KCI-Indexed Journal
ISSN 2384-0358(Print)
ISSN 2384-0366(Online)

JCCT

The Journal of the Convergence on Culture Technology

Vol.9 No.6 November 2023

■ Culture Convergence (CC)

A Study on English Article Errors in College Students' Writing — Kim, Wooyoung 1
The Effect of Self-Control on Life Satisfaction of Youth Participating in Drone Program — Kim kwang youl, Kim Youn soo 9
A New Generational Spirit?: A Study on Welfare Attitude of Korean Young Generations — Sin-Young Kim 17
Analysis and suggestion of research trends related to NLL-Focused on academic papers from 1998 to 2023- — Hyeon-Sik Kim, Jeong-Hoon Lee 25
Current status and needs for special education to support educational gaps for students with disabilities after COVID-19 — Janghyun Lim, Haein Jeon 33
Effects of an exercise program to strengthen the musculoskeletal system on the body of elderly women — Jung-Ho Lee 41
A Study on the Educational Methods of Convergence Major Based Learning (CMBL) for University Students — Hee-hwa Lee, Hyun-ju Kim 49
Exploring the effects of pre-service teachers' educational service continuity: Focusing on self-efficacy, pro-sociality, and work preference — Shin-hee Park, Sang-woo Jin, Mijung Choi 57
A Study on the Accuracy of Dental Abutments Manufactured by the Dental CAD/CAM Round Bar Milling Method and CNC Milling Machine — JUNG- SOOK KIM 67
The Effects of Gamification E-Learning Classes Based on Self-Determination Theory on University Students' Class Participation, Learning Immersion, Teaching Presence — Myoung-Heo, Sang-woo Jin 73
A Study on Social Network Characteristics, Social Support, Functional Recovery, and Life Satisfaction of People with Mental Illness — Kim, Jin-Mi, Shin, Hyo-Jin 85
Factors Affecting Walking at Night Anxiety among the Elderly — Lee Sungeun 97
Confucius's reflections in the Analects of Confucius - Consideration on overall implications and modern values — Jeum-Nam, Kim 105
A Study on the Jewelry Decorative Pattern based on Wa-Dang in Unified Silla Period — kyeng-Tae Kim 113
Analysis of The Relationships between Religions in Southeast Asia and Tourism Demand in Korea — Kim, Do-Hoon 123
Analysis of Risk Factors for Youth Population Outflow in Busan Based on Machine Learning — Seoyoung Sohn, Hyeseong Yang, Minseo Park 131
A Study on the Knowledge of Health and the Relationship Between Health Beliefs and Preventive Health Behavior of Public Health Center Officials (Central to Covid-19) — NO JI YEONG, KIM EUN JAE 137
Subway Line 2 Congestion Prediction During Rush Hour Based on Machine Learning — Jinyoung Jang, Chaewon Kim, Minseo Park 145
Exploration of the Current Status of the Career Counseling Teacher Training Course and Improvement Plans — Yoon Ok Han 151
The Effect of Major Choice Motivation and Academic Achievement on Career Maturity — Eun-Jo Monn, Ji-Won O, Young Seok Kim, Jung Hee Park 161
Exploring the Direction of Secondary School Career Education in a Lifelong Learning Society — Yoon Ok Han 169
Study on Expression Pattern of Jobs in Game from Perspective of Prospective Jobs in Future — Kwang Hee Cho, Jung Yi Kim 181
A Study on the User Problem Behavior in Overseas Public Libraries — Lee Eun-Ju, Youn You-Ra 187
Quality Characteristics and Antioxidative Activites of Acorn Mook Added Seoritae Powder — Lee Na Gyeom 193
Mediating effect of Self-efficacy and Social Support on the Relationship between SNS Use Time and Acculturation Stress of International Students — DING MEIJUN, Inyong Nam 201
In the Post-COVID-19 Era, Who Swims in Social Media? A Study on Social Media Use and Sociodemographic and Personality Factors — Yesolran Kim 209
Who Dives into Metaverse?: Exploring Sociodemographics and Personality of Metaverse Users — Yesolran Kim, Tae-eun Kim 217
The Serial Multiple Mediation Effect of Smart-media Addiction and ADHD-related Behaviors on the Relation between the Maternal Parenting Behavior and Children's Prosocial Behavior — Sung-eun Baek 229
Study on the feasibility of using AI image generation tools for fashion design development-Focused on the combined use of Midjourney — Park, Keunsoo 237
Designing Digital Twin Concept Model for High-Speed Synchronization — Chae-Young Lim, Chae-Eun Yeo, Ho-jin Sung 245
International Diesel Price Prediction Model based on Machine Learning with Global Economic Indicators — A-Rin Choi, Min Seo Park 251
Sensitivity analysis for the retailer's pricing and lot-sizing policies on the length of credit period — Seong-Whan Shinn 257
Examining the Impact of Short Video Media Characteristics on Organizational Commitment and Mental Health among College Students — Ahn Hyeon Mi, Lee Sin-Bok, Noh Hyeyoung 263
The effectiveness of Ceravida recovery technology on sleeping factors in bedding : Quantitative evaluation — Kim, Jong-Geun, Kim, Ji-Young, Lee, Young-Ik 273
Analysis on Research Trends of Early Childhood Software Education: Korean Articles Published in 2017 Through 2022 — Min Kyoung Lee, Sang Lim Kim 281
The Effect of Pre-Service Early Childhood Teachers' Motivation for Choosing Teaching on Career Adaptability: The Mediating Effect of Self-Directed Learning — Se Jin Eom*, Seung Hwa Jwa 291
Dust Prediction System based on Incremental Deep Learning — Sung-Bong Jang 301
Analysis on the English Translation of The First Chosen Educational Ordinance, Manual of Education of Koreans (1913), and Manual of Education in Chosen 1920 (1920) Using Text Mining Analytics — Jinyoung Tak, Eunjoo Kwak, Silo Chin, Minjoo Shon, Dongmie Kim 309
Impact Range Analysis of Small LPG Storage Tank Explosions at Highway Rest Areas — Seung duk Jeon, Soon Beom Lee, Jai Young Lee 319
The influence of Ego-Resilience on Self-Leadership in Nursing Students: Mediating Effect of Critical Thinking Disposition — Hye-Suk Kim, Mi-Hwa Park, Eun-Young Choi 329
The Age of Technology Addiction : Instagram Addiction from the Perspective of Design — Changhee Han 339
The influence of Nursing Students' Attitudes Toward the Use of Corporal Punishment on Children and Recognition of Children's Right on the Intention to Report Child Abuse — Lee Joo Yeon 347
Relationship between knowledge about the elderly, burn out, job satisfaction, and awareness of elder abuse of Healthcare Workers — Bae Hye-jin, Hong Sun-yeun 355
Impact Analysis of Abolition of Royalty on Non-fungible Tokens Market — Eun Mi Lee 365
Cross-border Search and Dynamic Capability on Business Model Innovation of SMEs in China — Zhou Ru, Ma Weiwei, Kim DongJoo 371
A Study on the Influence of Social Support on Chinese College Students' Entrepreneurial Intention : Based on the Mediating Role of Career Adaptability - — Yu Lunlun, Gao Jing, Wang Shuyang 388
Use of Menstrual Sanitary Products in Community Women of Childbearing Age — Hyunju Dan, Heeja Jung 401
Effect of Covert Narcissism, Self-directed learning Ability, Academic Achievement on Self-leadership of Nursing students — Kyoung Eun Lee, Eun Kyung Byun 409
The Mediating Effect of Emotional Intelligence on the Relationship between Multicultural Perception and Multicultural Efficacy of Nursing University Students — Eun-Ha Na, Mi-Jung Kim 419
Design of kitchen cabinet using complex link mechanism — Kibum Shim, Hoon Shim, Geon-Hyeok Lim, Jiwon Jang, Sang-Hyun Kim 429
The Effects of Depression, Self-efficacy, and Life Stress on the Smartphone Addiction of Nursing College Students — Eun-Hee Kang, Hyo-Jin Park, Mi-Young Kim 435
The Higher Education Possibility of Sound Art in Korea – Focusing on the Proposal of Creative Fusion Liberal Arts Learning — Irene Eunyoung Lee 443
A Case Study of Public Contents in Out-Of-Home Advertising: Focused on Visual Characteristics — Kim, Woon-Han, Jeong, Hyeon-Ju 453
Effects of Health Perceptions and Social Support on Health Promotion Behaviors among College Students: the Mediating Effect of Self-efficacy — Su Jeong Park, A Reum Lee, Byoung-Gil Yoon, Jung Hee Park 461
The mediating effect of subjective happiness in the relationship between parental abuse and neglect and Internet addiction in adolescents — Choi Jihyun, Jeong Misook 471
Differences in Conflict Management Style according to MBTI Indicators of Nursing Students — Su Jeong Shin 479
Factors Influencing Aging Anxiety in Middle-aged Women — Minjoo Hong, Yeong-Nam, Yeo 487
Perception survey analysis for legal support in case of legal disputes among firefighters — Young-Jin, Reem, Ha-Sung Kong 495
The Effects of Learning Strategies on Academic Achievement in College Students :Focusing on the Mediating Effect of Grit — Tae Hee Jang, Ju Hyeon Hwang, Jung Hee Park Woo Sok Han 509
Survey-based unstructured data analysis to predict flipped learning performance — Chayoung Kim, Yoon Kim 519
A Study on the evaluation technique rubric suitable for the characteristics of digital design subject — Cho, Hyun Kyung 525
A Study on the development of Creative Problem Solving Classes for University Students — Hyun-Ju Kim, Jinyoung Lee 531
Analysis of Video Advertisement Production Direction based on Generation Z Lifestyle and SNS Status — Cho, Hyun Kyung 539
A study on Materialization of Virtual Reality for Environmental Interface — Kang, Yoon Jeong 545
Imaginative Implication of John Burningham Picturebooks 『Come Away from The Water, Shirley』and 『Time to Get Out of The Bath, Shirley』: An Interpretation using Bakhtin's Conception of Carnival — Yoo Jung Jung 551
The Effectiveness of Environmental Management through Environmental Surveillance — Mi Hyang Lee, Jae Yeun Kim, Sang Ha Kim 557
The influence of calling and self esteem on nursing professionals of nursing students — Hyea-Kyung Lee, Yun-Soo Choi, Ji-Seon Kim, Myeong-Seo Kim, Chan-Young Jeon, Chae-Yoon Cho, Yeon-Jin Heo 563
Lifestyle habits, Self-growth, and Happiness of Nursing University Students — Kim Jin, Cha Nam Hyun 573
Elementary School Children's Trajectories of Self-Esteemin Grades 1 through 4 — Seul Gi Ko, Sang Lim Kim 581
A Study on the Independent Possibility of K-POP Dance through Various Cases — Chan-Yang Kim, Chang, So-Jung 589
The Mediating Effect of Resilience on the Relationship between Clinic Practice Stress and Psychosocial Well-being of Nursing University Students — Mi-Jung Kim, Eun-Ha Na 595
A Comparison study of Nursing process competency, Critical thinking disposition and SBAR technique knowledge between Clinical practice and Alternative clinical practicum — Oe-Seon Lee, Jung-Hye Lim 605
The effect of Positive psychology program using Complementary and Alternative Therapies on Negative emotions, Career decision making Self-Efficacy, Self-Compassion, and Flourish of Nursing students — Hyangjin Park, Hyun-Jung Jang 615
Effectiveness of Developing and Applying Problem Based Learning: Self-Directed Learning Ability, Critical Thinking, Communicative Ability, and Problem Solving Skills of Nursing Students — Park, Hyun Joo, Byun, Shang Hee 627

CROSSREF.ORG THE CITATION LINKING BACKBONE MEMBER

IPACT
문화기술의 융합
(사)국제문화기술진흥원
The International Promotion Agency of Culture Technology

JCCT
문화기술의 융합
제9권 제6호 2023.11
IPACT
사단법인 국제문화기술진흥원

Vol.9 No.6 November 2023

The Journal of the Convergence on Culture Technology

Nursing Students' Experience of Interpersonal Caring in an Enneagram-based Care Intervention Program — Shin Eun Sun 637
Confidence and Major Satisfaction in Performing Core Basic Nursing Skills of Nursing Students Who Have Experienced Clinical Practice — Kwon Yu jin, Jang Jae yeon, Gu Do gyeong, Lee Sang eun, Lee Hyun ji, Lim Eun jeong, Cha Nam Hyun 647
The Mediating Effect of Self-efficacy in the Relationship between Sense of Calling and Service Quality of Personal Assistants for People with Disabilities — So Yoon Lee , Young Chae Kwon 657
The effect of Job stress on Burnout of Wee Counseling Specialists : Focusing on Mediating effect of Competency and Emotional intelligence — Jung-Hye Lim, Mi-Jung Kim 667
Children's Trajectories of Elementary School Adjustmentin Grades 1 through 4 — En Ha Her, Sang Lim Kim 677
The Effects of Shared Leadership, Organizational Communication, and Nursing Service Quality Perceived by Nurses on Patient Safety Management Activities — Ji In Nam, Nam Joo Je, Gyeong Hye Kang, Kyeong Hwa Cho, Sung Ju Lee, Min Yeong Kim, Min Jung Lee 685
A study on the development of early childhood artificial intelligence education program — Kim Hee Young 695
Theory of planned behavior and use of Virtual Personal Assistant(VPA) — Eunji Lee 703
A Study on Spatial Therapy through Spatial Psychology — Hae Rang Park 709
A Study on ESG Factors on Corporate Image and Corporate Reputation from a Consumer Perspective — Park Jinwoo 715
Achievement Experience of Nursing Students Through Simulation Practicum — KUEMJU PARK 721
Work-Life Balance Policies in Germany and the Participation of Private Companies — Nam, Hyun-Joo 729
Flâneur in Balzac and Baudelaire — Hyub Lee 737
The Exploration of the Factors Affecting Burnout among Young Working Adults — Minkee Hong, Hyeonsu Byeon 743
The Effect of Social Participation of the Elderly on Human Rights Awareness: The Mediating Effect of Self-Esteem — PARK JU JONG, PARK SUN JU, KIM IN 751
A Study on the Reliability and Validity of the Korean Version of COVID-19 Stress Scale for Nursing Students — Jin-Ju Woo, Hye-Seon Choi 763
A Study of Strategies in Drama Using Literature-Centering on the drama <I will visit you if the weather is nice>(2020) — Son, Mi-young 771
Analyzing the Defense Budgetary in the Republic of Korea with the Punctuated Equilibrium Theory — Yongjoon Park 779
Optimized Evaluation of Counter Drone System for Defending National Major Facilities through a Thinking Process of RMA — Sang-Keun Cho, Ki-Won Kim, In-keun Son, Cook Rhie, Hyun-Ho Choi, Kang-Il Seo, Sang-Hyuk Park 789
A Case Study on the Use of Female Human Resources in the Canadian Military and Its Implications — In-Chan Kim, Jong-Hoon Kim, Jun-Hak Sim, Kang-Hee Lee, Myung-Sook Hong, Sang-Hyuk Park 795
A study on improvement of soldier mental health care using wearable devices — In-Chan Kim, Sang-Keun Cho, Jun-Hak Sim, Jong-Hoon Kim, Sang-Hyuk Park 801
A Study on the effectness of military training with Airsoft gun — Chang-In Lee, Dong-Seok Kim, Min-Gyu Kang, Sang-Hyuk
A Concet Analysis of Psychiatric Nurse's Compassionate Communication Competence: Hybrid Model — Won Hee Jun, Hye Suk Im 813
Factors affecting social capital awareness of social economy — Kuk-Gwen Lee, Seon-Gyeong Park 827
Case Study of Intellectual Property Rights of Pre-service Teachers through Convergence Capstone Design Class — Ko, Eun Mi, Park, Young Sin 833
A Study on the Indicators of Language Development Ability in Infants 18-24 Months — Kyung-sook Hwang, Wha-Soo Kim, Ji-Woo Lee 843

■ Technology Convergence (TC)

A Study on the Improvment of Safety and Health Education for Korea Post Workers — Hyungoo Lee, Taekeun Oh 849
Synthesis of CuO nanoparticles by liquid phase precursor process — Seong-Whan Shinn 855
Research and improvement of image analysis and bar code and QR recognition technology for the development of visually impaired applications — MinSeok Cho, MinKi Yoon, MinSu Seo, YoungHoon Hwang, Hyun Woo, WonWhoi Huh 861
Simultaneous Analysis of Cold Medicine Component by High-Performance Liquid Chromatography(HPLC) — Wonju Lee, Seung-Tae Choi, Keun-Sik Shin, Jin-Young Park, Jae-Ho Sim 867
Virtual PID Algorithm Tuning Technique and Data Analysis through Computer Simulation — Jin Moon Nam 875
Artificial Neural Network-based Thermal Environment Prediction Model for Energy Saving of Data Center Cooling Systems — Chae-Young Lim, Chae-Eun Yeo, Seong-Yool Ahn, Sang-Hyun Lee 883
The Effect of Cooperative Learning on Self-directed Learning Ability — KIM KYUNG HEE, CHOI JOO YOUNG 889
Latent Profile Analysis of Senior Lifestyle Profile: A stringent study of similarity and differences — Seo In-seog, Kim Young-mi, Oh Hyun-sung 899
Evaluation of Edge-Based Data Collection System for Key-Value Store Utilizing Time-Series Data Optimization Techniques — Woojin Cho, Hyung-ah Lee, Jae-hoi Gu 911
Study of speed Profile for Dynamic Stability of EOTS — Gyu-Chan Lee, Dong-Gi Kwag 919
A Study on the Rubber Damping Characteristics of Vibration Reduction Mounts for UAVs — Chan-Hwi Kang, Hun-Suh Park, Dong-Gi Kwag 927
A Study on Unstructured text data Post-processing Methodology using Stopword Thesaurus — Won-Jo Lee 935
A Study of the Longitudinal Stability of eVTOL UAM with Tilt Rotor and Tandem Wing — Joo Chan-Young, Kim Ha-Min, Kim in-Jae, Min Kyoung-Soon 941
Application of Fischer's Policy Evaluation Methodology to Employment and Jobs Policy for people with disabilities : Contextual Feasibility Evaluation — Sol Jung, Dongug Kang, Yun Seon Jang 947
Real-time Adaptive PID Temperature Control that limits Overshoot — Jin Moon Nam 957
Comparative analysis of the digital circuit designing ability of ChatGPT — Kihun Nam 967
The Effects on Micro-learning Contents on University Students' Learning Flow and Learning Motivation based on Extracurricular Program — Gwak Chan Mi, Dong Yub Lee 973
A Study on the Relationship between Organizational Culture and Organizational Citizenship Behavior Perceived by Naval Personnel: Mediating Effect of Affective Commitment and Moderating Effect of Coworker Social Loafing — Hong Jeong Lee 981
Optimization of mixing ratio of Polygala tenuifolia, Angelica dahurica and Elsholtzia splendens extracts for cosmetic material development — Jung Seo A, Song Ga Hyeon, Su In Park, Jung Youn Ok 993
Development of a Factory Energy Monitoring System based on Food Factory Collected Data — Chae-Eun Yeo, Woo-jin Cho, Jae-Hoi Gu 1001
Comparison of Antioxidant Activity and Flavor Effect According to Processing Method of Red ginseng and Herbal Medicine — Hyun Kyoung Kim, Ho Tae Kim, Pil Jae Lee 1007
Smart Contract Security Audit Trends and Services — Chansol Park, Janghwan Kim, R. Young Chul Kim 1017
The Impact of Global Content Experiences through OTT on Global Orientation and Global Brand Attitude — Kisuk Hong, ByoungJo Kim 1031
Is meaning-oriented consumption possible in the consumer society? : The case study of women's narratives on cosmetic experiences — Bong Hyun Kim 1039
Experimental Verification of the Characteristic Analysis of the Aricultural Drone using Smart Operating Mode — Wooram Lee 1049
Estimation Method of Resilience Pads Spring Stiffness for — Jung-Youl Choi, Sang-Wook Park, Jee-Seung Chung 1057
Using multi-sensor for Development of Multiple Occupants' Activities Classification Model Based on LSTM — Jin Su Park, Chul Seung Yang 1065
ADVERTISING EFFECTS OF VIRTUAL INFLUENCER -The Effect of Social Exclusion and Parasocial Relationship- — Wang, Wei Yan, Ahn, Hongmin 1073
Study on Development of Basic Fire Evacuation Scenarios considering Characteristics of Special Schools — Sammy Park, Sanghyun Ryu, Changhee Cho, Serim Kang, Yunseo Jeong, Younggeun Yoon 1081
Exploration of factors that improve the realism of virtual windows for the implementation of virtual environments — Kim, Jong Kouk 1089
Lighting Intensity, Leaf Temperature, Transpiration Rate, and Vapor Pressure Deficit between the Top and Branching Point of Stem during Growing Period of Paprika Plant — Seung Mi Woo, Ho Cheol Kim 1097
How Can the Metadata and File Structure of Audio Files Be Manipulated? — Sungwon Baek, Homin Son, Jae Wan Park 1103
Digital News Innovation and Online Readership: A Study of Paying Subscribers for Online News — Sun Ho Jeong 1111
A Study on Social Value Creation in Social Enterprise by Sector- Focusing on Social Enterpreise in Incheon — Yong-Gu kim, Jae Ho Kim 1119
Nursing Sudents' Experiences of Online Psychiatric Nursing Practice in COVID-19 : A Parse Research Method Study — Gyun-Young Kang, Jinju Kim 1127
Influence of Grit and Self-elasticity on Carrer Identity of Nursing Students — Yun Mi Jin, Jin Hye Kyung 1135
The Effects of Case-Based Learning (CBL) on Problem Solving Ability and Academic Self-efficacy in Nursing Students — Jin Hye Kyung, Yun Mi Jin 1143
A study on the analysis of the Chinese metaverse status — In-Suk Jung 1151
A Study on the Effect of Job Stress, Self-leadership and Social Supports of Long-Term Care Hospital Nurses on Nursing Performance — Park So-Young, Cho Jeong-Lim 1159
Design and Implementation of a Project Work Unit-based Scheduling Application — Bomin Kim, Minyoung Kim 1173

http://www.ipact.kr
Rm.612 Dongbu Sunville, #99-6, Garak-Dong, Songpa-Gu, Seoul, 138-169, Korea
TEL: +82-2-409-7718, FAX: +82-2-407-7716

The Journal of the Convergence on Culture Technology (JCCT)
Vol. 9, No. 6, pp.1017-1029, Noember 30, 2023. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2023.9.6.1017

JCCT 2023-11-122

스마트 계약 보안 감사 동향 및 서비스

Smart Contract Security Audit Trends and Services

박찬솔, 김장환, 김영철

Chansol Park, Janghwan Kim, R. Young Chul Kim

요 약 블록체인을 통해 많은 양의 거래가 일어나고 있다. 그중에서도 스마트 계약을 통한 거래의 비중이 커지고 있다. 이에 따라 스마트 계약에 대한 취약점 공격과 스마트 계약을 이용한 사기와 같은 문제점들도 증가한다. 스마트 계약에 대한 보안 감사를 통해 개발자는 취약점을 발견해 해결할 수 있고, 이용자는 스마트 계약의 사기 여부를 구분할 수 있다. 하지만 현재 스마트 계약에 대한 보안 감사에 대한 규정과 표준이 없으므로 보안 감사를 수행하는 서비스들이 불균일하다. 본 논문에서는 스마트 계약에 대한 보안 감사 동향을 분석하고 어떠한 서비스들이 제공되고 있는지 파악한다. 보안 감사 보고서를 중심으로 스마트 계약으로부터 어떠한 요소들을 분석하는지 조사한다. 또한 어떠한 취약점들을 검출할 수 있는지 조사한다. 마지막으로 스마트 계약에 대한 품질 지표와 설계 추출의 가시화 요소를 조사한다. 이를 통해 스마트 계약에 특화된 가시화 요소를 찾을 수 있을 것을 기대한다.

주요어 : 소프트웨어 가시화, 블록체인, 스마트 계약, 보안 감사, 복잡도

Abstract A large amount of transactions are taking place through Blockchain. Among them, the proportion of transactions through smart contracts is increasing. Accordingly, problems such as vulnerability attacks on smart contracts and fraud using smart contracts are increasing. Through security audits of smart contracts, developers can discover and resolve vulnerabilities, and users can distinguish whether smart contracts are fraudulent. However, there are currently no regulations and standards for security auditing of smart contracts, so services that perform security auditing are uneven. In this paper, we analyze security audit trends for smart contracts and identify what services are being provided. We investigate what elements are analyzed from smart contracts, focusing on security audit reports. Also, investigate what vulnerabilities can be detected. Finally, we investigate quality indicators for smart contracts and visualization elements of design extraction. Through this, we hope to be able to find visualization elements specialized for smart contracts.

Key words : Software Visualization, Blockchain, Smart contracts, Security audit, Complexity

Ⅰ. 서 론

코로나19 팬데믹 기간 암호 화폐 시장에 대한 투자와 관심이 증가했다[1]. 암호 화폐에 기반이 되는 기술인 블록체인에 관한 관심도 증가하여, 스마트 계약을 토대로 한 토큰 및 대체 불가능 토큰(NFT)에 대한 상당량의 투자가 진행되었다[2]. 2023년 하루 평균 약 8,000억 달러 이상의 암호 화폐가 거래되고 있다[3]. 또한 2022년 전 세계 스마트 계약의 시장 규모는 약 17억 달러 이상이었으며, 2030년까지 시장의 규모가 연평균 24퍼센트로 성장할 것으로 예측된다[4].

스마트 계약의 시장 규모가 커짐에 따라 스마트 계

*준회원, 홍익대학교 소프트웨어융합학과 석사과정 (제1저자)
**정회원, 홍익대학교 소프트웨어융합학과학과 박사과정 (참여저자)
***정회원, 홍익학교 소프트웨어융합학과학과 교수 (교신저자)
접수일: 2023년 10월 3일, 수정완료일: 2023년 10월 25일
게재확정일: 2023년 11월 10일

Received: October 3, 2023 / Revised: October 25, 2023
Accepted: November 10, 2023
***Corresponding Author: bob@hongik.ac.kr
Dept. of Software and Commuinications Engineering, Hongik Univ, Korea

약에 대한 취약점 공격과 스마트 계약을 이용한 사기 또한 증가하고 있다[5]. 이러한 문제들은 스마트 계약의 참여자에게 큰 손실을 초래하며, 스마트 계약에 대한 신뢰성을 크게 훼손한다. 스마트 계약의 개발자는 스마트 계약에 대한 신뢰성과 안전성을 보장하기 위한 방법으로 스마트 계약에 대한 보안 감사를 받고, 보안 감사 보고서를 스마트 계약 참여자들에게 공유한다. 이때 보안 감사 보고서에 대한 표준과 규정이 없으므로 보안 감사 업체마다 보고서의 양식과 들어가는 내용이 다르다. 또한, 보고서의 내용이 대부분 줄 글로 이루어져 있어, 블록체인 및 스마트 계약 코드에 대한 지식이 없는 일반 스마트 계약의 이용자가 이해하기 어려울 수 있다.

본 논문에서는 Ethereum 플랫폼의 Solidity로 작성된 스마트 계약에 대한 보안 감사 서비스를 중심으로 보안 감사의 동향을 파악한다. 보안 감사 서비스에서의 스마트 계약과 스마트 계약에 포함된 취약점의 분석 내용 및 기법을 분석한다. 또한, 스마트 계약에 대한 가시화 기법을 분석한다. 또한 기존 스마트 계약에 대한 가시화 기법을 비교한다.

본 논문의 구조는 다음과 같다. 우선 2장에서는 관련 연구로서 블록체인, 스마트 계약 그리고 스마트 계약에 대한 보안 감사를 설명한다. 3장에서는 기존 스마트 계약에 대한 보안 감사 서비스, 보안 감사 시 수행하는 스마트 계약 분석 그리고 스마트 계약으로부터 찾은 취약점을 어떻게 다루는지 분석한다. 4장에서는 스마트 계약에 대한 가시화로서 스마트 계약에 대한 품질 지표와 가시화 방법을 분석하고 기존 스마트 계약 가시화 연구와 비교한다. 마지막으로 5장에서는 결론과 향후 연구에 대해 언급한다.

II. 관련 연구

2.1. 블록체인

블록체인은 다수의 컴퓨터가 합의 알고리즘을 통해 분산된 원장을 관리하는 탈중앙화 기술이다[6]. 이를 통해 거래 기록 등과 같은 중요한 정보를 별도의 중앙 기관 없이도 위조 및 변조를 방지할 수 있다. Bitcoin은 블록체인을 통해 암호 화폐를 구현하고, 이를 통해 최초로 거래한 대표적인 1세대 블록체인이다[7]. Bitcoin은 암호 화폐의 거래를 기록하기 위한 수단으로 블록체인을 이용한다. Bitcoin 송금 요청 시 송금 정보가 담긴 트랜잭션이 발생하고, 새로 생성될 블록에 포함된다. 네트워크 구성원들은 새로 생성될 블록의 유효성을 검증하고 승인한다. 구성원들로부터 승인된 블록은 기존 블록체인에 연결되어 블록에 포함된 트랜잭션들이 커밋되며, 동시에 송금도 완료된다. Bitcoin의 잔고는 특정 자료 구조에 저장되지 않고 블록체인에 기록된 송금 기록의 합인 미사용 트랜잭션 출력(Unspent Transaction Output) 데이터로 대체된다.

Ethereum은 가장 처음 스마트 계약을 구현한 블록체인 플랫폼으로서 자동화된 거래가 가능하게 한 대표적인 2세대 블록체인이다[8]. Ethereum은 블록체인을 통한 스마트 계약을 구현하기 위해 거래 기록을 저장하는 블록체인과는 별도로 현재의 상태를 저장하는 World state를 추가했다.

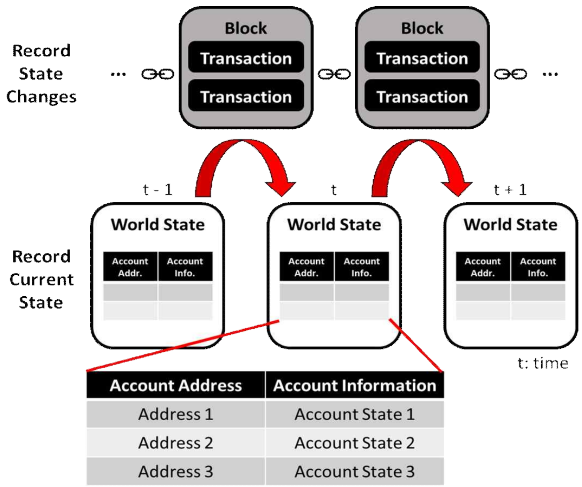

그림 1. World State와 블록체인의 관계[9]
Figure 1. Relationship between World State and Blockchain[9]

그림 1은 표로 그려낸 World state와 블록체인과의 관계를 나타낸 것이다. World state는 Ethereum 계정의 주소와 계정의 정보 쌍들이 저장된다.

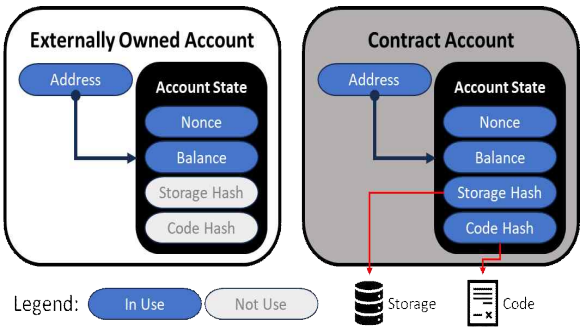

그림 2. 이더리움 계정 유형[9]
Figure 2. Type of Ethereum Account[9]

그림 2는 Ethereum 계정의 종류에 따라 저장되는 정보를 나타낸 것이다. Externally Owned Account(EOA)는 Ethereum 참여자에게 할당되는 계정 종류이다. 참여자가 직접 명령어를 전송하거나 지갑을 이용하여 EOA를 조작할 수 있다. Contract Account(CA)는 Ethereum에 배포된 스마트 계약에 할당되는 계정 종류이다. CA는 스마트 계약에 작성된 명령에 따라 자동으로 동작한다.

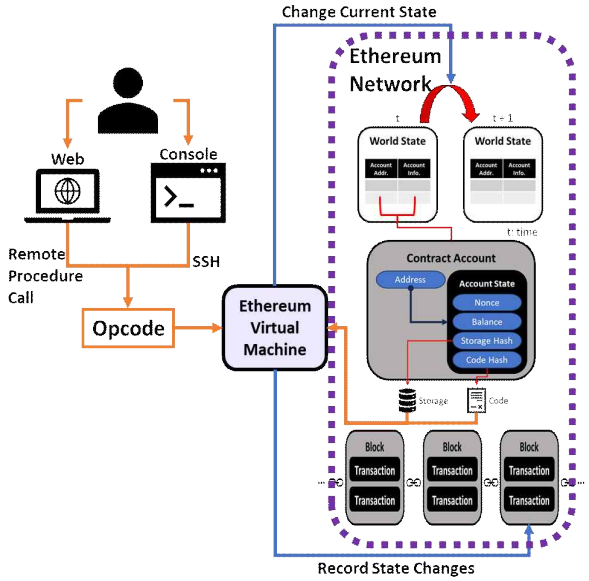

그림 3. EVM을 통한 사용자와 이더리움의 상호작용[9]
Figure 3. Interaction between User and Ethereum through EVM[9]

그림 3은 Ethereum 가상 머신(EVM)을 중심으로 Ethereum과 유저 간 상호 작용을 도식화 한 것이다. EVM은 Ethereum의 각 노드를 구성하는 가상 머신으로써 단순 트랜잭션 처리 뿐만 아니라, Opcode를 통해 Ethereum의 상태 변화를 처리할 수 있다[10]. 이를 통해 Ethereum은 분산된 노드들을 통해 멈추지 않고 가동되는 하나의 유한 상태 기계로써 동작한다. 이때 Ethreum의 상태는 World state에 저장되고, EVM에 의한 상태 변화들은 블록체인에 기록된다.

2.2. 스마트 계약

스마트 계약은 블록체인 네트워크에서 수행될 수 있는 자동화 스크립트이다[11]. 스마트 계약에는 계약 당사자들이 사전에 합의된 내용이 프로그래밍 되어 있다. 배포된 스마트 계약은 계약 조건의 충족 여부를 검증하여 송금, 토큰 발행 등과 같은 계약 내용을 자동으로 수행한다[12]. Ethereum에서 스마트 계약을 작성할 수 있는 언어는 고수준 언어인 Solidity, Vyper 그리고 저수준 언어인 Yul, Huff가 있다. 그중에서도 가장 먼저 발표된 Solidity의 점유율이 압도적으로 높다[13]. Ethereum의 4가지 스마트 계약 언어는 모두 EVM에서 실행할 수 있는 Opcode로 컴파일되어 World state에 배포된다. 이러한 스마트 계약은 탈중앙화 애플리케이션에서 중추적인 역할을 한다.

탈중앙화 애플리케이션은 블록체인 네트워크를 통해 동작하는 애플리케이션이다. 탈중앙화 애플리케이션은 중앙 집중식 서버에서 실행되는 기존 애플리케이션과 달리 투명성, 보안 및 분산 제어를 보장한다[14]. 탈중앙화 애플리케이션에는 게임, 탈중앙화 금융, NFT 거래 등의 종류가 있다[15].

2.3. 스마트 계약 보안 감사

스마트 계약에 대한 보안 감사는 스마트 계약을 분석하고, 취약점을 찾아, 이를 보고하는 일련의 과정이다[16]. 스마트 계약에는 다른 프로그램과 같이 개발자가 의도하지 않았더라도 취약점이 포함될 수 있다. 대표적으로 Smart Contract Weakness Classification (SWC)의 37개의 항목이 있다[17]. 스마트 계약이 주로 암호화폐, 토큰, NFT 등과 같은 가상의 재화를 다루는 만큼, 이러한 취약점은 큰 피해를 초래할 수 있다. 보안 감사를 통해 개발자는 스마트 계약에 포함된 취약점을 찾아 해결하여 취약점 공격을 방지할 수 있다. 또한 스마트 계약에 대한 보안 감사 보고서를 통해 스마트 계약을 통한 사기를 미리 발견할 수 있다.

III. 기존 스마트 계약에 대한 보안 감사 동향 및 서비스

3.1. 스마트 계약에 대한 보안 감사 서비스

몇몇 보안 업체에서 스마트 계약에 대해 보안 감사를 수행하고 보고서를 제공한다[18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29]. 그중 실적과 보고서를 공개한 감사 업체들에 대해 분석했다. 표 1은 스마트 계약에 대한 보안 감사 서비스를 제공하는 업체의 정보이다. 보안 업체마다 발표하는 실적의 내용이 다르다. 따라서 발표한 스마트 계약의 보안 감사 보고서의 개수, 보안

감사 완료한 스마트 계약의 개수, 보안 감사 과정에서 검출한 취약점의 개수, 보호한 기업의 개수 그리고 보안 감사 완료한 스마트 계약의 시가 총액 중 하나의 실적이라도 공개하고, 보안 감사 보고서를 공개한 보안 업체에 한해 동향 분석했다.

표 1. 스마트 계약 서비스 공급업체의 공개 기록
Table 1. Open Record of Smart Contract Service Vendors

Name of Smart Contract Audit Vendors	Total Audit Reports	Reviewed Smart Contracts	Detected Vulnerabilities	Protected Businesses	Market Cap° of the Reviewed Smart Contract
SourceHat[17]	1,700+	8,000+	2,000+	.	$50B+
Consensys-Diligence[18]	.	.	200+	100+	.
Certik[19]	4,400+	.	60,000+	4,000+	$364B+
Hacken[20]	1,200+	.	.	1,000+	.
Quilaudits[21]	850+	800K+ (LOC)	.	.	$30B+
Cyberscope[22]	1,200+	.	.	.	$1B+
Slowmist[23]	1,500+	.	.	.	.
Quantstamp[24]	.	.	.	500+	$200B+
OpenZeppelin[25]	350+	.	.	.	.
PeckShield[26]	450+	.	.	.	.
SolidProof[27]	850+	1,000+	.	350+	.
Chainsulting[28]	.	9M+ (LOC)	.	420+	.

그림 4는 일반적으로 스마트 계약에 대해 보안 감사를 수행하는 과정의 순서도이다.

a) 스마트 계약 코드 수집: 보안 감사를 위해 고객이 감사 업체에 스마트 계약 코드를 제공한다. 스마트 계약 코드를 공유하는 가장 보편적인 방법은 스마트 계약이 저장된 Github 저장소와 감사를 받을 버전 정보를 함께 제공하는 것이다. 코드가 Github 저장소에 업로드되지 않은 경우 보안 감사를 위해 직접 파일을 제공할 수도 있다.

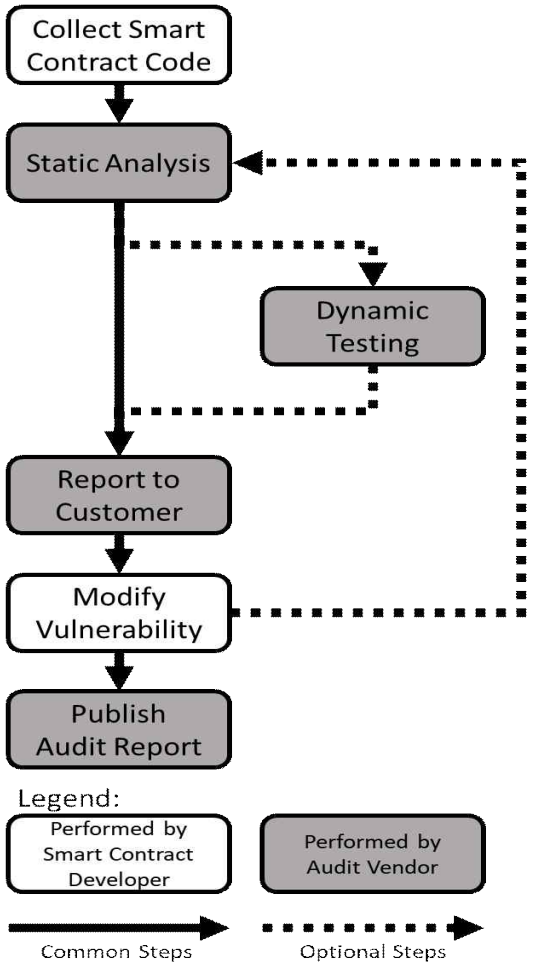

그림 4. 일반적인 스마트 계약 보안 감사 프로세스
Figure 4. Common Smart Contract Security Audit Process

b) 스마트 계약 정적 분석: 정적 분석 단계에서는 코드를 정적으로 분석하고, 이를 검토한다. 이 과정에서는 주로 도구를 통해 스마트 계약을 분석한다. 이후 도구를 통해 분석한 결과를 검토하여 계약에 대한 분석 및 취약점을 찾아낸다.

c) 스마트 계약 동적 분석: 일부 보안 감사 서비스에는 동적 분석 단계가 포함된다. 동적 분석 단계를 통해 취약점과 관련된 몇가지 시나리오를 시험 할 수 있다. 또한 각 계약과 계약에 포함된 기능들의 가스 소비량 등을 측정할 수 있다.

d) 보안 감사 결과 보고 및 취약점 수정: 스마트 계약에 대한 분석이 완료되면, 분석 결과를 고객에게 보고한다. 고객은 분석 결과를 토대로 스마트 계약을 수정한다. 두 번째부터 네 번째 단계는 심각한 취약점이 모두 수정될 때까지 반복될 수 있다.

표 2. 스마트 계약 감사 보고서에 포함된 스마트 계약 분석 결과
Table 2. Smart Contract Analysis Results Included in Smart Contract Audit Reports

		SourceHat	Consensys -Diligence	Certik	Hacken	Quilaudits	Cyberscope	Slowmist	Quantstamp	OpenZeppelin	PeckShield	SolidProof	Chainsulting
Smart Contract Overview	Contract Scenario	O	O	O	O		O	O	O	O	O	O	O
	Analysis of individual (important) scripts	O	O	O	O	O				O		O	O
	(Token) Contract Economy	O	O	△	O	O	O		O	O			△
	Priorities for Audit		O	O								O	O
	Project Score			△	O							O	
Actor Analysis	Type of Actor		O	O	O		O			O			
	Authorized Functions			O		O	O			O		O	
Functional Analysis	Description					O	O					O	O
	Modifier	O					O	O				O	O
	Restrict(Visibility, Mutability)	O					O	O				O	O
	Gas Consumption								O				

△: Available from external services rather than smart contract reports

e) 스마트 계약 보안 감사 결과 보고서 공개: 모든 감사 과정이 완료되면 감사 업체는 스마트 계약에 대해 보고서를 작성하고 이를 공개한다.

3.2. 스마트 계약에 대한 분석

스마트 계약에 대한 보안 감사 과정에는 스마트 계약에 대한 전반적인 분석이 포함된다. 보안 감사 보고서에는 이 과정에서의 분석 결과를 요약하여 기재한다. 표 2는 각 보안 감사 서비스에서 분석 후 결과 보고서에 포함한 스마트 계약 분석 결과를 요약한 것이다.

a) 스마트 계약 개요: 스마트 계약 및 해당 스마트 계약을 포함하는 탈중앙화 애플리케이션에 대한 분석 정보이다. 대부분의 감사 보고서에는 계약의 주요 시나리오를 간략한 설명과 함께 서술했다. 또한 여러 스크립트로 구성된 스마트 계약의 경우에는 개별 스크립트에 대한 심층적인 분석 후 나눠서 기재하는 경우도 있다. 스마트 계약 중 Ethereum Request Comments(ERC)-20 표준에 따라 대체 가능 토큰을 배포하는 계약의 경우에는 해당 토큰의 경제 시스템에 대해서도 보고서에서 설명한다. 정적 분석을 통해 토큰 경제 시스템의 수식 등을 유도한 후 이를 서술한다. 일부 감사 업체는 보고서가 아닌 동적 분석 서비스를 통해 토큰의 현황을 실시간으로 나타낸다. 보안 감사 과정의 체계를 중시하는 감사 업체의 경우 고객과 인터뷰 후 설정한 보안 감사의 우선순위를 추가로 기재했다. 소수의 감사 서비스에서만 계약 분석 결과를 수치화하여 기재했다.

b) 액터에 대한 분석: 스마트 계약에서 찾을 수 있는 액터에 대한 분석 정보이다. 관리자, 이용자 등과 같은 액터의 종류와 액터가 하는 일을 분석하여 정리한다. 또한 함수에 대한 분석을 통해 각 액터 별로 권한을 가지고 있는 함수를 정리한 경우도 있다. 액터에 대한 분석은 액터를 잘못 설정하여 발생할 수 있는 취약점을 막을 수 있다. 또한 액터를 교묘히 설정하여 사기에 이용하려는 스마트 계약도 찾아낼 수 있다.

c) 각 함수에 대한 분석: 스마트 계약의 각 함수에 대해 분석하여 기재한다. 많은 보안 감사 서비스에서는 함수 분석 결과를 보고서에 포함하지 않거나, 포함하더라도 도구를 통한 분석 결과를 그대로 포함하는 경우가 있었다. 단 하나의 감사 서비스에서만 함수별 가스 소비량을 보고서에 포함했다.

표 3. 스마트 계약 감사 서비스의 취약점 범위

Table 3. Vulnerability Coverage of Smart Contract Audit Services

	SourceHat	Hacken	Quilaudits	Slowmist	Quantstamp	PeckShield	SolidProof
Access Control & Authorization		O		O	O	O	
Address Hardcoded			O	O			
Adhering To Function Declaration Strictly						O	
Arbitrary Jump/Storage Write	O						
Arithmetic Accuracy Deviation				O			
Assert Violation		O					
Assets Integrity		O					
Authorization Through tx.origin		O	O	O			
Avoiding Use of Variadic Byte Array						O	
Blackhole						O	
Block Values as a Proxy for Time		O	O	O			
Calls Only to Trusted Addresses		O		O	O	O	
Centralization of Control	O		O		O		
Check-Effect Interaction		O					
Code Clones, Functionality Duplication					O		
Compiler Issues	O						
Constructor Mismatch						O	
Cross-Function Vulnerabilities					O		
Dangerous Strict Equalities		O	O				
Data Consistency		O					
Default Visibility		O	O				
Delegate Call to Untrusted Contract	O	O	O			O	
Denial of Service		O		O	O	O	
Dependence on Predictable Variables	O					O	
Deployment Consistency						O	
Deprecated Solidity Functions		O	O			O	
Digital Asset Escrow						O	
Divide before Multiply			O				
EIP Standards Violation		O					
Environment Consistency		O					
ERC20 Idiosyncrasies Handling						O	
Ether/Token Theft	O						
External Contract Referencing			O	O			
False Top-up				O			
Flash Loans	O	O		O			
Floating Pragma		O	O			O	
Following Other Best Practices						O	
Front Running	O					O	
Functionality Checks						O	
Gas Limit and Loops		O	O				
Gasless Send			O			O	
Holistic Risk Management						O	
Improper Events	O					O	
Improper Authorization Scheme	O						SWC Registry 100 ~ 136
Incorrect Inheritance Order		O	O				
Integer Over/Underflow	O	O	O		O		
Kill-Switch Mechanism						O	
Logical Issues	O		O	O	O	O	
Malicious Event Log				O			
Making Visibility Level Explicit						O	
Missing Zero Address Validation			O				
Mishandled Exceptions and Call Stack Limits					O		
Money-Giving Bug						O	
Number Rounding Errors					O		
Oracle Issues	O	O				O	
Outdated Compiler Version	O	O	O	O			
Overflow(& Underflow)				O		O	
Ownership Takeover						O	
Private Modifier			O				
Race Conditions	O	O	O	O			
Redundant Fallback Function						O	
Reentrancy Attack	O	O	O	O	O	O	
Replay Attack				O			
Requirements Compliance		O			O		
Scopeing and Declarations				O			
SELFDESTRUCT Instruction		O				O	
Semantic Consistency Checks						O	
Send Instead Of Tranfer						O	
Shadowing State Variable		O	O				
Signature Issues	O	O					
Stable Imports		O					
Style Guide Violation		O					
Sybil Attack	O						
Tests Coverage		O					
Timestamp dependence					O		
Token Supply Manipulation		O	O		O		
Transaction Ordering Dependence			O		O	O	
TypeCast/Inference			O			O	
Unbounded Loops	O					O	
Unchecked Call Return Value		O	O	O			
Uninitialized Storage Pointer				O			
Unpredictable state			O				
Unused Code	O	O					
User Balances Manipulation		O					
Variable Coverage				O			
Weak Sources of Randomness		O	O				
Zero Function Selector			O				

*The Smart Contract Security Audit service missing from this table did not disclose the coverage of the vulnerabilities.

이 외에도 Solidity의 버전과 스마트 계약에 적용된 표준 등과 같은 정보를 표기하는 경우가 있다.

3.3. 스마트 계약에서 찾은 취약점

표 3은 각 보안 감사 서비스 제공 업체들이 공개한 탐지할 수 있는 취약점의 종류를 요약한 표이다. 표 3에는 탐지할 수 있는 취약점을 종류를 공개한 감사 업체의 결과만 포함했다. 절반 이상의 감사 업체는 어떤 취약점을 검출할 수 있는지 명확히 공개하지 않았다. 보안 감사 서비스마다 검출하는 취약점의 종류 및 범위가 통일되어 있지 않았다. 같은 취약점에 대한 명칭 또한 감사 업체마다 통일이 되지 않은 경우가 많았다.

표 4. 감사 서비스의 취약점 분류
Table 4. Vulnerability Classification of Audit Services

	SourceHat	Consensys	Certik	Hacken	Quilaudits	Cyberscope	Slowmist	Quantstamp	OpenZeppelin	PeckShield	SolidProof	Chainsulting
Critical		O	O	O		O	O		O	O	O	O
High	O		O	O	O		O	O	O	O	O	O
Major		O										
Medium	O	O	O	O	O	O	O	O	O	O	O	O
Low	O		O	O	O		O	O	O	O	O	
Informational	O		O	O	O	O		O		O	O	
Minor		O										
Weakness							O					
Notes									O			
Suggestion							O					
Undetermined								O				
Number of Vul. Class	4	4	5	5	4	3	6	5	5	5	5	3

모든 감사 서비스는 취약점을 3개에서 6개 등급으로 나누어 관리하고 있다. 표 4는 각 보안 감사 보고서에서 정의된 취약점의 등급을 요약한 것이다. 취약점 분류와 마찬가지로 취약점의 등급 또한 감사 업체에 따라서 기준이 다르고 등급 분류가 달랐다.

감사 업체들은 스마트 계약에서 발견한 취약점에 대해 취약점에 대한 설명, 취약점의 원인, 권장 조치 사항 그리고 추후 조치 결과를 보고서에 기재했다.

a) 취약점에 대한 설명: 해당 취약점이 어떤 취약점인지, 어떤 위협을 내포하는지에 대한 설명이다. 일부 보고서에는 취약점에 관한 시나리오도 포함된다.

b) 취약점의 원인: 스마트 계약 코드에서 어떤 부분이 취약한지에 대한 표기이다. 서비스 제공 업체마다 각각 취약점이 발견된 계약의 이름, 함수의 이름 혹은 발견된 정확한 코드 라인을 나타낸다.

c) 권장 조치 사항: 발견된 취약점을 완화 혹은 해결하는 방법을 제시한다. 취약점의 해결책으로써 해당 취약점에 대한 보편적인 방법을 제시하거나 스마트 계약을 분석한 결과 구체적인 해결 방법이 포함된다.

d) 추후 조치 결과: 발견된 취약점에 대해 해결 여부를 추적하고 이를 기록한다.

Ⅳ. 스마트 계약에 대한 가시화 동향

글로 서술된 스마트 계약에 대한 감사 보고서는 일반 탈중앙화 애플리케이션 사용자 및 스마트 계약 참여자가 이해하기 어려울 수 있다. 이를 해결하기 위해 스마트 계약의 내용과 감사 보고서의 내용에 대해 품질 지표와 도표로 가시화할 수 있다. 소수의 감사 서비스에서만 스마트 계약 및 감사 결과에 대해 수치화 및 도표로 가시화했다.

4.1. 스마트 계약 품질 지표 분석

1) Hacken

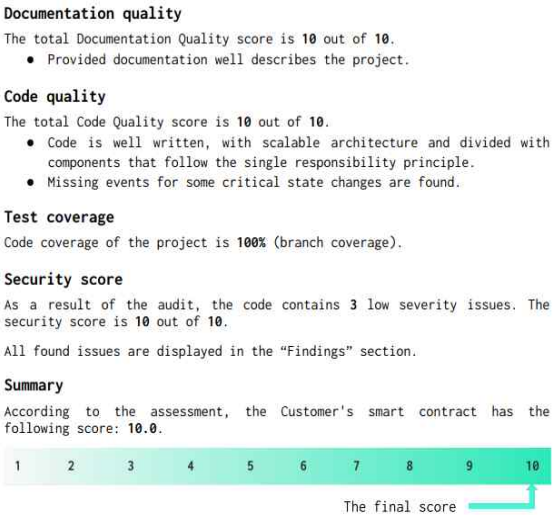

그림 5. Hacken의 계약 점수 예시[30]
Figure 5. Example of Hacken's Contract Score[30]

그림 5는 Hacken에서 감사 보고서에 첨부한 스마트 계약에 대한 점수의 예시이다. Hacken에서는 문서 품질, 코드 품질, 테스트 커버리지 그리고 보안 점수를 산출하고, 가중치를 합산하여 스마트 계약에 대한 점수를 산출한다[31].

a) 문서 품질 점수(d): 문서 품질은 요구사항 명세서를 기반으로 산출한다. 기능 요구사항 5점, 기술 요구사항 5점(Natspec 점수: 3, 프로젝트 기술 규격 점수: 1,

개발 환경 기술 점수: 1)을 더해 총 10점으로 계산된다.

b) 코드 품질 점수(c): 코드 품질에는 코딩 컨벤션과 개발 환경을 통해 산출된다. 총점은 10점으로 계산된다.

c) 테스트 커버리지(t): Solidity에 대한 테스트 커버리지는 분기 커버리지가 적용된다. 단 코드의 길이가 250줄보다 짧은 경우 테스트 커버리지 점수를 따로 반영하지 않는다.

d) 보안 점수(s): 보안 점수는 코드에서 검출된 취약점에 등급에 비례하여 총점에서 감점된다. 보안 점수는 최저 0점에서 최고 10점으로 계산될 수 있다.

e) 스마트 계약 점수: 스마트 계약에 대한 점수를 계산하는 방법은 Equation (1)과 같다.

$$(1) \qquad \frac{d + 2c + 7s\sqrt{t}}{10}$$

단 스마트 계약의 코드 길이가 250줄 미만이면 Equation (2)를 적용하여 계산한다.

$$(2) \qquad \frac{d + 2c + 7s}{10}$$

2) Quantstamp

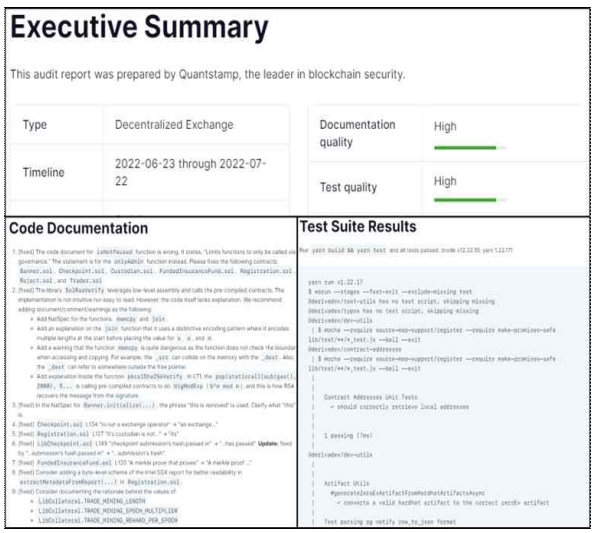

그림 6. Quantstamp의 감사 점수 예시[32]
Figure 6. Example of Quantstamp's Scores in Audit[32]

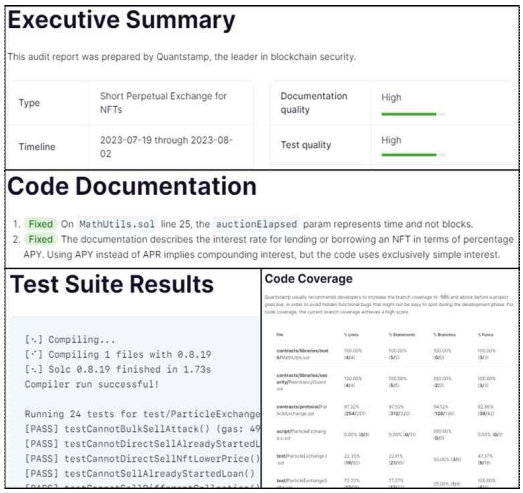

그림 7. 감사에서 Quantstamp 점수의 예[33]
Figure 7. Example of Quantstamp's Scores in Audit[33]

Quantstamp에서는 문서 품질 점수와 테스트 품질 점수를 산출한다. 그림 6과 그림 7은 감사 보고서의 요약 부분에 표기된 문서와 테스트에 대한 품질 점수와 보고서에서 찾은 점수와 관련되어 보이는 요소들에 대한 예시들이다. 하지만 감사 보고서에는 Code Documentation 항목과 테스트 결과와 점수와의 관계가 설명되어 있지 않다. 또한 Quantstamp에서 공식적으로 제공하는 보안 감사 서비스 관련 문서에도 품질 점수들이 어떻게 계산되는지 설명되어 있지 않다.

3) SolidProof, Chainsulting

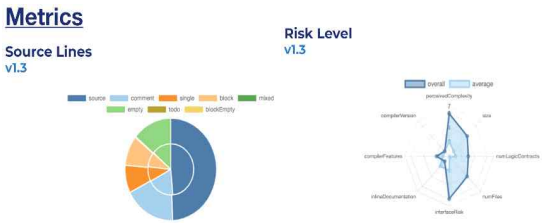

그림 8. SolidProof의 감사 지표 예시[34]
Figure 8. Example of SolidProof's Metrics in Audit[34]

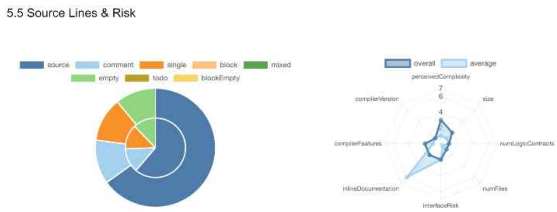

그림 9. Chainsulting의 감사 지표 예시[35]
Figure 9. Example of Chainsulting's Metrics in Audit[35]

그림 8은 SolidProof의 보안 감사 보고서 중 품질 지

표를 측정 및 가시화한 예시이다. 그림 9는 Chainsulting의 보안 감사 보고서 중 품질 지표를 측정 및 가시화한 예시이다. 두 업체 모두 같은 도구를 통해 품질 지표를 측정 및 가시화했다. 왼쪽의 원그래프는 전체 코드 라인 중 코드, 주석, 공백 등의 비율을 나타낸 그래프이다. 오른쪽의 레이더 차트는 스마트 계약의 규모, Logic Contract의 개수, 파일의 개수 등의 8가지 품질 지표를 측정하고 평균치와 비교하여 나타낸 것이다.

4.2. 스마트 계약 설계 추출

1) 상속 차트

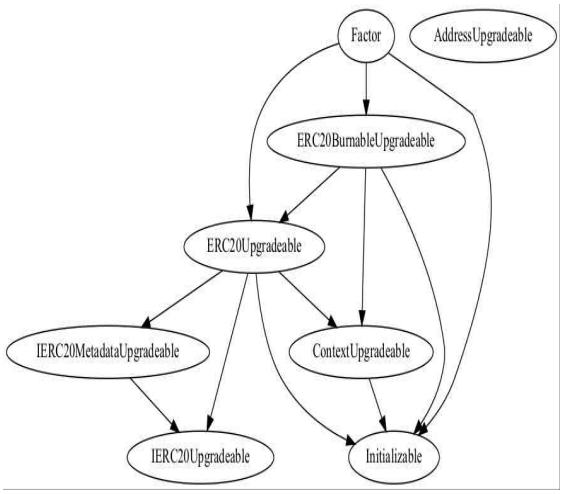

그림 10. 상속 차트의 예[36]
Figure 10. Example of Inheritance Chart[36]

상속 차트는 스마트 계약의 각 계약 간 상속 관계를 나타낸 그래프이다. 상속 차트를 통해 계약 간의 관계 및 연관된 표준 정보를 알 수 있다. 보안 감사 보고서에서 상속 차트를 통해 주로 계약 단위의 시스템 구조를 나타낼 수 있다.

2) 함수 그래프(Call Graph)

함수 그래프는 각 계약에 포함된 함수와 함수 간 호출 정보를 알 수 있다. 함수의 유형마다 테두리의 색을 다르게 하여 구분하였다. 호출의 성격마다 화살표의 색을 다르게 하여 내부 호출과 외부 호출을 구분하였다. 또 각 호출에 대해 하나의 화살표를 그려 화살표의 개수를 통해 함수 간 호출 관계가 복잡한 정도를 알기 쉽게 했다. 보안 감사 보고서에서 함수 그래프를 통해 함수 단위의 시스템 구조를 나타낼 수 있다.

3) 함수 개요표

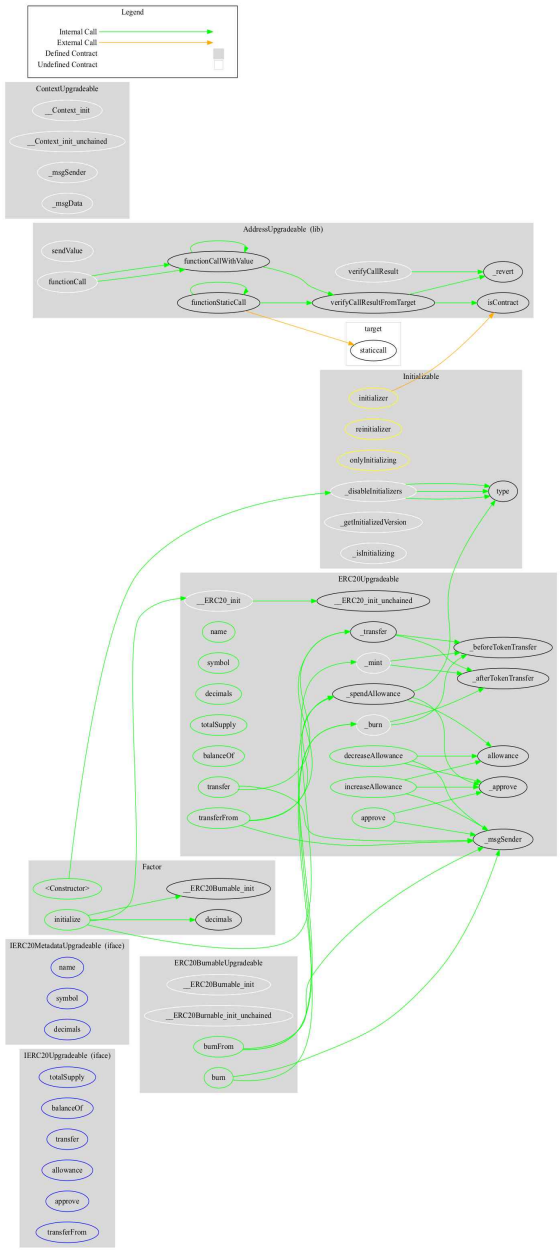

그림 11. 함수 그래프(콜 그래프)의 예[36]
Fig. 11. Example of Function Graph(Call Graph)[36]

함수 그래프는 각 계약에 포함된 함수와 함수 간 호출 정보를 알 수 있다. 함수의 유형마다 테두리의 색을 다르게 하여 구분하였다. 호출의 성격마다 화살표의 색을 다르게 하여 내부 호출과 외부 호출을 구분하였다. 또 각 호출에 대해 하나의 화살표를 그려 화살표의 개수를 통해 함수 간 호출 관계가 복잡한 정도를 알기 쉽게 했다. 보안 감사 보고서에서 함수 그래프를 통해 함수 단위의 시스템 구조를 나타낼 수 있다.

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
OwnableUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__Ownable_init	Internal	✓	onlyInitializing
	__Ownable_init_unchained	Internal	✓	onlyInitializing
	owner	Public		-
	_checkOwner	Internal		
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
Initializable	Implementation			
	_disableInitializers	Internal	✓	

그림 12. 기능 개요 테이블의 예[37]
Figure 12. Example of Function Overview Table[37]

그림 12의 함수 개요표는 함수에 대한 정보를 표로 단순하게 나타낸 것이다. 각 계약이 포함하는 함수의 이름, 함수의 수정자와 가시 제한자와 기능 제한자를 표에 정리한다. 다른 설계 가시화와는 달리 표 형식이기 때문에 보고서 별로 차이가 거의 없는 다른 설계에 비해 보고서 별로 용도에 맞게 자유롭게 표현하는 경향이 있다. 함수 개요표를 통해 계약 내부의 함수의 종류와 각 함수 별 성격을 쉽게 유추할 수 있다.

4) 시스템 다이어그램

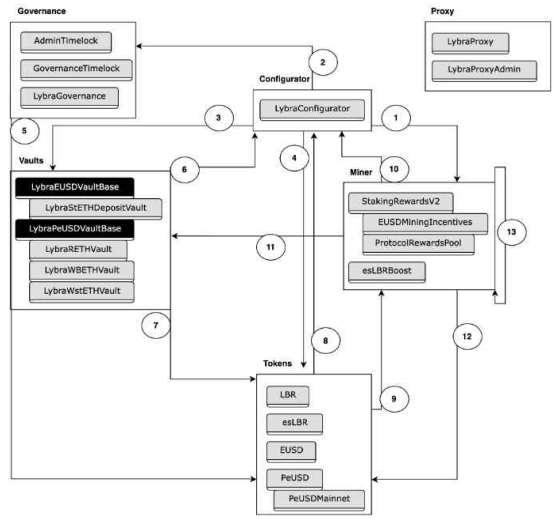

그림 13. 시스템 다이어그램의 예[38]
Figure 13. Example of System Diagram[38]

그림 13의 시스템 다이어그램은 Consensys 사의 Diligence 서비스에서 사용하는 설계 가시화 기법이다. 시스템 다이어그램은 시스템 내부에 역할과 계약이 중심이 되어 통화와 데이터 흐름에 초점을 맞춰 도식한다. 시나리오의 흐름을 번호가 표시된 화살표와 각 화살표에 대한 설명을 통해 표현한다. 보안 감사 보고서에서 시스템 다이어그램은 복잡할 수 있는 경제 시스템의 이해를 돕는데 사용 될 수 있다.

5) 역할 그래프

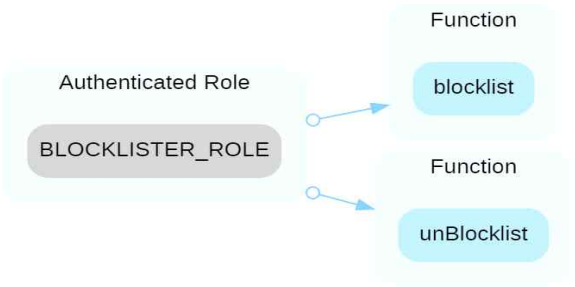

그림 14. 역할 그래프의 예[39]
Figure 14. Example of Role Graph[39]

그림14의 Certik의 역할 그래프는 역할별로 권한을 가지는 함수를 읽기 쉽게 표현한다. 단순 글로 서술된 역할 설명에 비해 쉽게 역할을 파악할 수 있다.

4.3. 기존 스마트 계약 가시화 연구와 비교

Solidity는 스마트 계약을 작성하기 위해 개발된 객체지향 언어이다[40]. 따라서 기존 스마트 계약 가시화 연구에서는 객체 지향 언어의 품질 지표와 다이어그램을 Solidity의 스마트 계약에 적용했다.

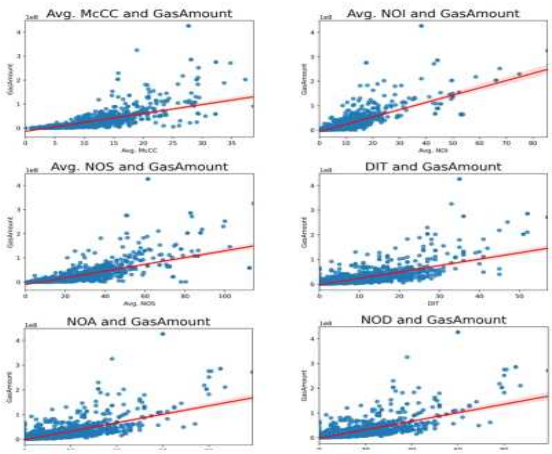

그림 15. 객체지향 복잡성과 가스 소비량의 관계[41]
Figure 15. Relationship between Object-Oriented Complexity and Gas Consumption[41]

그림 15는 객체 지향 언어에 대한 복잡도가 Solidity에 유효한지 확인하기 위해 가스 소모량과의 상관관계를 분석한 연구의 결과이다. 그 차트로 그린 6개의 복

잡도는 가스 소모량의 상관 계수가 0.7 이상으로 서로 유의미한 상관관계를 보였다. 또한 그 외 실험한 대부분의 복잡도도 0.5 이상으로 상관관계가 있음을 보였다.

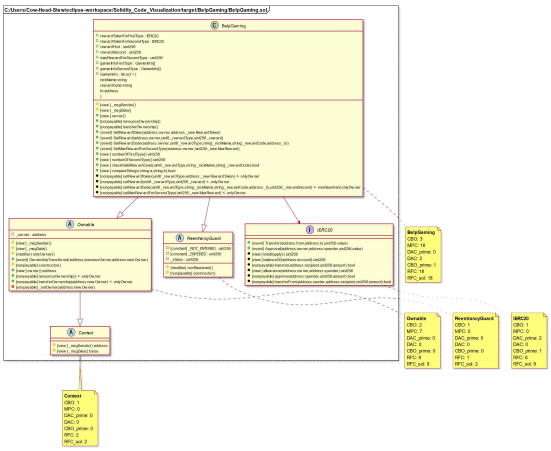

그림 16. Solidity를 위한 클래스 다이어그램과 객체지향 복잡성[42]
Figure 16. Class Diagram and Object-Oriented Complexity for Solidity[42]

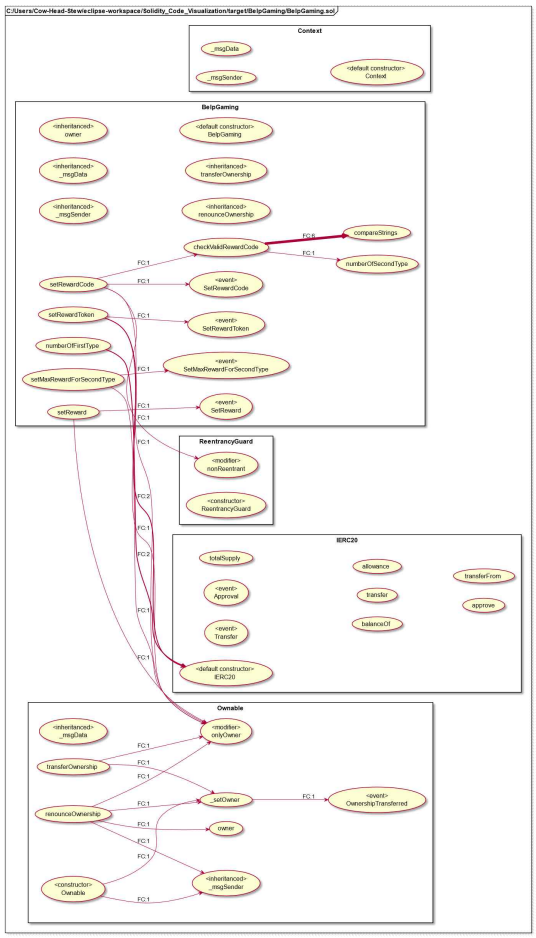

그림 17. Solidity에 대한 호출 그래프[43]
Figure 17. Call Graph for Solidity[43]

그림 16은 Solidity에 Class Diagram과 객체지향 복잡도를 적용하여 가시화한 연구이다. Class Diagram을 통해 각 계약의 상태 변수 및 함수들을 나타냈다. 또한 각 계약에 대해 복잡도를 표기하여 복잡한 계약을 표시했다. 그림 17은 Solidity에 Call Graph를 적용하여 가시화한 연구이다. Call Graph를 통해 각 계약 내부의 함수를 표시했다. 또한 계약 간 내부 및 외부의 함수 호출과 그 횟수를 표시했다. 잦은 호출일수록 더 굵은 화살표로 나타내어, 복잡한 함수 호출을 알기 쉽게 했다.

5. 결론 및 향후 연구

본 논문에서 스마트 계약 감사 보고서를 중심으로 스마트 계약에 대한 보안 감사 동향과 서비스를 정리했다. 스마트 계약에 대한 보안 감사는 정적 분석 및 동적 분석을 통한 분석 결과를 통해 스마트 계약에 대한 정보를 추출하고, 계약 내의 취약점을 검출한다. 스마트 계약으로부터 계약의 시나리오를 포함한 계약의 정보를 추출한다. 토큰의 경우 토큰 경제 시스템 또한 분석한다. 분석 결과를 세부적으로 기재하는 감사 보고서의 경우 각 함수에 대해 수정자, 접근 및 기능 제한자를 분석하여 기재한다. 스마트 계약을 표현하기 위해 가시화를 적용한 사례도 있지만 스마트 계약의 특성을 반영한 품질 지표와 도표가 필요하다. 스마트 계약에서 검출한 취약점에 관해서는 설명, 검출 위치, 권장 조치 그리고 조치 결과를 파악하여 기재한다. 스마트 계약에서 발견할 수 있는 취약점들의 항목 명과 분류기준이 통일되지 않았다는 문제가 있다. 추후 스마트 계약에 대한 품질 지표 및 도표에 관한 연구를 진행할 예정이다.

References

[1] D. Vidal-Tomás, "Transitions in the cryptocurrency market during the COVID-19 pandemic: A network analysis," Finance Research Letters, Vol. 43, No. 101981, 2021.
[2] Kim, T., & Yang, J. Y. (2022). How to Prove the Identity of Artist When Creating Non-fungible Tokens. The Journal of the Convergence on Culture Technology, 8(5), 669 - 676. https://doi.org/10.17703/JCCT.2022.8.5.669
[3] Raynor de Best, Daily 24h volume of all crypto

combined up until August 2, 2023 [Internet], https://www.statista.com/statistics/1272903/cryptocurrency-trade-volume/.
[4] PR Newswire, Global Smart Contracts Market to Reach USD 9850 Million by 2030 with 24% CAGR | Revolutionizing Contract Management, Exploring the Opportunities and Trends Report by Zion Market Research [Internet], https://finance.yahoo.com/news/global-smart-contracts-market-reach-160000824.html.
[5] Andrew Kamsky, Crypto Hacks 2023: Full List of Scams and Exploits as Millions Go Missing [Internet], https://www.ccn.com/education/crypto-hacks-2023-full-list-of-scams-and-exploits-as-millions-go-missing/.
[6] H. S. Jin, D. O. Kim, Y. C. Kim, J. T. Oh and K. Y. Kim, “Technology Trends in Blockchain Distributed Agreements,” *Journal of the Institute of Electronics and Information Engineers*, Vol. 48, No. 5, pp.63-74, 2021.
[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized business review, 2008.
[8] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, 2014.
[9] T. Takenobu, "Ethereum EVM illustrated." Github Pages, 2018.
[10]G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, pp.1-41, 2022.
[11]A. Savelyev, "Contract law 2.0:‘Smart’contracts as the beginning of the end of classic contract law." Information & communications technology law, Vol. 26 No.2, pp.116-134, 2017.
[12]H. Taherdoost, "Smart Contracts in Blockchain Technology: A Critical Review." Information, Vol. 14, No. 2, 2023.
[13]Languages - DefiLlama [Internet] ,https://defillama.com/ languages.
[14]W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," *IEEE Access,* Vol. 6, pp. 53019-53033, 2018.
[15]M. Tian, and C. Wei, "Portrait of decentralized application users: an overview based on large-scale Ethereum data," *CCF Transactions on Pervasive Computing and Interaction,* Vol 4, No. 2, pp.124-141, 2022.
[16]A. M. Rozario and M. A. Vasarhelyi, "Auditing with Smart Contracts," *International Journal of Digital Accounting Research*, Vol. 18, pp.1-27, 2018.
[17]Smart Contract Weakness Classification (SWC) [Internet], https://swcregistry.io.
[18]Smart Contract Audits by SourceHat [Internet], https:// sourcehat.com/audits/.
[19]Public Smart Contract Audits and Security Reviews | Consensys Diligence [Internet], https://consensys.io/ diligence/audits/.
[20]Smart Contract Audit - Web3 Security Leaderboard [Internet], https://www.certik.com/products/smart-contract -audit.
[21]Smart Contract Audit reports - Hacken [Internet], https://hacken.io/audits/.
[22]Smart Contract Auditing Services for Ethereum Blockchain [Internet], https://www.quillaudits.com/services/ethereum- smart-contracts-auditing.
[23]Ethereum Smart Contract Audit - Cyberscope [Internet], https://www.cyberscope.io/ethereum-smart-contract-audit.
[24]Smart Contract Security Audit Service Introduction, Exchange Security Solution - SlowMist - Focusing on Blockchain Ecosystem Security [Internet], https:// www.slowmist.com/service-smart-contract-security-audit.html.
[25]Quantstamp: Audits [Internet], https://quantstamp.com/ audits.
[26]OpenZeppelin [Internet], https://www.openzeppelin.com/ #secure-code.
[27]PeckShield - Industry Leading Blockchain Security Company [Internet], https://peckshield.com/#services.
[28]Audit | Solidproof.io | DE Trust Made In Germany [Internet], https://solidproof.io/audit.
[29]Smart Contract Audit - Chainsulting [Internet], https:// chainsulting.de/smart-contract-audit/.
[30]DeXe Network_SC Audit Report_22052023[SA-962] [PDF], https://wp.hacken.io/wp-content/uploads/2023/08/DeXe-Network_SC-Audit-Report_22052023SA-962.pdf.
[31]SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS SCORING METHODOLOGY [Internet], https://docs.google.com/document/d/1cPKijtHoNsPX8P6UJmeQVc9Un44_FgNh0QV32F_RFCw/edit.
[32]DerivaDEX 2 - Report [Internet], https://certificate.quantstamp.com/full/deriva-dex-2/260ed58a-a197-4dd7-bda3-6586453de89f/index.html.
[33]Particle - Report [Internet], https://certificate.quantstamp.com/full/particle/3cd57a7b-681f-4f38-b0cd-9fd6f2f37a89/index.html.

[34] SmartContract_Audit_Solidproof_Unicrypt_V2_ENMT [PDF], https://github.com/solidproof/projects/blob/main/UNCX%20Network/SmartContract_Audit_Solidproof_Unicrypt_V2_ENMT.pdf.
[35] Lossless_Smart_Contract_Audit_Wrapped_ERC20_20042023 [PDF], https://github.com/chainsulting/Smart-Contract-Security-Audits/blob/master/Lossless/Lossless_Smart_Contract_Audit_Wrapped_ERC20_20042023.pdf.
[36]Factor Smart Contract Audit by SourceHat (formerly Solidity Finance) [Internet], https://sourcehat.com/audits/Factor/.
[37]dkeepernft [PDF], https://github.com/cyberscope-io/audits/blob/main/deeplink-l3-atom/dkeepernft.pdf.
[38]Lybra Finance | Consensys Diligence [Internet], https://consensys.io/diligence/audits/2023/08/lybra-finance/.
[39]Gala Games - CertiK Skynet Project Insight [Internet], https://skynet.certik.com/projects/gala-gala-games.
[40]The Solidity Authors, Solidity - Solidity 0.8.21 documentation [Internet], https://docs.soliditylang.org/en/v0.8.21/.
[41]J. H. Kim, C. S. Park, S. Y. Moon and R. Y. C. Kim, "Best Practices on Improving Gas Consumption through Simplifying Quality Complexity of Solidity code for Smart Contracts in Distributed Network Environments." in *Proceedings of the International Conference on Green and Human Information Technology,* Jeju, 2022, pp. 166-167.
[42]C. S. Park, B. K. Park, S. Y. Moon and R. Y. C. Kim, "Extracting Code Complexity for Auditing A Smart Contract," in *Proceedings of the Korean Institute of Smart Media* 2022 Comprehensive Academic Conference, Daejeon, pp. 63-65, 2022.
[43]C. S. Park, B. K. Park, S. Y. Moon and R. Y. C. Kim, "Applying Code Visualization into Solidity for Auditing of Smart Contract," *Advanced Engineering and ICT-Convergence Proceedings*, Vol. 5, No. 2, pp. 333-336, 2022.

※ 본 연구는 2023년도 문화체육관광부의 재원으로 한국콘텐츠진흥원(과제명: 인공지능 기반 사용자 대화형 멀티모달 인터랙티브 스토리텔링 3D장면 저작 기술 개발, 과제번호: RS-2023-00227917,기여율:25%) 지원, 2023년도 행정안전부 재난안전산업 기술사업화 지원 사업(과제명:프로그래시브 웹 앱(PWA) 기반의 시설물 상태평가 엔진을 적용한 AR 시설물 인터페이스 개발,과제번호: RS-2022-00155579,기여율:25%)의 지원, 교육부 및 한국연구재단의4단계 두뇌한국21 사업의 지원(F21YY8102068, 기여율: 25%)과 2023년도 정부(교육부)의 재원으로 한국연구재단 기초연구사업(과제명: NLP BERT Model 기반 자동 리팩토링을 통한 무결점 코드화 연구, 과제번호: No.2021R1I1A3050407,기여율:25%)의 지원을 받아 수행된 연구임.