). Social influence may occur when an individual's opinions, feelings or actions are affected by other people.

H-4 was accepted because H-M had a positive influence on U-B significantly at the level of α= .05 (ß= .190, $p \leq$ .000). The higher perceived enjoyment was, the higher use behavior of cryptocurrency services was.

H-5 was accepted because S-C had a negative impact on U-B significantly at the level of α= .05 (ß= -.201, $p \leq$ .000). Security concerns will be measured by the perception of potential loss due to fraud or hacking compromising insecurity of the cryptocurrency services. The lower security concerns was, the higher use behavior of cryptocurrency services was.

H-6 were accepted because R-S had a negative impact on at the level of α= .05 (ß= -.201, $p \leq$ .000). Risks means the degree of the perception of the uncertainty in the cryptocurrency transaction situation. The lower was risks, the higher was use behavior of cryptocurrency services.

Table 6: Results of Multiple Regression Analysis

Dependent Variable	***Independent Variables***	***B***	***Standard Error***	***ß***	***t***	***P-value***	***Accept/Reject***
Use	Constant	.645	.374		1.726	.086	
Behavior	E-E	.069	.058	.063	1.178	.240	Reject
	P-E	**.251**	**.067**	**.231**	**3.750**	**.000**	**Accept**
	S-I	**.229**	**.066**	**.195**	**3.487**	**.001**	**Accept**
	H-M	**.208**	**.058**	**.190**	**3.607**	**.000**	**Accept**
	S-C	**-.216**	**.061**	**-.201**	**-3.562**	**.000**	**Accept**
	R-S	**-.229**	**.051**	**-.201**	**-4.531**	**.000**	**Accept**
R^2				**.690**			
F-value				**81.337**			

4.5 Smart Partial Least Squares (PLS) Analysis

To test moderating effects of security concerns proposed by H-7, H-8, H-9, and H-10, this research followed Chin et al.'s Partial Least Squares Product-Indicator approach [30]. And to test mediating effects of risks proposed by H-11, H-12, H-13, and H-14, this study also followed Chin et al.'s method. Table 7 illustrated the results of testing security concerns and risks factors as mediators. We created the interaction variables by cross-multiplying the items of E-E and S-C, P-E and S-C, S-I and S-C, H-M and S-C, E-E and R-S, P-E and R-S, S-I and R-S, and H-M and R-S. In order to reduce risk of multicollinearity, all items were standardized before multiplication. As shown in Table 7, all mediating effects were significant: interaction between E-E and S-C (ß= 1.206, $p \leq$ .000), interaction between P-E and S-C (ß= 1.275, $p \leq$ .000), interaction between S-I and S-C (ß= 1.112, $p \leq$ .000), interaction between H-M and S-C (ß= 1.211, $p \leq$ .000), interaction between E-E and R-S (ß= 2.408, $p \leq$ .000), interaction between P-E and R-S (ß= 1.488, $p \leq$ .000), interaction between S-I and R-S (ß= 1.245, $p \leq$ .000), and interaction

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

between H-M and R-S (ß= 2.271, $p \leq .000$). Based on these results, hypotheses of H-7, H-8, H-9, H-10, H-11, H-12, H-13, and H-14 were supported. Therefore, we could conclude that a user's security concerns mediated the impacts of E-E, P-E, S-I, and H-M on use behavior of cryptocurrency services, which implies that the higher impacts of E-E, P-E, S-I, and H-M on U-B of cryptocurrency services were, the higher a user's S-C was. We also concluded that a user's risks mediated the impacts of E-E, P-E, S-I, and H-M on use behavior of cryptocurrency services, which implies that the higher impacts of E-E, P-E, S-I, and H-M on U-B of cryptocurrency services were, the higher a user's R-S was.

The proposed model was analyzed using Smart PLS. We evaluate the properties of measurement model and estimate the parameters of the structured model taking into account the mediating latent constructs [21]. In this study, path of the structured model was evaluated. Each path in Figure 2 corresponded to a hypothesis [31]. As shown on Figure 2, the bottom line is that Smart PLS analysis results provided support for the hypotheses of H-7, H-8, H-9, H-10, H-11, H-12, H-13, and H-14.

Table 7: Results of Smart PLS Analysis

Variables	B	SEr	ß	t	P-value	Acc./Rej.
E-E→S-C→U-B	1.319	.134	1.206	9.865	.000	Accept
P-E→S-C→U-B	1.383	.125	1.275	11.103	.000	Accept
S-I→ S-C→U-B	1.303	.108	1.112	12.062	.000	Accept
H-M→S-C→U-B	1.325	.126	1.211	10.480	.000	Accept
E-E→ R-S→U-B	2.632	.689	2.408	3.820	.000	Accept
P-E→R-S→U-B	1.614	.224	1.488	7.202	.000	Accept
S-I→R-S→U-B	1.447	.172	1.235	8.393	.000	Accept
H-M→R-S→U-B	2.486	.590	2.271	4.216	.000	Accept

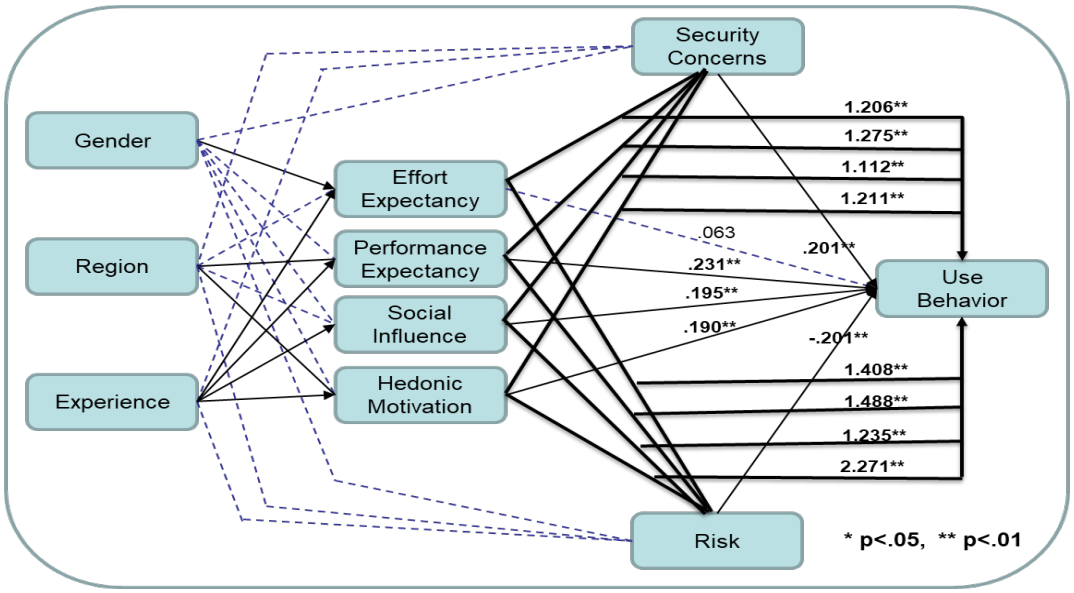

Figure 2: Results of Smart PLS Analysis

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.6 Policy Implications for Security Concerns and Risks

Based on the research results, security concerns and risk have been proved to be important moderating effects as a great interest for cryptocurrency users. Recently, hacking problems of the cryptocurrency exchange markets have occurred in Japan and Korea, which may cause a sudden market contraction [32]. To prevent the hacking of the markets, relevant and complementary measures should be taken for security concerns and risk with regards to the law of the cryptocurrency exchange markets.

Cryptocurrency transmission itself ensures safe exchange processing since it is encrypted for transmission through blockchain network. But there have been many hackings of cryptocurrency through the exchange markets in Japan and Korea.

For the safe transmission in the financial industries, Korean Article 49 of the Enforcement Decree of Information and Communication Network Act requires the Information Security Management System (ISMS) authentication to a company that has a sales figure equal to or higher than 10 billion won for the previous year or that has an average user equal to or higher than 1 million users for 3 months. Even though the ISMS authentication is the minimal security measure for the company, none of Korean cryptocurrency exchange markets satisfied it [33]. Thus, most of the exchange markets for the cryptocurrency are not required to have the ISMS authentication due to their small size and the others neither meet the ISMS standards.

In addition, although the current ordinance can penalize companies that failed to meet the ISMS authentication requirements, Korean government cannot continuously monitor their security activities after companies get the ISMS authentication because of lack of regulations [34]. The government also lacks the interest to regulate these exchange markets because regulating these exchange markets may signify a formal recognition of cryptocurrency as a legal currency, which it is trying to avoid.

For the safe transactions of cryptocurrency, the paper suggests three solutions for security concerns and risk in the aspect of law relevant to the cryptocurrency exchange markets.

First, security breaches and monetary damages experienced by the exchange markets require government regulations. These exchange markets should be regulated similarly to other financial industries which are regulated by the Electronic Financial Supervision and Regulation. The government should specifically focus on Article 8 (Labor Force, Structure and Budget), Article 15 (Hacking Prevention Measures), Article 18 (IP Address Management Plans), Article 22 (Constructing Processing System), Article 34 (Electronic Financial Transactions Compliance), and Article 37 (Authentication Method Standards) of the Electronic Financial Supervision and Regulation.

Second, the standards of Article 49 of the Enforcement Decree of Information and Communication Network Act should lower a sales figure equal to or higher than 10 billion won for the previous year, to encompass the smaller exchange markets.

Third, the standards of Article 49 should lower an average user equal to or higher than 1 million users for 3 months, to encompass the smaller exchange markets. And so, most of the cryptocurrency exchange markets should be regulated by the ISMS.

In spite of hackings and accidents related to the cryptocurrency, there are limitations of law for the cryptocurrency in that the cryptocurrency's lack of legal status makes dispute resolutions difficult, and that the personal privacy protection within the distributed ledger system of the cryptocurrency cannot be mandated by law.

5. DISCUSSIONS AND CONCLUSIONS

The research performs quantitative analysis of moderating effects of security concerns and risks for management of cryptocurrency systems and proposes solutions for security concerns and risks. The research results show some important implications for the management of cryptocurrency systems. Particularly, (a deep understanding of performance expectancy, social influence, hedonic motivation, security concerns, and risk in cryptocurrency system can be very useful to determine strategies and actions in leading cryptocurrency users to become real traders. Thus,) performance expectancy can be headed for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

management and system design strategies of cryptocurrency service providers, and the cryptocurrency systems should be elaborated in the pleasant and beneficial way. (One of the system design strategies for cryptocurrency should be reputation-building, by gaining a favorable opinion from referents.) This research also illustrates that perceived security concerns and perceived risks might negatively affect cryptocurrency use and trading.

Based on the research results, security concerns and risks have been proved important moderating effects as a great interest for cryptocurrency users. Recently, hacking problems of the cryptocurrency exchange markets have occurred in Japan and Korea, which may cause a sudden market contraction. To prevent the hacking of the markets, relevant and complementary measures should be taken for security concerns and risk. For the safe transactions of cryptocurrency, the paper suggests three solutions for security concerns and risk relevant to the cryptocurrency exchange markets. For the safe transmission of cryptocurrency in the financial industries, the research suggests that Korean Article 49 of the Enforcement Decree of Information and Communication Network Act should require higher standards to the cryptocurrency exchange markets.

The rise of cryptocurrencies and related technology brings to the fore a number of policy questions. Authorities are looking for ways to ensure the integrity of markets and payment systems for financial stability. An important challenge is to combat illicit usage of funds. And a related question is whether central banks should issue their own central bank digital currency [35].

Security violations and monetary damages experienced by the cryptocurrency exchange markets require government regulations. These exchange markets should be regulated similarly to other financial industries which are regulated by the Electronic Financial Supervision and Regulation.

Even though there are hackings and accidents related to the cryptocurrency, there are limitations of law for the cryptocurrency in that the cryptocurrency's lack of legal status makes dispute resolutions difficult, and that the personal privacy protection within the distributed ledger system of the cryptocurrency cannot be mandated by law. As a result, they can be regulated indirectly only.

ACKNOWLEDGEMENTS

This work was supported by Hankuk University of Foreign Studies Research Fund of 2019

REFRENCES:

[1] Andy Greenberg (20 April 2011). "CryptoCurrency". Forbes.com. Archived from the Original on 31 August 2014. Retrieved 8 August 2014.

[2] Cryptocurrencies: A Brief Thematic Review Archived 2017-12-25 at the Wayback Machine… Economics of Networks Journal. Social Science Research Network (SSRN). Date accessed 28 August 2017.

[3] Patrick Schuettel (2017). The Concise Fintech Compendium. Fribourg: School of Management Fribourg/Switzerland. Archived from the original on 2017-10-24.

[4] Bank for International Settlements, *BIS Annual Economic Report 2018*, 17 June 2018, pp. 95-96.

[5] Patrick McDonnell "PK" (9 September 2015). "What Is the Difference Between Bitcoin, Forex, and Gold". NewsBTC. Archived from the Original on 16 September 2015. Retrieved 15 September 2015.

[6] Ian Allison (8 September 2015). "If Banks Want Benefits of Blockchains, They Must Go Permissionless." NewsBTC. Archived from the original on 12 September 2015. Retrieved 15 September 2015.

[7] H. Natarajan, S. Krause and H. Gradstein, "Distributed Ledger Technology (DLT) and Blockchain", World Bank Group, *FinTech Note*, No 1, 2017; BIS.

[8] "Cryptocurrency FAQ - What is Distributed Ledger Technology?", CryptoCurrency Works. Retrieved 21 May 2018.

[9] Matteo D'Agnolo. "All You Need to Know about Bitcoin". timesofindia-economictimes. Archived from the Original on 2015-10-26.

[10] Economist Staff (31 October 2015). "Blockchains: The Great Chain of Being Sure about Things". The Economist. Archived from the Original on 3 July 2016. Retrieved 18 June 2016.

[11] Mamta Badkar (May 14, 2018). "Fed's Bullard: Cryptocurrencies Creating 'Non-uniform' Currency in US". Financial Times. Retrieved May 14, 2018.

[12] R. M. Bratspies, "Cryptocurrencies and the Myth of the Trustless Transactions", March 2018, pp. 6-7. (electronically available via https://ssrn.com/abstract=3141605)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[13] R. Houben and A. Snyers, "Cryptocurrencies and Blockchain", In-depth Analysis Requested by the European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance, *Policy Department for Economic, Scientific and Quality of Life Policies*, July 2018, pp. 12-13. (electronically available via https://www.europarl.europa.eu/swupporting-analyses)

[14] Jerry Brito and Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers" (PDF). Mercatus Center. George Mason University. Archived (PDF) from the original on 21 September 2013. Retrieved 22 October 2013.

[15] "How Cryptocurrencies Could Upend Banks' Monetary Role". Archived 2013-09-27 at the Wayback Machine., American Banker. 26 May 2013.

[16] J. Chiu and T. Koeppl, "The Economics of cryptocurrencies – Bitcoin and Beyond", Bank of Canada working Paper", September 2017. https://ssrn.com/abstract=3048124 or https://dx.doi.org/10.2139/ssrn.3048124

[17] V. Venkatesh, M. Morris, G. Davis, and F. Davis, "User Acceptance of Information Technology: toward a Unified View", *Management Information Science Quarterly*, Vol. 27, No. 3, 2003, pp. 425-478.

[18] Michael D. Williams, Nripendra P. Rana, Yogesh K. Dwivedi, "The unified Theory of Acceptance and Use of Technology (UTAUT): A Literature Review", *Journal of Enterprise Information Management*, Vol. 28, Issue 3, 2015, pp. 443-488. http://doi.org/10.1108/JEIM-09-2914-0088.

[19] Mohammed A. Alshehri, "Using the UTAUT Model to Determine Factors Affecting Acceptance and Use of E-government Services in the Kingdom of Saudi Arabia", *Doctoral Dissertation*, Griffith University, 2012.

[20] Young-Ho Hwang and Yoo-Jin Moon, "Statistical Analysis of Impact Factors Affecting Strategies of the Virtual Reality Service Systems and Intervening Effects of Performance Expectancy", *Journal of Theoretical and Applied Information Technology*, Vol. 49, No. 1, 2018, pp. 7435-7445.

[21] Hyun Shik Yoon and Linsey M. Barker Steege, "Development of a Quantitative Model of the Impact of Customers' Personality and Perceptions on Internet Banking Use", *Computers in Human Behavior*, Vol. 29, 2013, pp. 1133-1141.

[22] C. Kim, M. Mirusmonov, and I. Lee, "An Empirical Examination of Factors Influencing the Intention to Use Mobile Payment", *Computers in Human Behavior*, Vol. 26, No. 3, 2010, pp. 310-312.

[23] W. Newman, *Social Research Methods: Qualitative and Quantitative Approaches* (6th ed.), Boston, MA: Allyn & Bacon, 2006.

[24] C. J. McDaniel & R. Gates, *Marketing Research Essentials* (5th ed.), Hoboken: John Wiley & Sons, Inc., 2006.

[25] P. D. Leedy, *Practical Research: Planning and Design*, New York: Maxwell Macmillan, 1993.

[26] D. E. Gray, *Doing Research in the Real World*, Los Angeles: Sage Publication, 2009.

[27] J. Hair, W. Black, B. Babin, R. Anderson, and R. Tatham, *Multivariate Data Analysis* (6th ed.), Upper Saddle River, NJ: Pearson Education, Inc., 2006.

[28] Young-Ho Hwang and Yoo-Jin Moon, "Analysis of Factors Influencing Intention to Use the Online-only Bank and Interaction Effects among the Factors", *Advanced Science Letters*, Vol. 22, No. 9, 2016, pp. 2588-2591.

[29] P. s. Turocy, "Survey Research in Athletic Training: The Scientific Method of Development and Implementation", *Journal of Athletic Training*, Vol. 37, 4S, 2002, pp. 174-179.

[30] W. W. Chin, R. A. Peterson, and S. P. Brown, "Structural Equation Modeling in Marketing: Some Practical Reminders", *The Journal of Marketing Theory and Practice*, Vol. 16, No. 4, 2008, pp. 287-298.

[31] Joseph F. Hair Jr., G. Tomas, M. Hult, Christian M. Ringle, and Marko Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Los Angeles: Sage, 2017.

[32] Hacking of the Cryptocurrency Exchange Market, "Bithumb", https://m.post.naver.com/viewer/postView.nhn?volumeNo=16094921&memberNo=3939441&vType=VERTICAL, E-Daily News, June 20, 2018.

[33] http://cointalk.co.kr/bbs/board.php?bo_table=coinnews&wr_id=12537

[34] http://www.boannews.com/media/view.asp?idx=70 576

[35] A. Carstens, "Central Banks and Cryptocurrency: Guarding Trust in a Digital Age", *Remarks at Brookings Institution*, Washington D. C., 17 April 2018.