

## 가상화폐를 이용한 자금세탁 도구화에 관한 연구

## A Study on the Tooling of Money Laundering Using Cryptocurrency

송혜진\*

Hye Jin Song\*

Professor, Department of Police Administration, Semyung University, Jecheon, Republic of Korea

\*Corresponding author: Hye Jin Song, knupe1@hanmail.net

## ABSTRACT

**Purpose:** The purpose of this study is to examine the path of money laundering of criminal proceeds through cryptocurrency using criminal script analysis and to devise measures to prevent and prevent criminal justice agencies from doing so. **Method:** Based on the results of a prior study on the profit path of cryptocurrency through money laundering and criminal cases in Korea, the path of money laundering was analyzed using criminal script techniques. **Result:** Most of the cryptocurrencies that have been launched are converted into criminal proceeds, which are re-launched and cashed or have a vicious cycle of being used as criminal funds are used. According to the script, the route of money laundering is mainly converted to criminal proceeds from cryptocurrency exchanges using anonymity, which is repeated several times, making it very difficult to find the money using cryptocurrency in criminal justice institutions. **Conclusion:** As the method of money laundering using cryptocurrency is becoming more sophisticated, legal sanctions and preventive institutionalization should be prepared for the prohibition or confiscation of cryptocurrency transactions for money laundering after understanding the flow.

**Keywords:** Cryptocurrency, Criminal proceeds, Money laundering, Defi, Blockchain

## 요약

**연구목적:** 본 연구의 목적은 가상화폐를 통한 범죄수익금의 자금세탁 경로를 범죄스크립트 분석을 이용하여 살펴보고, 이에 대한 형사사법기관의 예방 및 대책 방안을 강구하기 위함이다. **연구방법:** 자금세탁을 통한 가상화폐의 수익 경로에 대하여 선행연구 조사결과와 우리나라에서 발생된 범죄사례 등을 바탕으로 범죄스크립트 기법을 활용하여 자금세탁 경로를 분석하였다. **연구결과:** 자금세탁을 한 가상화폐 대부분이 범죄수익금으로 전환되고, 이 수익금은 다시 세탁되어 현금화 되거나 범죄자금으로 쓰이는 악순환이 발생하는 특징을 가지고 있다. 이에 스크립트를 통해 본 결과 자금세탁의 경로는 익명성을 이용한 가상화폐거래소에서 주로 범죄수익금으로 전환되고 있으며, 이 경로를 여러 번 반복되기 때문에 가상화폐소를 이용하여 세탁되어진 자금을 형사사법기관 등에서 찾는 것이 매우 어려운 것으로 파악되었다. **결론:** 가상화폐를 이용한 자금세탁의 방법이 교묘화 되어가고 있어 이에 따른 흐름을 파악한 뒤 자금세탁에 대한 가상화폐 거래금지 또는 몰수에 따른 강력한 처벌과 피해를 예방할 수 있는 제도적 보완장치가 마련되어야 할 것이다.

**핵심용어:** 가상화폐, 범죄수익금, 자금세탁, 디파이, 블록체인

Received | 6 August, 2021

Revised | 7 September, 2021

Accepted | 7 September, 2021

OPEN ACCESS



This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/4.0>) which permits unrestricted noncommercial use, distribution, and reproduction in anymedium, provided the original work is properly cited.

## 서론

최근 몇 년 사이 전 세계적으로 가상화폐 열풍이 불면서 자본주의 사회에서 투자하고 보호받는 일반적인 금융이 아닌 가상이라는 이름의 화폐가 현재의 경제시스템을 변화시키고 있다. 2030 세대에서 붐이 불고 있는 가상화폐 투자는 분명 부의 축적을 가져왔다. 하지만 범죄의 심각성과 범죄피해액의 기하급수적 증가라는 이면 역시 존재한다. 2021년 경찰청 통계를 살펴보면, 2017년부터 2020년 범죄피해액은 평균 4035억 원이지만 2021년 전반기 피해액만 해도 4조 1615억이다. 이 중 범죄수익금이 자금세탁으로 이어져 세상 밖으로 나오는 금액도 크다고 볼 수 있다. 이를 전세계적으로 본다면 범죄피해액, 즉 범죄수익금에 대한 자금세탁 금액은 상당할 것으로 추산된다. 가상화폐는 이미 사기, 유사수신, 랜섬웨어, 보이스피싱, 도박, 자금세탁, 마약거래, 성매매, 외국환거래법 위반에 이르기까지 범죄수단으로서의 도구로 활용도가 상당하다. 특히, Lee(2016)는 가상화폐는 비트코인의 도입 이후 비약적으로 발전해왔으나 거래시 정확한 실명확인 절차를 거치지 않고 거래상대방에 대한 익명성 허용 등으로 인해 자금세탁행위에 이용되는 사례들이 해외에서 다수 발생되고, 현재 주요국들은 가상화폐가 송금 및 환전과정에서 자금세탁위험에 노출되어 있다는 점을 감안하여 자금세탁방지 의무를 부과하고 있다고 언급했다.

2021년 9월까지 등록이 안된 가상화폐거래소를 강력히 규제하겠다고 법무부가 입장을 밝혔고, 신고하지 않는 거래소는 모두 폐쇄될 예정이라고 경고하였다. 우리나라만 해도 언론에서 보도되는 가상화폐는 이미 200여 개이고 가상화폐거래소만 해도 100여 개가 육박하고 있다. 이렇게 빠른 속도로 증가하고 있는 가운데 새로운 금융거래의 시작을 알린다는 의미에서 긍정적인 부분도 있겠지만, 가상화폐를 이용한 자금세탁의 경우 익명성이 보장되기 때문에 범죄를 저지르기에는 큰 장점을 가졌다. 따라서 가상화폐를 이용한 자금세탁에 대한 범죄를 제지하고 예방할 수 있는 방법을 모색해보고자 한다.

현재 가상화폐를 이용한 자금세탁이 이루어지는 과정을 시도한 연구는 찾아보기 힘들기 때문에 본 연구는 가상화폐를 이용한 자금세탁의 경로와 그 경로로 이용되고 있는 디파이, 디파이를 구축하고 있는 블록체인을 통해 이루어지고 있는 거래들에 있어 범죄로 악용되는 부분과 범죄 수법들을 통해 가상화폐가 어떻게 도구화되어 가고 있는지에 대해 연구해보고자 한다. 연구방법으로는 기존 문헌연구들과 각종 통계자료를 기초로 분석하였고, 자금세탁에 대한 범죄 흐름을 토대로 스크립트 분석을 진행하였다.

## 이론적 논의 및 선행연구의 검토

가상화폐는 기존의 중앙금융서비스에서 제공하는 법정화폐가 아닌 현물이 존재하지 않는 화폐이다. 말 그대로 가상인 것이다. 가장 많이 알려진 가상화폐는 비트코인으로 암호기법을 사용하였다 해서 암호화폐라고 불리기도 한다.

Kang(2021)은 국제자금세탁방지기구(FATF)에서의 가상화폐 정의는 디지털적으로 거래되는 가치의 디지털 표현으로 (1) 교환의 수단, (2) 가치의 척도, (3) 법적인 통화의 지위를 갖지는 않지만, 어디에서든 가치의 저장 수단으로 기능한다고 했으며, 어떠한 국가에 의해 발행되거나 보증되지도 않고, 위의 기능을 오로지 가상화폐 사용자들이 사회 내의 합의에 의해 기능한다고 말하고 있다. 가상화폐 시스템의 특징은 크게 탈중앙성, 익명성, 불가역성이라는 특징이 있다. 가상화폐는 일반 중앙금융 시스템에 의해 운용되는 방식이 아닌 블록체인을 기반으로 탈중앙화 금융서비스를 제공하고 있는데 이것을 디파이(Defi)라고 한다. 디파이를 탈중앙화 금융 서비스에 더하여 ‘블록체인 네트워크에서 작동하는 탈중앙화 금융서비스’라고 정의할 수 있다. 즉 디파이 금융서비스는 기본적으로 가상자산을 기반으로 하고 있다.

Choi(2016)는 이런 가상자산을 기반으로 한 디파이는 금융, 보험, 결제, 대출, 외환, 투자, 신탁, 발행 등 모든 분야를 현실 화폐나 금융경제와 연결되지 않은 블록체인 네트워크 금융서비스라고 했고, 블록체인은 별도의 중앙관리시스템을 두고 있지 않기 때문에 네트워크에 문제가 발생하는 경우에 책임소재가 모호해질 수 있고, 불법한 거래 대금 결제나 마약, 탈세 등과 같은 불법적인 용도에 블록체인 기술이 악용될 수도 있다고 했다. 따라서 이러한 가상화폐를 이용하여 자금세탁이 이루어지고, 범죄수익 또한 이런 가상화폐를 통해 축적하고 현금처럼 사용할 수 있다고 했다.

Hwang(2018)은 가상화폐의 익명성과 중개자가 없이 비밀스럽게 금융서비스를 이용할 수 있다는 장점을 악용하여 발생하는 범죄가 자금세탁이며, 2013년도 초반까지만 하여도 가상화폐를 결제수단으로 인정한 업체들은 대부분 온라인 게임이나 도박, 마약 거래 등 불법적인 거래와 연관된 것들이었다고 주장하고 있다. 가장 대표적인 사례가 미국의 실크로드(Silkroad)로, 암호화폐를 통한 환치기는 익명성이 보장되어 마약거래 및 보이스피싱, 온라인 도박 등을 통한 범죄수익을 해외로 반출하는데 활용된 경우이다. Seo(2018)는 테러단체가 테러자금 조달을 위해서 비트코인을 모금하기도 하고, 범죄수익을 자금 세탁하는 등 암호화폐를 이용하는 범죄도 날로 증가하고 있다며, 이슬람 극단주의 테러단체인 IS가 추적이 어렵다는 이유에서 비트코인과 같은 암호화폐를 이용하고 있다고 주장했다. 또한 유럽연합안보연구에서 발간한 보고서에 따르면, IS 지지자들이 당국에 포착될 수 있는 위험을 최소화하면서 신속하게 송금하기 위해서 비트코인과 같은 암호화폐를 이용하고 있고, 이것이 IS의 주요 수입원이 되고 있다고 하였다.

우선, 국내 연구로는 암호화폐를 이용한 자금세탁 행위에 대한 법적 규제에 대한 연구로 Yeon et al.(2017)는 암호화폐 관련 범죄유형을 분류하여 암호화폐를 이용한 자금세탁 및 시세조종 행위에 대하여 보다 적극적인 형사정책적 수단이 투입되어야 하며, 특히 범죄 목적 믹싱 서비스 제공행위에 대한 처벌조항이 신설되어야 한다고 제시하였다. Kang(2018)은 가상화폐의 이용증가와 함께 범죄자의 범죄수익을 은닉하고 돈세탁의 수단으로 가상화폐의 익명성을 이용한 사례도 증가하고 있기 때문에 이를 위해서는 돈세탁방지를 위한 규제 및 입법 필요성에 대해 제시하였다. Baek et al.(2021)는 암호화폐를 이용한 자금세탁방지를 위한 방안을 제시하고 있다. Hwang(2018)은 가상화폐의 악용사례에 대한 문제점을 제시하고 건전한 거래를 활성화할 수 있는 방안을 모색하였다. 또한 Buxton et al.(2015), Barray et al.(2016)의 연구에서는 암호화폐가 자금세탁을 용이하게 하여 테러조직의 자금조달이나 범죄, 부정부패 등 범죄에 악용될 가능성이 크다는 것을 지적하였다.

최근 다양한 분야에서 가상화폐에 대한 활발한 연구들이 이루어지고 있다. 특히, 가상화폐 시장의 자금세탁이 외국에서 빈번하게 발생하고 있다는 점에서 우리나라와도 밀접한 관련이 있다. 이미 각종 아동·성인물 사이트에서 가상화폐로 결제가 진행되고 있고, 마약 거래 또한 가상화폐 등을 이용하고 있다. 특히, 마약 거래방법으로 가상화폐를 받은 뒤 물건은 약속한 장소에 묻어두는 식의 ‘보물찾기’ 수법을 사용하고 있어서 그 문제가 심각하다고 할 수 있다. 이러한 국내외 연구들을 살펴보면 가상화폐를 이용하여 얻은 범죄수익금과 테러 자금 등을 조달하기 위해 자금세탁이 발생하고 있다고 언급하였고, 범죄 유형들에 대한 법적 대응방안과 법 제도 개선에 대해 연구한 결과들이 주를 이루고 있다. 또한 법적 제도 개편을 통한 범죄 예방에 치우쳐 있는 연구들이 많아 범죄 특성과 경로를 파악하는데는 한계가 있다. 특히, 가상화폐에 대한 범죄는 크게 암호화폐 침해범죄와 암호화폐 이용범죄로 나뉘고 있고, 자금세탁의 경우 이용범죄 유형에 속하고 있다. 자금세탁의 경우 각종 범죄의 수익을 변환하여 사용하는 경우로 대상범죄의 도구가 되고 있는 가상화폐에 대해 범죄스크립트를 분석해 경로를 알아보고 그에 따른 형사사법기관의 범죄 예방 및 대책 방안을 수립 할 수 있는 기초적인 자료로 활용하고자 하는데 그 연구의 의의가 있다.

## 스크립트 분석을 통한 자금세탁 도구화 진행과정 및 논의

### 범죄 스크립트 분석

본 연구는 가상화폐를 이용한 자금세탁 범죄에 대한 진행 과정을 논의하기 위해 범죄스크립트 분석을 채택하였다.

Cornish(1994)는 범죄를 성공적으로 완수하는데 필요한 범죄 행위자, 도구, 장소 등에 필요한 체계적인 분석 틀을 개발하기 위하여 인지 심리학에서 스크립트(script) 개념을 차용하였고, 이것이 범죄스크립트 분석기법(Crime Script Analysis)으로 발전하여, 범죄자가 범죄 전·중·후 전 과정에서 행하는 절차를 각 단계별로 설명, 분석하는 것이라고 하였다. 범죄스크립트는 범죄단계분석을 통하여 범죄수법을 일반화하고 가상화폐가 자금세탁의 도구화되어 가는 과정을 살펴볼 수 있다. 특히 가상화폐를 이용한 범죄수익금에 대한 자금세탁은 경로에 대한 연구가 부족하고 범죄자에 대한 추적이 어렵기때문에 기존 사례들을 분석하여 범죄스크립트를 작성하였다. 대표적인 Silk road나 BCT-e, 러시아, 중국 등지에서 발생하는 사건 사례들을 통하여 국제적으로 이루어지고 있는 가상화폐를 통한 자금세탁 진행 과정을 논의하고 우리나라에서도 적용될 수 있는 정책적 방안과 법제도 마련을 제언하고자 한다.

### 준비단계

사례분석 결과 가상화폐를 이용한 자금세탁의 경우 준비단계는 크게 마약 거래를 통한 수입, 인터넷 상의 도박, 아동·성인 음란물사이트에서의 결제, 랜섬웨어, 보이스 피싱을 통해 현물화폐를 받은 뒤 바로 가상화폐로 전환하는 방법과 거래소 간 해킹을 통한 가상화폐 습득, 유사수신 등을 이용해 얻은 범죄수익금을 가상화폐로 수집하게 된다. 범죄조직은 범정화폐나 전자화폐가 아닌 익명성이 높은 가상화폐를 이용하여 안전하게 세탁할 수 있는 행동 패턴을 보이는 것으로 확인됐다. 뿐만 아니라 개인의 탈세나 재산은닉을 위한 방법으로 가상화폐를 통한 자금세탁을 시도하고 있고, 자금세탁을 의뢰받고 있는 업체도 생겨나고 있다. 즉 개인이 어렵게 노력하지 않아도 자금세탁을 할 수 있는 구조가 되어 언제든지 의뢰할 수 있게 되었다. 실제 2021년 3월 국세청은 가상재산을 은닉한 고액체납자 2,416명에 대한 세금 366억 원을 거둬들였다. 고액체납자들은 가상화폐를 통해 재산을 은닉하여, 세금탈루를 하고 있었고, 이런 자산들이 결국에 자금세탁을 통해 다시 현금화되어 지는 것이다. 하지만 여기에서도 조심해야 할 부분은 자금세탁을 의뢰받은 거래소조차 사기인 경우가 많다. 자금세탁의 각종 범죄사례를 살펴본 결과 대부분이 범죄로 인해 얻은 수익금을 은닉하기 위한 방법으로 자금세탁을 택했고, 테러 자금조달을 위한 방법으로 가상화폐를 이용해 자금세탁을 시도해왔다. 이렇게 모인 가상화폐들은 자금세탁을 위한 실행단계로 넘어간다.

### 범죄실행

범죄실행 단계에서는 준비단계에서 얻은 범죄수익금을 의뢰받은 자금세탁거래소가 또는 가상화폐거래소가 각국의 가상화폐거래소에 전송 및 송달하고, 수십 여 개국의 수십 여개의 거래소를 거쳐 의뢰받은 자금 또는 범죄수익금을 세탁을 하게 된다. 여러 단계를 거쳐 범죄수익을 세탁하게 되면 결과적으로 추적이 어려워지기 때문에 찾아내기가 쉽지 않다. 더군다나 가상화폐가 가진 익명성은 합법적으로 쓰였을 때 안전할 수 있지만 사법기관으로부터 범죄 인지를 피하기 위한 자금세탁의 수단으로 쓰이게 된다면 이러한 익명성을 남용하게 되는 결과를 낳는다. 이러한 방법으로 범죄자들은 범죄수익금을 세탁하여 다시 한곳으로 통합한 다음 가상화폐 또는 실물화폐로 전환하여 사용하는 방법을 택하고 있다.

실제로 자금세탁을 하는 업체들은 자금세탁을 할 수 있는 나라가 약 67개국이고 거래소만 250여 개를 보유하고 있기 때문

에 한번 범죄수익금을 세탁할 때 최소 19개국 20여 명의 요원이 한 달에 걸쳐 세탁을 진행해 추적하기 어렵다고 광고하는 경우도 있다. 미국에 가상화폐를 이용하여 자금세탁을 하다 기소된 사례를 살펴보면, 2013년 미국에서 Leberthy Reserves를 발행하였던 Leberthy Reserve는 자금세탁과 무허가송금영업의 혐의로 기소되었고, 약 5500만 건의 불법 거래, 60억 달러에 달하는 사기, 신원도용, 컴퓨터해킹, 아동포르노, 마약밀거래 등과 같은 범죄수익을 자금세탁을 한 사실이 드러났으며, 사용자들에게 일정 금액을 받고 거래 계좌를 숨겨주어 거래 추적이 불가능하게 하기도 하였다. Leberthy Reserves는 사용자들이 직접적으로 입금하는 것을 허용하지 않고 거래소를 통하여 거래하는 방식을 취하므로 철저하게 자금세탁할 수 있는 방법을 모색하였다. 다음 사례로 Silk Road의 경우에는 비트코인을 사용하여 마약, 총기 등 불법적인 상품서비스를 제공하는 암시장을 운영하였고, 불법적 거래로부터 얻은 수익 달러의 범죄수익을 자금세탁 하는데 사용하였다. 그 외에도 가상화폐거래소가 또 다른 가상화폐 거래소를 해킹하여 얻은 수익 등으로 실제 달러 등 현금 세탁하는 사례도 발생하였다. 이렇듯 범죄로부터 얻은 수익은 추적하기 어렵게 시스템을 운영(다크웹 등)하여 자금세탁을 하고 있는 것으로 나타났다.

### 범죄실행 후 행동

범죄실행 후 단계에서는 크게 두 가지 형태를 보이고 있다. 첫 번째는 세탁된 가상화폐를 현금화하거나 다시 가상화폐로 전환하는 방법이 있고, 두 번째는 은닉 및 축적하는 행동패턴을 보이고 있다. 이렇게 세탁된 화폐(현물화폐, 코인)는 다시 범죄자금으로 쓰이거나 테러조직의 자금 등으로 조달되고 있다. 앞서 보았듯이 가상화폐 시장은 현물화폐나 전자화폐보다 성장 속도가 빠르게 증가하고 있고, 범죄수익금도 기존 현물화폐에서 통용되는 거래수준보다 빠르게 증가하고 있다. 우리나라의 가상화폐 거래량만 하루에 14조 원에 이르고 있고, 범죄피해액이 4조 원 가까이에 다다르고 있어 가상화폐는 현재 세계 경제와 암시장을 움직일 만큼의 금액으로 늘어났다. 이런 일련의 모든 범죄가 사실상 현실 공간에서 이루어진다고 해도 금전적인 부분은 가상공간에서 이루어지기 때문에 추적하기가 쉽지 않고 영원히 찾을 수 없는 경우들도 발생하고 있다. 가장 큰 문제는 이러한 자금세탁이 가상공간에서는 범죄로 인식되지 않는다는 것이다. 현실 공간에서의 자금세탁의 경우 페이퍼컴퍼니나 대포통장 등을 이용했다면, 가상화폐로 얻은 범죄수익에 대해서는 범죄로 인지하지 않는 경우들도 있고, 이를 다시 세탁해도 별 문제가 없다고 판단하는 범죄자들의 생각이 더 위험한 것이다. 최근 들어 일반 사람들조차 세무에 대한 문제로 자금세탁을 의뢰하는 경우도 종종 발생하고 있다. 그만큼 범죄를 저지르고 실행하는 동안 이런 방법들이 정당하다고 느끼고 죄책감이 없는 행동양식을 보이고 있다.

### 논의

다음 Fig. 1은 가상화폐를 이용한 자금세탁 도구화 과정을 구체적으로 분석하여 범죄진행과정을 스크립트 한 결과이다. 가상화폐를 통한 자금세탁 범죄 진행 스크립트를 통해 몇 가지 공통적으로 나타나는 몇 가지 특징들을 추론해보면 다음과 같다.

첫 번째로 국제적 범죄라고 할 수 있다. 가상 또는 현실에서 이루어지는 수많은 범죄와 그 범죄로부터 얻은 수익금을 가상화폐로 축적하여 가상화폐거래소를 통해 세탁하는 과정으로, 기존의 법 제도에서는 범죄를 인지하는 것이 어렵다. 현재 전 세계 가상화폐를 한 눈에 볼 수 있는 coinmarketcap.com에서 거래되는 화폐는 6000여 개가 넘고 미비하게 거래되는 코인까지 합치면 만개 가까이 되는 숫자이다. 이러한 거래량이 보여주듯이 가상화폐가 전 세계적으로 활발하게 움직이고 있고, 이는 바로 범죄수익금에 대해 은닉할 수 있다는 뜻이기도 하다. 위에서 언급한 바와 같이 범죄수익과 자금세탁 금액은 전 세계

적으로 방대한 양일 것이라 추산된다. 그것은 가상화폐를 통해 수익을 얻는 범죄자들이 익명성을 통해 추적 자체가 안되는 복잡한 구조의 방향으로 확장되어 가고 있기 때문이다. 국내가 아닌 외국의 거래소 등에서 환치기 등의 자금세탁이 이루어지는 것은 훨씬 조직화, 지능화되어가고 있다는 증거이기도 하다.

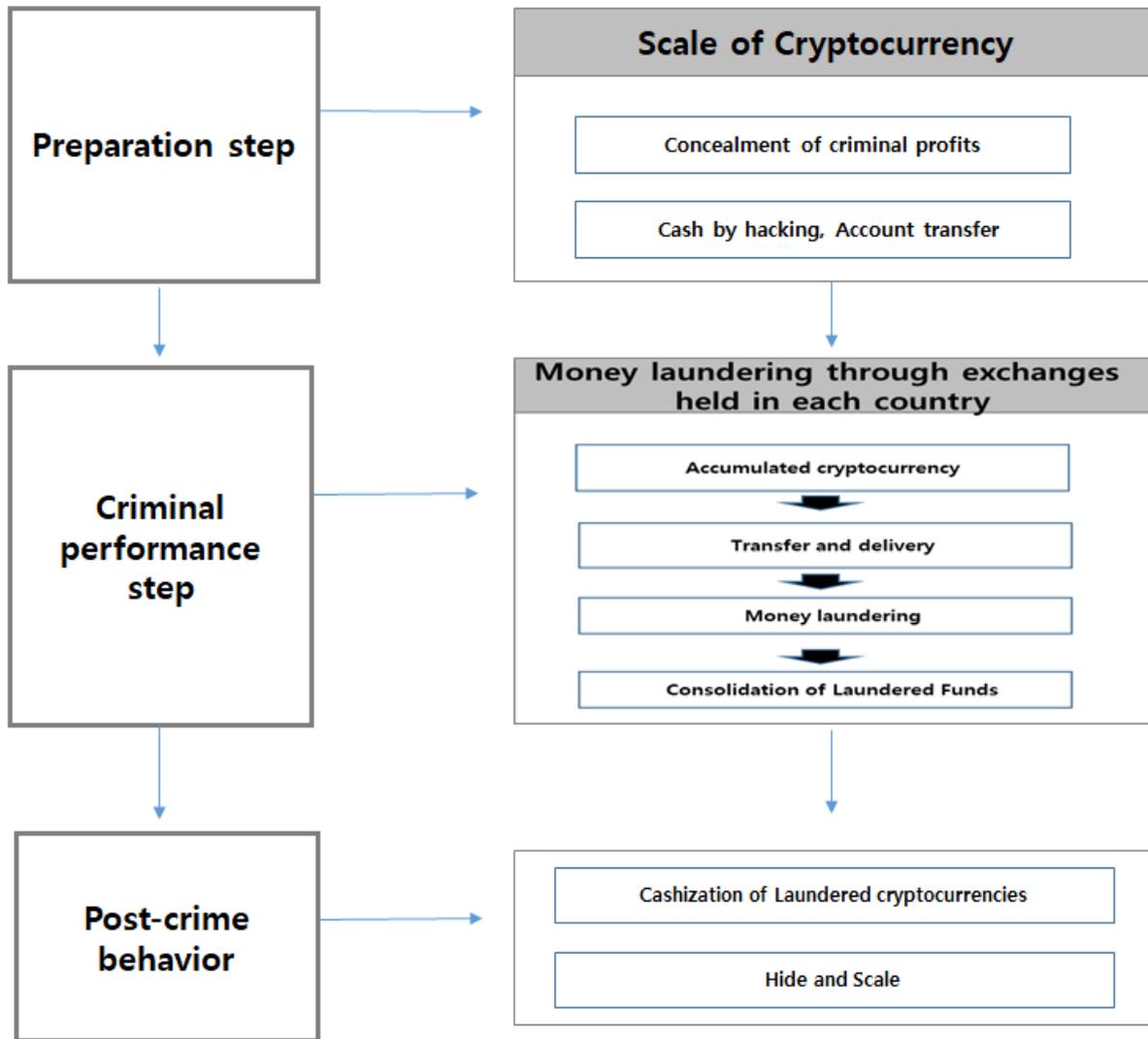


Fig. 1. The money laundering using the virtual currency crime script

둘째, 범죄수익금은 현물화폐가 아닌 가상화폐로 이용한다는 점이다. 마약, 음란물사이트, 도박, 사기 등 여러 가지 오프라인 범죄라도 그 수익을 가상화폐로 받기 때문에 추적이 더 어려울 뿐만 아니라 우리나라의 경우 제대로 된 법제도가 마련되어 있지 않기 때문에 추적해서 몰수 한다해도 실효성 또한 의문이 들 수 밖에 없는 상황이다. 우리나라는 현재 신고하지 않은 거래소만 약 200여 개에 달하고 2021년 9월부터 규제가 들어가 거래소 신고를 한 업체는 겨우 4개소에 불과하다. 가상화폐 시장은 더 커질 것이고 중개자 없는 금융서비스를 이용하는 디파이를 활용하기 때문에 제대로 허가받지 않은 거래소들의 경

우 범죄를 더욱 부추길 수 있다.

셋째, 가상화폐는 이미 범죄수익을 통해 자금세탁을 하여 다시 범죄에 사용되거나 현금화하거나 테러자금 등으로 조달 또는 세금탈루에 쓰여지고 있다. 특히, 블록체인 분석업체 엘립틱에 의하면 범죄수익금 등에 대해 러시아에서 세력을 확장하고 있는 다크넷 시장 히드라(Hydra)를 통해 암호화폐를 현금으로 전환하고 있다고 했다. 엘립틱에 의하면 히드라는 단순히 대량의 암호화폐를 현금으로 바꿔주는 것뿐만 아니라 마약 거래처럼 현금을 지정된 장소에 물어두면 고객이 찾아갈 수 있는 방식을 취하고 있다. 특히 히드라의 마약 거래 시장은 거대한 비밀경제처럼 움직이고 있다. 그렇기때문에 조직적으로 일어나는 자금세탁에 대한 법적 규제와 예방책이 미비한 것이 사실이고, 기술을 법 제도가 따라가지 못하는 실정이다.

## 결론 및 제언

기존 금융서비스에서 자금세탁을 방지를 목적으로 범죄 관련 거래를 감시하기 위해 법으로 규제하고 있지만, 가상화폐 등 장으로 범죄자들은 자금세탁을 시도하고 있다. 가상화폐는 높은 익명성을 유지하기 때문에 범죄자들이 범죄 수익을 쉽게 세탁할 수 있고 기존 현물화폐보다 이용도가 높아진 것이 사실이다. Kang(2018)은 가상화폐는 이용자들의 프라이버시를 지키기 위한 합법적인 목적으로 익명성을 보장하였지만 이러한 특성은 범죄자들이 법집행기관들로부터 자신들의 불법수익을 은닉하고 추적을 힘들게 하는데 오용되었고, Anonymizer, Mixer, Tor, Dark Wallet, Cold, Storage 등과 같은 전자적 수단을 이용하여 거래의 익명성을 더욱 강화하고 추적을 어렵게 하였다고 주장하였다. 가상화폐를 통한 자금세탁에 관한 범죄사례들이 나타나고 있지만, 통계적으로 분석할 만한 자료가 미비하고 법적 제도 또한 제대로 마련되지 않아 그 실체를 파악하기에는 한계가 있다. 2021년 4월 금융위에서는 가상화폐 투자자에 대해서 제도적으로 보호하지 않겠다고 하였으나, 이미 국제청에서는 고액채납자들의 가상화폐를 확보하여 세금징수를 하는 등 제도권 내에서 활용하고 있다고 할 수 있는 상황이다. 이처럼 법 제도가 제대로 마련되지 않고 있는 시점에 9월부터 신고하지 않은 거래소의 가상화폐는 인정하지 않는다면서 6개월의 유예기간을 두었다. 이에 본 연구에서는 선행연구의 부족과 범죄사례의 파악이 쉽지 않은 한계로 심각하게 발생하고 있는 범죄사례들에 대한 분석을 가상화폐를 통한 자금세탁 도구화 과정에 대해 범죄스크립트를 통해 연구하였다.

가상화폐를 통한 자금세탁의 범죄스크립트의 분석결과 첫째, 자금세탁을 하는 가상화폐의 경우 대부분이 범죄수익금이나 해킹을 통해 얻은 것이고, 둘째, 가상화폐를 통해 얻은 범죄수익금은 각국이 보유한 거래소를 통해 반복적으로 거래소를 돌면서 세탁이 되어 현금화되거나 한곳으로 다시 통합하는 형태로 나타난다. 셋째, 세탁된 가상화폐는 현금화하거나 다시 테러자금이나 은닉 또는 축적하는 형태로 나타난다. 넷째, 이러한 경로를 통한 자금세탁은 추적하기가 어려울 뿐만 아니라 범죄사실이 인지조차 안 되는 경우들이 있다. 특히 우리나라의 경우 형사처벌이나 법적인 제도마련이 미비하다. 우리나라는 3월부터 가상화폐 거래소 등 가상자산 사업자에게 자금세탁 방지 의무가 부과되었고, 2021년 9월까지 신고 접수를 하지 않은 상태에서 영업을 계속하면 미신고 사업자로서 처벌을 받게 된다. 특히 가상자산 사업자에 부과되는 자금세탁방지 의무는 고객 확인, 의심 거래보고 등을 해야만 한다. 과연 얼마나 실효성이 있을지 의문이 제기된다. 하지만 우후죽순 생겨난 거래소로 인해 가상화폐 거래소를 규제하고 있지만 범죄수익금으로 발생하는 가상화폐에 대한 제재는 아직 미흡하다. 따라서 금융당국과 수사기관의 상호 정보교류를 통해 자금세탁에 대한 신호를 수집하고 대응할 수 있는 예방적 차원의 방안이 마련되어야 할 것이다.

가상화폐는 빠른 속도로 진화하고 있지만, 자금세탁의 흐름을 조사할 수 있는 기술적 제도가 마련되어 있지 않기 때문에

가상화폐 관련 범죄와 그에 따른 자금세탁이 이루어지는 과정에 빨리 대응할 수 있도록 정책적 보완과 입법이 동시에 마련되어야 할 것이다.

## Acknowledgement

본 논문은 2021년도 세명대학교 교내 학술연구지원에 의해 진행된 연구입니다.

## References

- [1] Baeck, N.J, Ryu, J., Kim, B.J. (2021). “Countermeasures study on money laundering using cryptocurrency for cyber safety.” *The Journal of Humanities and Social Science*, Vol. 12, No. 3, pp. 1399-1414.
- [2] Cornish, D.B. (1993). “Crime as scripts.” Paper presented at the Second Annual Seminar on Environmental Criminology and Crime Analysis, University of Miami, Coral Gables, FL, US. May. pp. 26-28.
- [3] <http://www.coindesk.com/news/articleView.html?idxno=73163>
- [4] <https://www.hankyung.com/economy/article/2021031675656>
- [5] <https://coinmarketcap.com/?page=60>
- [6] Hwang, S.J. (2018). “A legal review on abuse cases of virtual currency and legal responses.” *Korea Academy Industrial Cooperation Society*, Vol. 19, No. 2, pp.585-594.
- [7] Kang, S.Y. (2018). “Virtual currency, money laundering, and corruption - From law enforcement perspective -” *Journal of Digital Forensics*, Vol. 11, No. 1, pp.77-91.
- [8] Kim, H.J. (2020). “A study on criminal policy implication of crypto currency based on block chain technology in the fourth industrial revolution.” *Korean Research Memory*, pp.183-209.
- [9] Lee, Y.S. (2016). “The risk of money laundering and policy implications in virtual currency transactions.” *Korea Institute of Finance*, Vol. 25, No. 38, pp. 10-11.
- [10] Seo, J.Y. (2018). “Study on the countermeasures on the bitcoin.” *Police Science Institute*, Vol. 32, No. 3, pp. 323-354.