J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

자금 세탁 방지를 위한 블록체인 기반 스마트 컨트랙트 메커니즘 설계☆

A Study on the Design of Smart Contracts mechanism based on the Blockchain for anti-money laundering

강 희 정1 김 혜 리1 홍 승 필2*
Heejung Kang Hye Ri Kim Seng-phil Hong

요 약

블록체인은 네트워크 내의 모든 참여자들이 공동으로 소유하고 검증함으로서 데이터의 조작을 방지하고 무결성 및 신뢰성을 보장하는 기술이다. 블록체인은 보안성 및 확장성·투명성을 특징으로 하며 전 세계에서 이용가능하기 때문에 최근 송금을 포함하여 물류·유통, IoT 등 다양한 분야에서 활용되고 있다. 그 중에서도 최근에는 블록체인을 기반으로 하여 다양한 형태의 계약을 체결하고 이행을 자동화할 수 있는 스마트 컨트랙트에 대한 관심이 높아지고 있다. 스마트 컨트랙트를 활용하면 계약 사항을 미리 프로그래밍하여 작성하고, 조건이 충족되면 즉시 시행되기 때문에 디지털 데이터에 대한 신뢰도를 더욱 높일 수 있다. 본 논문에서는 스마트 컨트랙트 설계에 관한 연구를 진행하면서 최근 이슈가 되고 있는 가상화폐의 불법적 자금 악용 등의 문제를 해결하는 방안으로써, 스마트 컨트랙트 설계 방안에 대한 연구를 진행하였다. 이를 통해 고객확인(KYC:Know Your Customer)과 자금세탁방지 과정을 스마트 컨트랙트를 활용해 적용해 보았으며, 자금세탁방지의 가능성을 확인 및 ASM(AML SmartContract mechanism) 설계 방안을 제시해보고자 한다.

☞ 주제어 : 블록체인, 스마트 컨트랙트, 자금세탁방지, 보안

ABSTRACT

The Blockchain is a technique that prevents data from being manipulated and guarantees the integrity and reliability of the data by all participants in the network jointly owning and validating the data. Since the Blockchain characterized by security, scalability and transparency, it is used in a variety of fields including logistics, distribution, IoT and healthcare, including remittance. In particular, there is a growing interest in smart contract that can create different forms of contracts and automate implementation based on Blockchain. Smart Contract can be used to pre-programme contracts and are implemented immediately when conditions are met. As a result, digital data can be more reliable. In this paper, we are conducting a study on the smart contract design as a way to solve such problems as illegal misuse of funds on virtual currency, which has become an issue recently. Through this process, we applied the customer identification and money laundering prevention process using smart contract, and then check the possibility of preventing money laundering and propose the ASM (AML SmartContract Mechant) design.

☞ keyword : Blockchain, Smart Contract, AML, Security

1. 서 론

블록체인은 다수의 참여자가 데이터를 공동으로 소유하여 기존의 신뢰할 수 있는 중간자(TTP·Trusted Third Party) 없이도 신뢰성을 보장한다.[1] 블록체인 기술 활용 시, 수수료 및 유지비용을 절감 할 수 있으며 높은 보안성과 같은 특징으로 가상화폐뿐만 아니라 많은 분야에서 활용되고 있으며, 특히 최근에는 블록체인 기술을 활용한 스마트 컨트랙트에 대한 관심이 높아지고 있다. 스마트 컨트랙트는 블록체인에 계약을 프로그래밍하여 실행 할

1 Department of Computer Science, Sungshin Women's University, Seoul, 02844, Korea.
2 Department of Convergence Security Engineering, Sungshin Women's University, Seoul, 02844, Korea.
* Corresponding author (philhong@sungshin.ac.kr)
[Received 16 March 2018, Reviewed 23 March 2018(R2 5 June 2018, R3 23 July 2018), Accepted 6 September 2018]
☆ This work was supported by the Sungshin University Research Grant of 2017.
☆ 본 논문은 2017년도 한국인터넷정보학회 추계학술발표대회 우수 논문 추천에 따라 확장 및 수정된 논문임.

수 있게 함으로써 제 3자의 개입 없이도 강제력 있는 계약의 이행을 담보하여 신뢰도를 높이고 계약과 관련된 다른 거래 비용을 줄일 수 있다. 그렇기 때문에 금융거래, 부동산 계약 및 공증 등 다양한 형태의 계약에 스마트 컨트랙트를 활용하고자 하는 시도가 증가하는 추세이다.

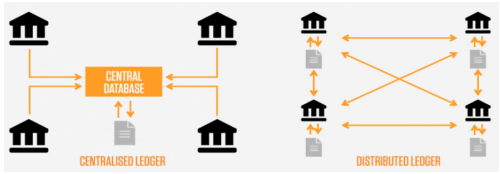
본 논문에서는 최근 가상화폐의 익명성을 악용하여 불법적인 자금 세탁 및 테러 자금 조달 같은 신종 범죄에 가상화폐가 이용되는 문제에 대한 해결 방안으로 스마트 컨트랙트를 활용해 보고자 연구를 진행하였다. 가상화폐는 단일국가가 아닌 전 세계에서 이용 가능하기 때문에 해외로 송금이 가능한데 이는 현재 외국환 거래법등 현 법령에 위반될 뿐만 아니라 이를 통한 환치기 및 자금세탁을 하는 사례가 계속적으로 증가하는 추세를 보여 시중 은행은 가상화폐를 이용한 해외 송금에 대해 모니터링 강화 및 차단하고 있다.[2, 3]하지만 무조건적으로 송금을 막을 수 없으며 가상화폐는 기존 해외송금과는 완전히 다른 망을 이용하기 때문에 모니터링에는 한계점이 존재한다. 또한, 블록체인은 다수의 노드들이 네트워크를 유지하고 있는 형태로 중앙의 제어하는 사람이 없기 때문에 통제가 어렵고 익명성의 특징을 갖기 때문에 자금 추적에 어려움이 있다.[4]

그리하여 본 논문에서는 가상화폐의 이용이 증가함에 따라 가상화폐가 불법적 용도로 악용되는 문제에 대한 해결 방안으로써 스마트 컨트랙트를 활용해 보고자 하였고, 그 적용 방안을 제시해보고자 한다.

2. 관련 연구

2.1 블록체인

블록체인은 신뢰할 수 있는 제3의 기관을 두어 신뢰성을 보장하던 기존 중앙 집중형 시스템에서 벗어나 다수의 참여자에 의해 신뢰성을 보장함으로서 중간의 불필요한 수수료 절감 및 투명성을 특징으로 한다. 블록체인은 정보를 다수가 공동 소유하는 형태로 이루어져있기 때문에 일부 시스템의 성능저하 및 오류가 전체 시스템에 큰 영향을 주지 않아 기존 시스템보다 안정성이 높다. 또한, 데이터 조작 및 해킹을 하려면 엄청난 컴퓨팅 파워가 필요하기 때문에 외부의 악의적 공격이 어려워 기존의 중앙 집중형 시스템 보다 보안성이 높다. 그림 1은 기존 중앙집중형 시스템과 블록체인 방식을 비교한 그림이다.[5]



(그림 1) 중앙집중형 시스템과 블록체인 방식 비교
(Figure 1) Comparison of Centralized Systems and Blockchain

퍼블릭 블록체인에서는 모든 사람이 네트워크에 참여할 수 있으며 실제 사용자 정보와 시스템 상의 사용자 정보의 연관성이 없기 때문에 익명성을 특징으로 한다.[6] 이러한 특징은 자금 추적 및 악의적 노드의 구별을 어렵게 하기 때문에 기존 서비스에 적용하기에 어려움이 있었다. 이에따라 허가받은 사용자만 접근가능하게 하는 컨소시엄 블록체인과 프라이빗 블록체인의 필요성이 대두되었다. 표 1은 블록체인 유형에 따른 특징을 보여주는 표이다.[7]

(표 1) 블록체인 유형 별 특징
(Table 1) Characteristics by Blockchain Type

	퍼블릭 블록체인	컨소시엄 블록체인	프라이빗 블록체인
관리 주체	모든 거래 참여자	컨소시엄에 소속되어 있는 참여자	한 중앙기관이 모든 권한 보유
데이터 접근	누구나	허가받은 사용자만	허가받은 사용자만
식별성	익명성	식별 가능	식별 가능
활용 사례	비트코인	R3 CEV	나스닥의 링크(Linq)

2.2 스마트 컨트랙트

스마트 컨트랙트는 Nick Szabo[8]가 최초로 제안한 개념으로써 조건에 따라 계약의 내용을 자동으로 실행하는 것을 의미하며, 블록체인 기반의 스마트 컨트랙트는 합의 프로토콜에 의해 강제적으로 실행되는 프로그램을 의미한다[9]. 스마트 컨트랙트는 비트코인 블록체인의 스크립트 언어[10]에서의 활용을 시작으로 2013년 비탈릭 부테린이 블록체인 기술을 이용하여 대금결제 및 송금 등 금융거래 뿐만 아니라 다양한 종류의 계약을 처리할 수 있도록 기능을 확장한 이더리움[11]을 발표하며 널리 확산

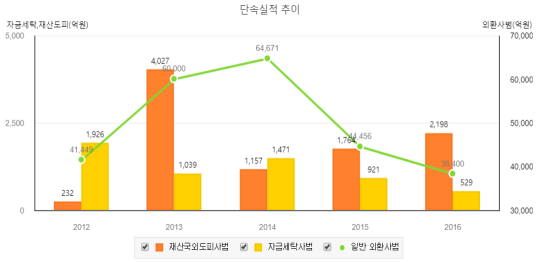
되었다.이더리움 기반에서는 개발자가 직접 계약 조건을 코딩할 수 있기 때문에 다양한 형태의 계약을 이더리움 플랫폼을 활용하여 구현할 수 있다[11]. 이러한 스마트 컨트랙트의 발전으로 이더리움은 가상화폐이면서도 저작권, 헬스 케어, IoT 등 다양한 서비스를 개발 및 구동할 수 있는 플랫폼으로 확장되었다.

스마트 컨트랙트는 제3자의 개입 없이도 신뢰할 수 있는 계약의 이행을 제공하고, 계약과 관련된 다른 거래 비용을 줄이는 것을 목표로 한다. 실제 사람이 계약서대로 수행하는 데에는 예기치 못한 일들이 생길 수 있는 반면, 스마트 컨트랙트를 사용하면 명확한 계약 사항을 프로그래밍 하여 계약을 작성하기 때문에 조건에 충족되면 즉시 계약을 시행하여 복잡한 프로세스를 훨씬 간소화 하고 빠르게 처리할 수 있다.

2.3 자금세탁방지 현황

2.3.1 자금세탁 규모 추이

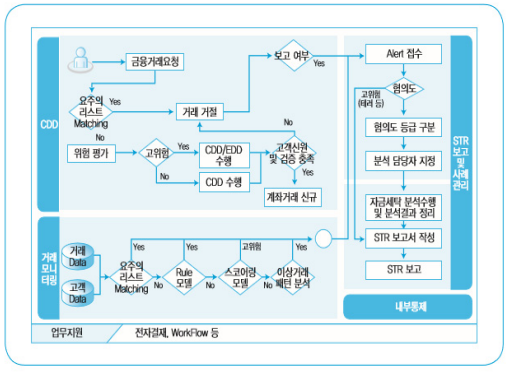
세계경제 환경의 변화에 따라 자금의 흐름이 과거에 비해 그 규모가 훨씬 커졌을 뿐만 아니라 횟수 또한 크게 증가하고 있다. 이에 따라, 불법적인 자금을 감시하기 위한 필요성이 제시되었고 지속적으로 단속해왔다. 자금세탁은 큰 규모의 자금세탁이 적발되지 않아 2014년 이후로 꾸준히 감소하는 추세[12]를 보이고 있으나 이는 가상화폐를 통한 자금세탁은 포함하지 않는 지표이다. 최근 가상화폐를 통한 자금세탁 사례의 횟수가 증가하고 있으며 방법도 다양해지고 있다.[13]



(그림 2) 외환사범 단속 현황[12]
(Figure 2) Status of foreign currency violation

2.3.2 자금세탁방지 프로세스

일반적으로는 자금세탁방지 시스템은 크게 4가지로 구성되어있다, 자금세탁방지 시스템은 고객확인의무 수행을 원활히 지원하고 통제하기 위한 CDD 시스템, 자금세탁 행위로 의심되는 거래를 추출하는 거래모니터링 시스템, 의심거래보고 및 고액현금거래보고 시스템, 효과적인 운영을 모니터링 하는 내부통제 시스템으로 구성되어 있으며 그 흐름은 그림 3과 같다. 특히 거래 모니터링 시스템은 거래를 이상거래를 분류하는 것으로 프로세스에서 중요한 역할을 한다, 모니터링 분석기법은 아래 표 2[14]와 같다.



(그림 3) 자금세탁방지 업무/시스템 흐름도[14]
(Figure 3) Financial Clearing System Flow Diagram

(표 2) 거래모니터링 분석기법[14]
(Table 2) Transaction Monitoring Analysis Method

	주요내용
룰 모델 (Rules-Based Technology)	• 일정금액 이상, 일정 기간 분할거래 횟수와 같이 특정 거래 또는 행위를 기반으로 의심거래 추출 • 금융거래 조건 및 환경등이 변함에 따라 지속적인 업데이트
이상거래 패턴분석 (Outlier Detection)	• 나이, 직업 등 고객의 성격 및 특성에 따라 Peer 그룹을 분류한 후 그룹별 Profile 생성하고, 이후 거래 발생 시 분석대상 고객과 Peer 그룹 Profile 비교하여 이상거래 탐지 • 거래패턴 인식을 통해 알려지거나 또는 알려지지 않은 이상거래 탐지 가능
스코어링 모델 (Scoring Technology)	거래, 고객, 국가 등 자금세탁 리스크 요인을 고려하여 스코어링을 수행하고 스코어링 결과에 따라 위험 파악
Watch List 필터링 (Watch List Filtering)	금융기관이 고객을 대상으로 고객의 이름과 테러리스트 & 범죄자 및 이상거래고객 명단을 비교 분석

2.3.3 가상화폐를 통한 자금세탁문제

자금세탁 문제는 익명성을 특징으로 하는 가상화폐 시장이 활성화 되면서 더욱 더 대두되었다. 정부는 탈세 등 조세관련 정보 및 불법 재산 등 범죄와 관련된 정보를 수집하기 위해 가상화폐 전담부서를 설립[15]하여 가상화폐를 통한 자금세탁에 대한 감시를 강화하였으며 자금세탁방지 가이드라인을 발표하여 2018.01.30.일부터 시행을 발표했다. 발표된 자금세탁과 관련된 대부분의 법률은 은행에서 가상화폐 사이에 입금되는 자금을 감시하는 형태로 이루어져 있기 때문에 다수의 은행과 최근 급격히 증가하고 있는 다수의 거래소를 감시하는 것에는 어려움이 있다. 표 3은 가상화폐 자금세탁방지 가이드라인의 주요내용[16]을 정리한 표이다.

(표 3) 가상화폐 자금세탁 방지 가이드라인[16]
(Table 3) Guidelines for the Prevention of Washing of Virtual Money Funds

	주요내용
고객확인 강화	금융회사등은 취급업소를 자금세탁등의 위험이 높은 고객으로 고려하여 생년월일, 주소, 연락처 등을 포함한 신원사항 확인 및 입출금계정서비스 이용여부 및 이용계획등을 확인
고객에 대한 지속적 확인	금융회사등은 취급업소를 자금세탁등의 위험이 높은 고객으로 고려하여 6개월 이하의 주기마다 지속적으로 확인, 취급업소가 실명확인 입출금계정서비스를 이용하지 않는 등 특별한 주의를 요하는 경우 3개월 이하의 주기마다 지속적으로 확인
주요 의심거래 유형	금융회사등은 취급업소의 금융거래, 금융회사등의 고객과 취급업소 간 금융거래가 1일 금융거래 금액이 1천만원 이상이거나 7일 동안 합산한 금융거래 금액이 2천만원 이상을 거래하는 경우 등과 같을 경우 금융정보분석원에 그 사실을 보고
거래 모니터링 강화	금융회사등은 가상통화와 관련한 거래에 금융거래에 대해 기존 의심거래보고기준(Rule)에 근거한 모니터링 강화 및 새로운 의심거래보고 기준 설립
내부통제 강화	금융회사는 자금세탁 방지를 위한 전사적 내부통제가 가능하도록 조치하고, 이사회・경영진 및 보고책임자에게 다음과 각 호의 역할과 책임을 부여하고 준수
위험의 평가 및 관리	금융회사는 가상통화와 관련한 금융거래에 대해 자금 세탁과 같은 위험을 평가할 수 있는 절차를 수립하고 운영 특히, 가상통화와 관련된 금융거래는 상품과 서비스에 대한 위험을 평가 시, 위험이 높은 상품 및 서비스로 취급

하지만 위 가이드라인에서도 볼 수 있듯이 블록체인 기반 가상화폐의 송금 시 생기는 문제를 해결하기 위한 정부 정책과 관련 법률은 대부분 은행에서 가상화폐 사이에 입금되는 자금을 감시하는 형태로 이루어져 있다. 이러한 형태의 자금은 감사히는 형태는 한계점이 존재한다.

첫째, 거래소들은 독자적인 시스템을 구축해야 하는데 현재 시스템이 정형화되어 있지 않기 때문에 많은 오류 및 에러를 야기할 수 있다. 이러한 오류 및 에러는 자금세탁방지에 대한 신뢰성을 낮추기 때문에 신뢰성 있는 시스템을 위해서는 정형화되어 자동적으로 실행되는 시스템이 필요하다.

둘째, 일일이 거래소들에 입금되는 자금의 출처를 추적하는 것은 매우 어렵다. 최근 생겨난 많은 거래소에 자금을 일일이 감시한다는 것은 비용 및 시간소모가 많이 소요된다.

셋째, 입금 후 사용처가 불분명하다. 자금세탁방지란 자금이 어디에 쓰이는지를 알기 위함인데 은행과 거래소를 관리하면 이후 거래소에서 바꾼 가상화폐의 사용처를 파악 할 수 없다.

셋째, 개별적 인증 및 프로세스 적용의 어려움이 있다. 사용자는 각각의 거래소마다 다시 인증을 거쳐야하는 불편함을 겪으며 거래소는 프로세스 적용에 독자적으로 개발을 해야 한다는 어려움이 있다. 현재는 거래소가 각각마다 사용자 인증 프로세스를 거쳐 자금세탁방지 프로세스를 적용해야한다. 이는 각각의 거래소 마다 구현이 필요한 부분이므로 많은 비용 및 시간이 소모된다.

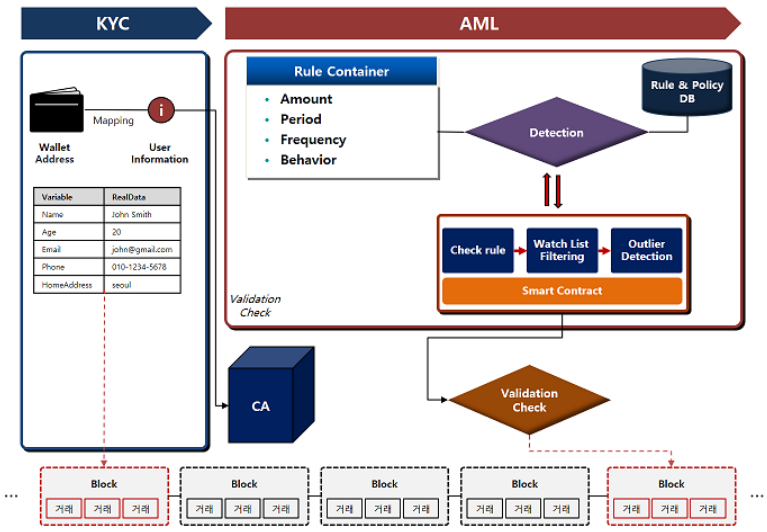
이러한 한계점 때문에 가상화폐에서 자금세탁을 방지를 하는데 있어 많은 어려움을 겪고 있다.

3. 자금세탁 방지를 위한 스마트 컨트랙트 메커니즘 설계

익명성을 특징으로 하는 블록체인 기반 가상화폐의 송금 시 생기는 문제를 해결하기 위한 정부 정책은 앞서 언급했듯이 한계점을 갖는다. 가상화폐는 기존 해외송금과는 완전히 다른 망을 이용하기 때문에 기존 제시된 방식으로의 해결하는 것에는 한계점이 존재한다.

따라서 본 논문에서는 스마트 컨트랙트를 활용하여 자금세탁 문제를 해결할 수 있는 방안에 대한 연구를 진행하여 사용자와 거래소의 편리성을 확보하며 조금 더 신뢰성 있는 자금세탁 메커니즘을 구현해보고자 하였다.

스마트 컨트랙트를 활용하여 자금세탁 방지를 할 경우



(그림 4) 자금세탁 방지를 위한 스마트 컨트랙트 메커니즘
(Figure 4) AML Smart Contract Mechanism(ASM)

기존 은행에서 실행하고 있는 자금세탁방지와 비교하여 많은 비용을 절감 할 수 있으며, 모든 정보가 투명하게 공개되므로 사용자가 많아질수록 신뢰성이 증대하게 된다. 또한, 스마트 컨트랙트는 한 번 구축하면 모든 사용자가 사용 할 수 있으며 정형화된 프로세스를 제공하기 때문에 보다 오류 및 에러의 가능성을 줄일 수 있으며 하나의 스마트 컨트랙트만 관리하면 되므로 각각의 거래소에서 유지・보수하는 것 보다 효율적이다. 이렇기 때문에 기존 방법보다 스마트 컨트랙트를 활용하여 자금세탁 방지를 할 경우 많은 이점을 갖는다.

그림 4는 본 논문에서 제시하고자 하는 자금 세탁 방지를 위한 스마트 컨트랙트 메커니즘이다. 크게 사용자를 인증하는 KYC기능 부분과 자금세탁 방지 기능을 구현한 AML기능 부분으로 구성되어 있으며 전체적인 프로세스는 그림 5와 같다.

① KYC 등록

고객확인(KYC: Know Your Customer)을 하기 위해서는 KYC 등록 과정을 거쳐야하는데 이는 최초에 사용자가 자신의 정보를 입력해 자신을 등록하여 고객을 식별할 수 있도록 하는 기능이다.

이 때, 사용자가 입력하는 기본정보와 개인정보 및 식별정보를 분리하여 개인정보 및 식별정보를 입력한 사용자는 동의를 해야만 서비스를 이용할 수 있다.

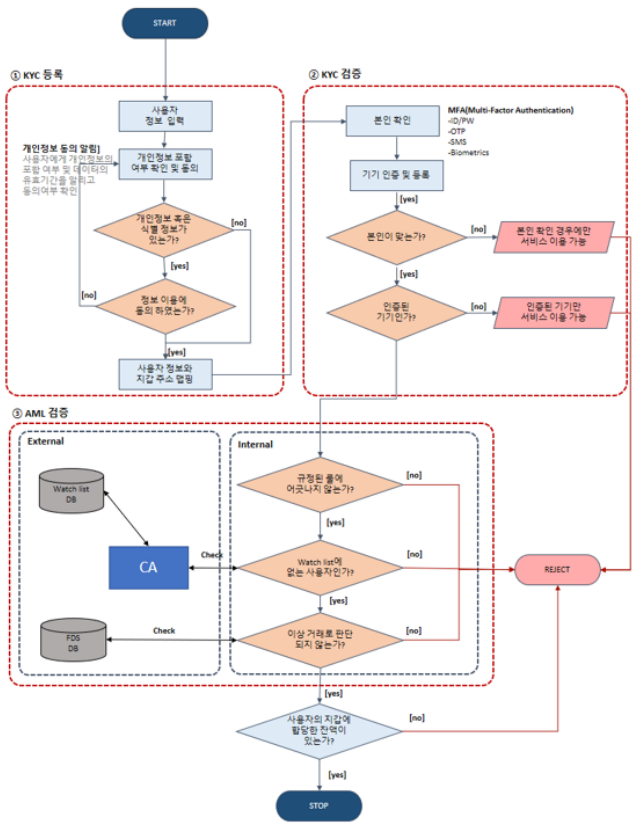
② KYC 검증

사용자는 본인이 등록한 정보가 정말 자신이 맞는지에 대한 V&V(Verification & Validation)과정을 거쳐야 한다. 특히 금융관련 거래에서는 등록한 사용자가 정말 본인인지 확인하는 과정이 중요하기 때문에 사용자는 ID/PW, OTP, SMS, 지문 및 홍채와 같은 생체인증 중 최소 두 개 이상의 본인 인증 과정을 거쳐야하는 MFA(Multi-Factor Authentication)을 통해 자신의 신원을 확인받아야 한다.

또한, 더 높은 보안성을 위해 사용자가 등록한 기기에서만 서비스를 이용할 수 있도록 기기 등록과 인증 과정을 거친다.

③ AML 검증

KYC과정을 마친 사용자는 서비스 이용 시 자금세탁이 의심되지 않는지 AML 검증 과정을 거쳐야한다. AML 과정은 크게 External과 Internal로 나눠진다. Internal 과정에서는 정해진 룰에 어긋나지 않은지 Compliance 점검 과정을 거치고 Watch list에 있는 부당한사용자인지 아닌지 여부를 체크한다. 또한 너무 많은 금액을 보내지 않는지 이상거래 여부를 판단하게 되는데 이러한 과정에서 Watchlist 및 이상거래 판단 여부와 같은 것은 기존에 많



(그림 5) 자금세탁 방지를 위한 전체 프로세스
(Figure 5) Overall process for anti-money laundering

은 사례들이 있기 때문에 외부의 기관과 협력하여 기존에 평가 여부에 이가 해당되는지 아닌지 여부를 판단한다. 이러한 과정을 거쳐 최종적으로 정상적인 거래로 판단되면 사용자의 잔액이 타당한지 Balance Check 후 타당하면 서비스 이용을 완료 할 수 있다.

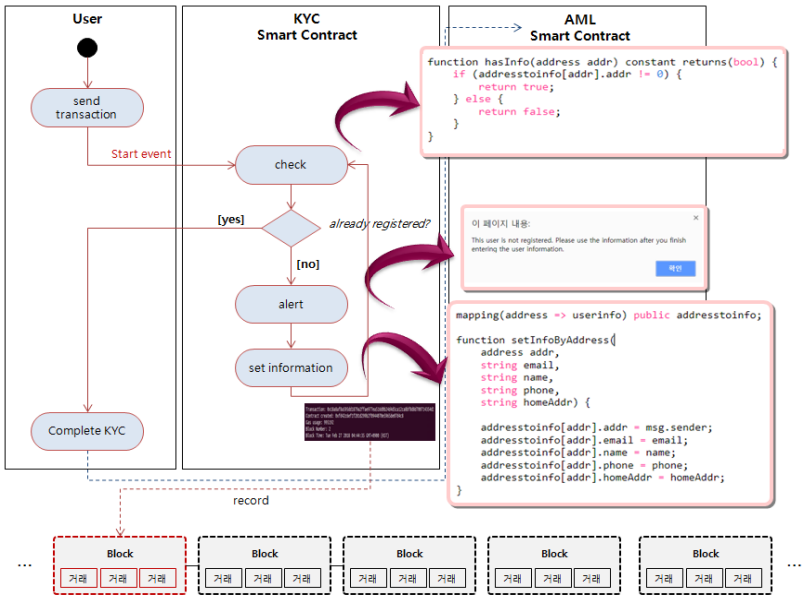
3.1 사용자 인증(KYC) 기능

자금세탁과 같은 문제해결을 위해서는 사용자에 대한 명확한 판별이 이루어 져야 한다. 사용자가 누구이며 어떠한 사람인지에 대한 확인이 이루어져야 자금세탁 여부를 판단할 수 있기 때문에 사용자는 고객확인(KYC) 과정을 거치도록 하였다.

KYC란 금융회사에서 제공하는 서비스가 자금세탁과 같은 불법행위에 이용되지 않도록 고객의 신원 및 거래 목적 등을 확인하는 것을 의미한다. 보통 인증 수단으로는 핀번호, SMS인증, 여권번호, 여권 셀카 사진, 은행 계좌, 우편 인증 등을 적용하며 최근 해킹과 같은 이슈 때문에 많은 거래소에서 KYC를 도입하려 하고 있다.

하지만 일일이 고객의 정보를 확인해야하며 고객확인 정보가 공유되지 않기 때문에 거래소마다 고객확인 절차에 대한 비용을 각각 지불해야한다는 단점이 있다. 그래서 본 논문에서는 MFA 인증을 통한 KYC 절차를 거쳐 사용자를 검증하고 스마트 컨트랙트로 관리하여 다른 서비스에도 재사용 가능하도록 설계 하였다.

앞서 언급했듯이 사용자가 누구인지 파악이 가능하여야 자금세탁 여부를 판단 할 수 있기 때문에 사용자은 서비스 이용 전에 고객 확인 과정을 거쳐야 하며, 고객확인 과정을 거치지 않은 사용자는 서비스 이용에 제한을 갖게 설계해야한다. 사용자가 송금을 원하면 우선적으로 스



(그림 6) KYC 기능 설계
(Figure 6) Design of KYC

마트 컨트랙트에서 고객 확인 여부를 확인 한다. 확인 되지 않은 사용자가 서비스를 이용하려고 하면 사용자에게 이용이 제한되었다는 알림을 주도록 설계하였다. 따라서 사용자는 서비스를 이용하기 전에 성명, 핸드폰번호, 핸드폰 번호와 같은 식별 가능한 사용자 정보를 입력 [18, 19]하여 등록을 해야하며 사용자가 거짓으로 정보를 등록할 경우에 대비하여 외부 인증기관을 통해 휴대폰 인증과 같은 인증이 확인된 사용자만 사용자로 등록된다. 이렇게 입력된 사용자 정보는 지갑 주소와 맵핑되어 관리되도록 설계하였다.

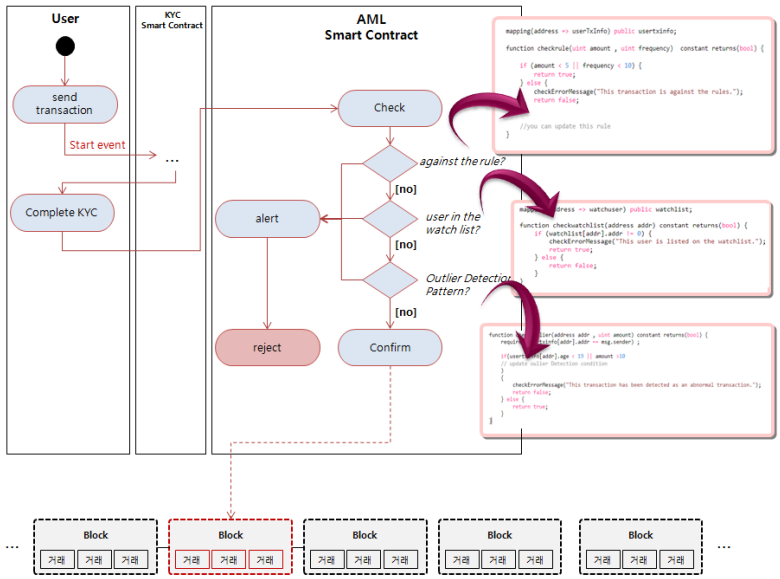
이러한 스마트 컨트랙트를 통한 KYC과정은 재사용 가능하기 때문에 각 서비스마다 지불해야했던 인증과정 시 드는 비용을 대폭 감소시킬 수 있으며 사용자도 각 서비스마다 다시 인증과정을 거치지 않는다는 점에서 가용성을 높여준다. 전체적인 KYC 기능 설계는 아래 그림 6과 같다.

3.2 자금세탁방지(AML) 기능

가상화폐는 기존 자금의 경로를 추적하고 악용되는 것을 방지하던 메커니즘의 도입이 불가능하다. 가상화폐의 등장과 더불어 많은 국가에서 자금세탁으로 문제를 겪고 있으며, 이를 해결하고자 하는 노력을 하고 있다. 최근 일본의 경우, 일본 금융청이 암호화폐 거래소 6곳에 대하여 자금세탁방지 개선을 요구했다.[17] 하지만 늘어나는 사용자에 대해 지속적으로 자금세탁을 모니터링 한다는 것은 매우 어려우며 KYC와 마찬가지로 각 거래소는 자금세탁에 대한 비용을 각각 지불해야한다. 그래서 본 논문에서는 스마트 컨트랙트를 통해 자금세탁 여부를 자동적으로 판단하며 이 결과를 투명하게 공개하여 비리가 일어 날 수 없도록 하였다.

앞서 고객확인이 완료된 사용자는 서비스를 이용 할 수 있으며 이 때, 정해진 자금세탁 룰에 어긋나는지 확인하는 과정이 필요하다. 자금세탁방지 기능을 하는 스마트 컨트랙트에서는 최대금액 이상을 송금하는지, 일정기간 동안 분할거래를 몇 번 시도했는지 횟수 등을 체크하여 정해진 룰에 어긋나거나 이상이 있는지 여부를 체크한다.

또한 Watch List 필터링을 통해 현재 거래가 불가능한 사용자인지 주의해야할 사용자인지와 같은 여부를 확인한다. Watch List는 추후 사용자의 평판에 따라 업데이트 될 수 있다.[17] 또한 나이, 직업 등 고객의 성격에 어긋나는 거래인지 일반적인 거래 패턴과 다른지와 같은 이상 거래 패턴 여부를 판단하고 정상적인 거래라고 판단될 경우 최종적으로 서비스 이용이 가능하다. 이를 바탕으로 제시하는 AML 기능 설계는 아래 그림 7과 같다.



(그림 7) AML 기능 설계
(Figure 7) Design of AML

본 논문에서는 모든 자금세탁방지 기능을 구현하는 것은 어렵기 때문에 최소한의 조건으로만 가능성 여부를 확인할 수 있도록 설계하였다. 사용자가 송금 서비스 이용 시, 스마트 컨트랙트에서 일정 금액 이상이 송금되는지, 사용자가 Watch List에 있는지, 나이에 맞지 않게 너무 많은 돈을 송금하지 않는지 여부 등을 확인하게 되며 조건에 맞을 경우 승인 되지만 그렇지 않을 경우에는 부당한 거래로 간주되어 사용자에게 알람 및 승인이 거절된다.

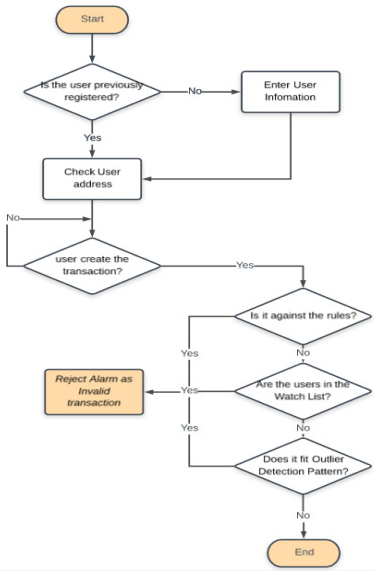
4. 사례 적용

앞서 제시한 설계를 바탕으로 거래소에서 송금 하는 경우에 대해 사례를 적용해보았다, 사례적용 환경은 아래 표 4와 같다.

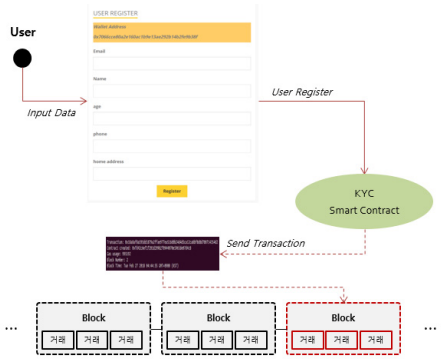
(표 4) 사례적용 환경
(Table 4) Environment Applied Case

구분		내용
웹	OS	Ubuntu 16.04
	Server	Apache tomcat 8.0.42
	Language	NodeJS
블록체인	Client	testRPC
	Solidity	^0.4.0

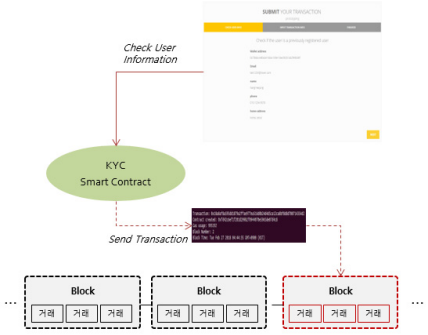
사례 적용 프로세스는 크게 사용자 인증과 자금세탁 방지로 나눌 수 있으며, 전체적인 프로세스는 그림 8과 같다.



(그림 8) 자금세탁 방지를 위한 스마트 컨트랙트 프로세스
(Figure 8) Smart Contact Process to Prevent Financial Wash

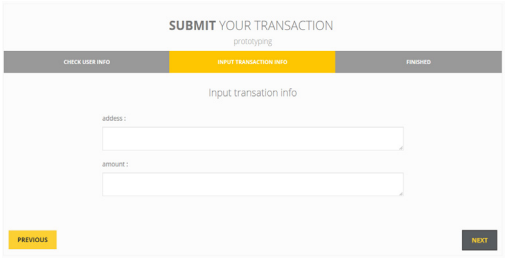


(그림 9) 사용자 등록
(Figure 9) User registration

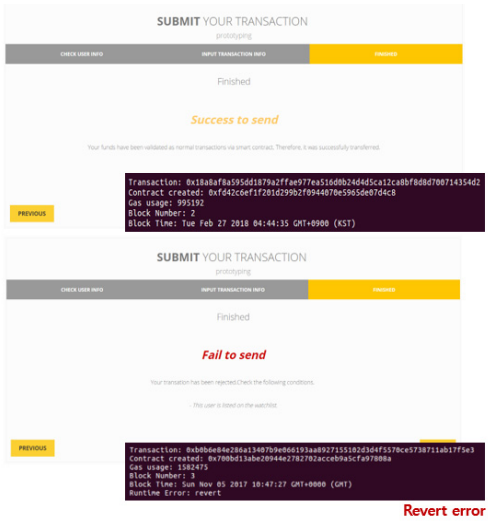


(그림 10) 사용자 정보 확인
(Figure 10) User information check

사용자 등록 페이지에서는 사용자는 이름, 핸드폰 번호, 이메일등 식별에 필요한 정보를 입력해야 하며 고객 확인 정보는 스마트 컨트랙트에서 관리된다. 그림 9과 그림 10는 사용자 등록페이지 및 등록된 사용자의 정보를 확인하는 페이지이다.



(그림 11) 송금 정보 입력
(Figure 11) Transaction information Enter



(그림 12) 송금 성공 및 실패 화면
(Figure 12) Transaction success and failure screen

그림 11은 사용자가 송금정보를 입력하는 화면이고 그림 12의 성공부분은 문제없이 스마트 컨트랙트의 자금세탁 방지 프로세스를 통과했을 때이며 실패부분은 주어진 조건에 하나라도 부합하지 않을 때에 대한 화면본이다.

5. 결론 및 향후연구

블록체인은 4차 산업혁명의 핵심기술로 평가받으며 다양한 분야에서 활용되고 있다. 특히 최근에는 블록체인 기반의 스마트 컨트랙트를 활용하고자 다양한 분야에서 시도하고 있는데, 본 연구에서는 스마트 컨트랙트에 대한 설계 방안의 연구로써, 이를 활용한 가상화폐 악용 문제를 해결해 보고자 하였다. 이는 가상화폐 이용 증가에 따라 증가하는 가상화폐의 악용을 막을 수 있다는 것에 의미가 있다고 사료된다. 향후 연구에서는 자금세탁방지를 위한 고도화된 스마트 컨트랙트의 개발이 필요하며 실증을 위해 다양한 시나리오 개발 및 정량화 된 테스트를 진행할 예정이다.

참고문헌(Reference)

[1] DongSeop Kim, “The Present Status and Implications of distributed ledger technology and Digital Currency”, KFTC (Korea Financial Telecommunications &

Clearings Institute), 2016.

[2] HyeonCheol Park, “Introduction of a small overseas Remittance and Changes in the Foreign Remittance Market”, report of A financial letter, 2017.

[3] YoonSeok Lee, “Money Laundry Risk and Policy Implications in Virtual Money”, KIF Research, vol 25, 38, 2016.

[4] JungHo Seo, Daeki Lee, Gonpil Choi, “Financial Block Chain Utilization and Policy Issues”, KIF Research, 2017.

[5] Stephen Harrison, Capco: What Blockchain Isn’t?, http://www.risktech-forum.com/opinion/what-blockchain-isnt, 2016.

[6] Hanjae Jeong, “Design and Implementation of Blockchain Based Digital IdentityManagement System”, Soongsil Univ, 2017.

[7] YoungHee Seo, Ji-Hwan Song, Young-Il Gong, “Blockchain Technology: Prospect and Implications in Perspective of Industry and Society”, SPRi, vol2017-004, 2017.

[8] N. Szabo. Smart Contracts. http://szabo.best.vwh.net/smart.contracts.html, 1994.

[9] Byung-hee Kim, “Modeling Smart Contract by Timed Automata”, 44-46, Korea Univ, 2016.

[10] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008.

[11] V. Buterin, “Ethereum White Paper : A Next Generation Smart Contract & Decentralized Application Platform”, Ethereum.org, 2014.

[12] Korea Customs Service, “Status of foreign currency violation”, 2017. http://www.index.go.kr/.

[13] Korea Customs Service, “Find out about illegal foreign currency transactions, such as new currency transactions using virtual currencies”, 2018. http://www.customs.go.kr/kcshome/.

[14] Financial Services Commission, Price waterhouse Coopers, “Experiences and methodology of Korea’s anti-money laundering system deployment and development”, KDI, 2013.

[15] Financial News, “Establishment of an organization dedicated to the recovery of profits from a virtual monetary crime”, 2018. http://www.fnnews.com/news/201802121255405396.

[16] Financial Services Commission, “AML guidelines for virtual currencies”, Financial Services Commission, 2018.

[17] Coindesk, “Japan, Cryptographic Exchange 6 orders to improve anti-money laundering (AML)”, 2018, https://www.coindeskkorea.com

[17] Kyoungsoo Bok, Jinkyung Yun, Yeonwoo Kim, Jongtae Lim and Jaesoo Yoo, ″User Reputation computation Method Based on Implicit Ratings on Social Media,″ KSII Transactions on Internet and Information Systems, vol. 11, no. 3, pp. 1570-1594, 2017. http://dx.doi.org/10.3837/tiis.2017.03.018

[18] Chun-Ta Li, Cheng-Chi Lee, Chi-Yao Weng and Chun-I Fan, ″An Extended Multi-Server-Based User Authentication and Key Agreement Scheme with User Anonymity,″ KSII Transactions on Internet and Information Systems, vol. 7, no. 1, pp. 119-131, 2013. http://dx.doi.org/10.3837/tiis.2013.01.008

[19] Yanrong Lu, Lixiang Li, Haipeng Peng and Yixian Yang, ″Robust ID based mutual authentication and key agreement scheme preserving user anonymity in mobile networks,″ KSII Transactions on Internet and Information Systems, vol. 10, no. 3, pp. 1273-1288, 2016. http://dx.doi.org/10.3837/tiis.2016.03.018.

[20] L. S. Sankar, M. Sindhu and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications”, 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 6-7 January, 2017.

[21] SeungHwa Chung, “ Legal Issues for the Introduction of Distributed Ledger Based on Blockchain Technology-Focused On the Financial Industry”, Korea Financial Law Association, Vol.13 No.2, 2016.

◐ 저 자 소 개 -

강 희 정(Heejung Kang)
2013년 성신여대 IT학부(공학사)
2017년~현재 성신여대 대학원 컴퓨터공학과(이학석사)
관심분야 : 정보보안, 블록체인.
E-mail : heejung@sungshin.ac.kr

김 혜 리(Hyeri Kim)
2007년 성신여대 미디어정보학부 (공학사)
2009년 성신여대 전산학과 (이학석사)
2009년~2011년 한국정보인증
2011년~2013년 금융보안연구원
2013년~2018년 성신여대 컴퓨터학과 박사
관심분야 : 개인정보보호, 블록체인, 스마트 컨트랙트
E-mail : hrkim@sungshin.ac.kr

홍 승 필(Seng-phil Hong)
1993년 B.S. in Computer Science, Indiana State University, USA.
1994년 M.S. in Computer Science, Ball State University at Indiana, USA.
1997년 Ph.D. Candidate in Computer Science, Illinois Institute of Technology, USA.
2003년 Ph.D. in Information Security, KAIST University, Korea.
1997년～2005년 LG-CNS Research and Development Center
2005년～현재 성신여대 융합보안공학과 교수
관심분야 : 개인정보보호, 정보보안, E-business 보안, 블록체인, IoT 보안
E-mail : philhong@sungshin.ac.kr