Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.187

개인용 보안장치를 통한 안전한 분산형 암호 화폐 거래 모델

이 창 근,† 김 인 석‡
고려대학교 정보보호대학원 금융보안학과

Secure Distributed Cryptocurrency Transaction Model Through Personal Cold Wallet

Chang Keun Lee,† In-Seok Kim‡
Department of Financial Security, Graduate School of Information Security, Korea University

요 약

2014년 3월, 세계 최대의 비트코인 거래소였던 마운트곡스(Mt. Gox)가 해킹 공격으로 폐쇄된 사건 이래로 최근까지 국내 암호 화폐 거래소인 코인레일(Coinrail)이 해킹되는 등 사건이 잇달아 발생하고 있다. 이러한 거래소 해킹 사건은 단순한 시스템 해킹 수준을 넘어 사용자들의 자산이 탈취되는 자산 손실로까지 피해가 확산되고 있어, 암호 화폐 거래소에 대한 보안 이슈가 발생하였다. 위와 같은 문제를 해결하기 위해 탈중앙화 거래소(DEX, Decentralized Exchange)가 활발히 연구되고 있으나 이 또한 문제를 완화시킬 뿐 해결방안으로서는 부족한 실정이다. 따라서 본 논문에서는 기존의 암호 화폐 거래소들에 대한 보안위협을 분석하고 이에 대한 보안 요구사항을 도출한다. 또한 개인용 보안장치를 통한 안전한 분산형 암호 화폐 거래 모델을 제안하여 본 논문에서 제안하는 거래 모델이 앞선 보안위협에 대한 해결책임을 입증한다.

ABSTRACT

Ever since the world's largest Bitcoin Echange, (Mt. Gox), was closed in March 2014 due to the series of hacking, still many other Exchages incl. recent Coinale in Korea have been attacked. Those hacking attempts never stopped and have caused significant threats to the overall industry of Crypto Currency and resulted in the loss of individual investors' asset. The DEX (Decentralized Exchange) has been proposed as a solution to fix the security problem at the Exchange, but still it is far away to resolve all issues. Therefore, this paper firstly analyzes security threats against existing Crypto Currency Exchanges and secondly derives security requirements for them. To do that it proposes a secure and distributed Crypto Currency Transaction Model through Personal Security devices as a solution. The paper also proves this new attempt by demonstrating its unique modelling; ultimately by adopting this modeling into Crypto Exchange is to avoid potential security threats.

Keywords: Distributed network, Flexible trading, HTLC, Cold wallet, Cryptocurrency exchange

Received(10. 24. 2018), Modified(12. 17. 2018), Accepted(12. 28. 2018)

† 주저자, klee@keypair.co.kr
† 교신저자, iskim11@korea.ac..kr(Corresponding author)

I. 서 론

블록체인 기반 전자금융거래는 본래 분산형 구조를 목표로 한다. 하지만 매수 및 매도와 같은 거래 주문 매칭 문제로 중앙화 거래소가 출현하게 되었고, 이는 중앙형 처리구조에서 분산형 처리구조로 탈바꿈을 목표로 하는 블록체인 기술 적용의 취지에 위배되는 구조이다. 이 외에도 중앙화 거래소에는 개인키 관리 저장소를 항상 온라인 상태로 유지, 거래소를 무조건 신뢰해야 한다는 투명성 부족, 환전율 일치 시에만 거래가 가능 등 다양한 문제들이 존재한다. 이러한 문제들로 최근 탈중앙화 거래소가 출현하게 되었지만 탈중앙화 거래소 역시 중앙화 거래소가 가지는 보안성 문제, 투명성 부족 등을 완전히 해결하지 못한다.

따라서 본 논문에서는 위와 같은 문제를 해결하기 위해 기존 거래소 시스템이 가지는 보안 위협을 분석하고 블록체인 기반 전자금융거래가 가져야 하는 보안요구사항을 체계화시킨다. 또한 이를 해결하기 위한 방안을 제시하고 제안하는 모델이 앞서 설명한 보안 위협에 안전함을 입증한다. 본 논문의 우수성은 아래와 같이 정리할 수 있다.

- 거래소가 개입하지 않고 거래를 성사시키는 방안을 제시한다.
- 개인용 안전장치를 통해 분산형 암호 화폐 거래를 가능하게 함으로써 블록체인 기반 전자금융거래의 본래 취지를 달성한다.
- 기존 시스템에 대한 보안 위협 분석 및 보안요구사항을 도출함으로써 블록체인 기반 시스템을 위한 보안기능을 체계화하였다.
- 가변적인 환율을 사용함에도 불구하고 지갑 내에서 환전하려는 사용자에게 안정적인 서비스를 제공하는 방안을 모색하였다.

2장 관련 연구에서는 암호 화폐 지갑에 대한 분류 분석을 하며, 3장 암호 화폐 거래소에 대한 보안 분석에서는 CEX(Centralized Exchange) 및 DEX (Decentralized Exchange)에서 가능한 공격을 바탕으로 시스템에 존재하는 보안 위협을 분석하고 이에 따른 보안요구사항을 도출한다. 4장 제안하는 암호 화폐 거래 모델에서는 본 논문에서 제안하는 모델을 설명하며 이 모델이 앞서 말한 보안 위협에 안전함을 입증한다. 마지막으로 5장에서 결론을 맺으며 본 논문을 마친다.

II. 관련 연구

암호 화폐 거래의 본래 취지에 맞도록 탈중앙화 거래소에 대한 연구가 활발히 되어왔으나, 탈중앙화 거래소는 하나의 서비스를 제공하는 데에 시스템을 나누어 관리하는 것으로 해킹 등의 위험이 나누어졌을 뿐 근본적인 문제는 해소되지 않는다. 또한 이 역시 거래소이기 때문에 거래에 대한 투명성이 제공되지 않는 한 신뢰하기 어렵다는 한계가 있다. 아래는 이러한 중앙화 및 탈중앙화 거래소에 대한 비교 분석이다.

위 Table 1을 보고 알 수 있듯이 탈중앙화 거래소는 중앙화 거래소가 갖는 많은 보안 위협을 완화시키는 것을 볼 수 있다. 따라서 중앙화 거래소에 대한 현실적인 대안방안으로 탈중앙화 거래소가 활발히 연구되고 있다. 하지만 아래 Fig. 1을 보면 알 수 있듯이 탈중앙화 토폴로지는 중앙화 토폴로지에서 중앙이 분리되었을 뿐 분산형과 동일한 토폴로지가 아니다. 따라서 탈중앙형 거래소는 블록체인 기술 도입의 근본적인 취지에 부합하지 못한다. 그러므로 블록체인 기술의 근본적 목적인 분산화 금융거래를 가능하게 하며 기존에 거래소가 갖는 보안 위협에 안전한 모델을 구축해야 한다.

Table 2는 본 논문의 이해를 위한 용어 설명이다.

마지막 유동성 공급자의 경우 본 논문에서는 거래

Table 1. Comparison with CEX and DEX.

	Centralized	Decentralized
Hack issue	very high	high
Knowledge requirements	low	high
Transparency	no	no
Early buy-in	possible	possible
transaction fee	high	medium
Speed	medium	slow

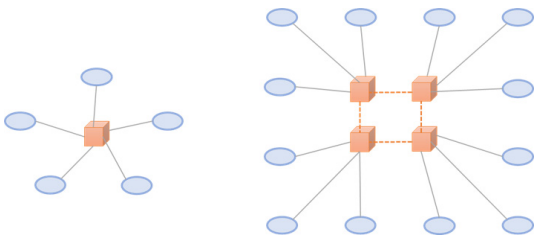

Fig. 1. Exchange network topology.Centralized (left) and Decentralized (right).

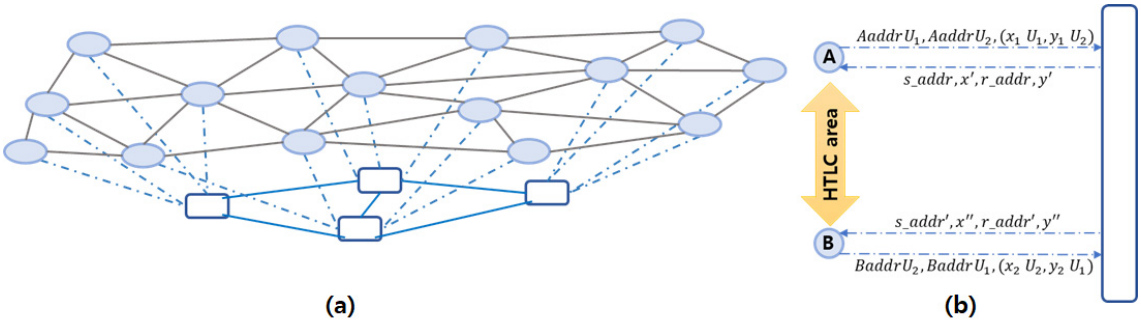

Fig. 2. Proposed transaction model. (a) Transaction network and (b) FACCS protocol.

자들이 거래소를 사용하지 않고 매수 및 매도를 할 수 있도록 화폐 교환 기능을 수행하는 주체로 사용된다.

Table 2. Terminology as a background

Term.	Description
Hot Wallet	This wallet always connected network. (online state)
Cold Wallet	This wallet always disconnected network without operating time. (offline state)
CEX	The platforms or/and the applications make traders exchange their crypto assets using a specific center.
DEX	The platforms or/and the applications are similar with CEX. But this systems are consist of servers more than two.
Liquidity Provider	This subject provides liquidity to traders on blockchain service.

III. 암호 화폐 거래소에 대한 보안 분석

암호 화폐 거래소는 고객의 지갑을 거래소 서버에서 관리하기 때문에 항상 온라인 상태라는 문제가 있다. 고객의 지갑을 항상 온라인 상태로 유지하는 것은 공격자에게 원격접속을 할 수 있는 가능성을 열어두는 것과 같다. 따라서 이러한 암호 화폐 거래소는 사용자가 PC 또는 스마트폰 등 네트워크를 통해 어디서나 쉽게 이용할 수 있다는 장점이 있지만 해킹의 위험에서 제외되지 못한다는 문제가 있다.

이에 금융보안원에서는 금융권 블록체인을 도입할 시 보안 위협을 아래 Table 3과 같이 분류하였다.

Table 3. A taxonomy of security threats on blockchain-based financial system[3].

Category	Threat
Key Management	Theft and Loss
	Generating Weak Key
Transaction Authentication and Verification	Consensus Intercepting
	Unusual transaction within side-chain
Management of Permissions	Privacy Violation
	Privilege Abuse
Blockchain S/W security	Vulnerablity of Blockchain S/W
	Vulnerability of Smart Contract
Service Security	DDoS Attack
	Availability Attack
	Hard to Fraud Detection
	No Interoperability

IV. 제안하는 암호 화폐 거래 모델

본 논문에서 제안하는 분산형 암호 화폐 거래 모델은 Fig. 2의 (a)와 같으며 (b)는 (a)에서 파란 실선에 해당하는 부분으로 FACCS protocol에 대한 그림이다.

4.1 Flexible Atomic Cross-Chain Swap

블록체인 기술 적용의 본래 목적은 완전한 P2P 통신임에도 불구하고 거래소가 출현하게 된 이유는 매수 매도와 같은 거래뿐만 아니라 Cross-Chain Swap와 같은 서비스를 제공받기 위함도 있다.

Cross-Chain Swap이란 서로 다른 종류의 암호

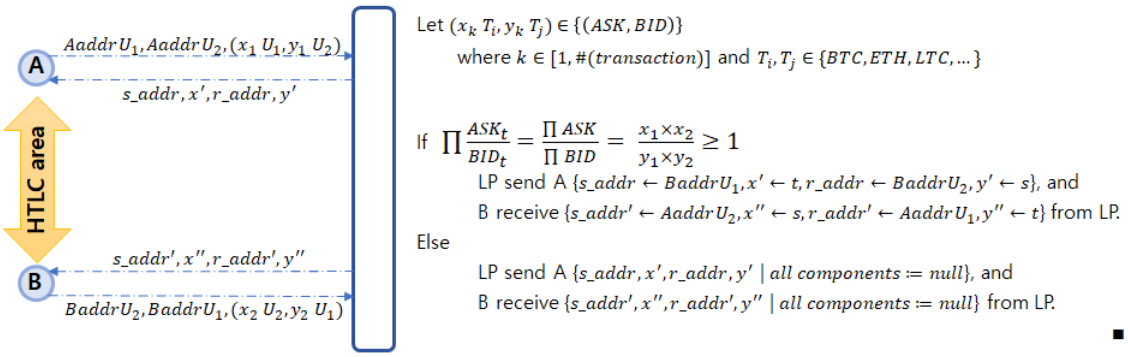

Fig. 3. FACCS protocol using HTLC(hashed time-lock contract) between two users with LP.

화폐가 서로 교환되는 기능을 얘기한다. 쉽게 예를 들어 설명하자면, A는 10000원을 US USD로 환전하고자 하고 B는 보유하고 있는 USD에서 10000원 만큼만 환전하고자 한다. 이 둘은 서로 조건이 부합하기 때문에 그 때의 시세에 따라 원화와 USD를 교환할 수 있다. 하지만 이는 A와 B가 서로 교환하고자 하는 화폐 종류와 금액을 알고 있을 경우에 해당된다. 위의 상황을 암호 화폐 시장으로 반영하여 생각해보았을 때, 이러한 요구를 취합하여 중매를 해주는 곳이 필요하게 되는데 이는 사람들이 암호 화폐 거래소를 사용하는 이유 중 하나가 될 수 있다.

ACCS(Atomic Cross-Chain Swap)[1]는 거래소 없이 사용자가 보유하고 있는 지갑 내에서 서로 다른 종류의 화폐를 교환하는 기능을 말한다. 이 때 교환하는 두 주체 중 한명이 악의적으로 상대의 자산을 받은 후 잠적하지 못하도록 막는 것이 중요하다. HTLC(Hashed Time-Lock Contract)[7]는 이를 위한 기능이 구현된 스마트 컨트랙트로 서로 합의가 이루어졌을 때에만 화폐 교환이 성사되고 그렇지 않은 경우는 전송한 자산이 반환되도록 한다. 더 자세하게, HTLC란 Time-Lock 시간 내에 Hold된 트랜잭션을 열기 위해서는 서로 합의된 비밀값에 대한 해시값이 제시되거나 위조가 불가능 할 만큼의 블록이 작성되기 전(즉, Time-Lock 시간 내)에 거래를 성사시키지 않는 기능이다.

아래 Fig. 4는 Hashed Time-Lock을 통해 상호간 자산 교환이 안전하게 성사되는 것을 보여준다.

본 논문에서는 FACCS(Flexible Atomic Cross-Chain Swap) 모델을 두어 유동성을 높이고 거래소 없이 유동성 제공자만으로 거래를 성사시키는 방법을 제시한다. Fig. 3은 사용자가 지갑 내에서 화폐 교환을 할 때의 프로토콜을 설명하는 것으로 사용자는 화폐 교환을 위해 주문을 LP에 전달하고 LP는 사용자들의 주문을 취합하여 판별식을 통과하는 주문들에 한해 해당 사용자들에게 교환이 가능한 사용자들의 지갑 주소를 보내준다.

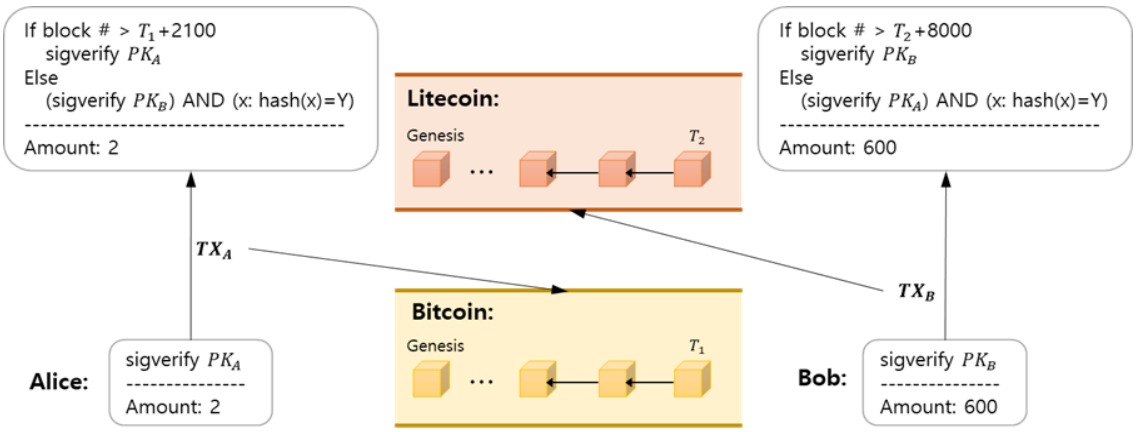

Fig. 4. An atomic cross-chain swap[1]

Table 4. Notation on FACCS protocol

Notation	Description
$Aaddr\,U_1$	A's wallet address for U_1.
$Aaddr\,U_2$	A's wallet address for U_2.
$Baddr\,U_1$	B's wallet address for U_1.
$Baddr\,U_2$	B's wallet address for U_2.
s_addr or s_addr'	Receiver's wallet address for ASK order.
r_addr or r_addr'	Sender's wallet address for BID order.

ASK는 s_addr로 전송하고 BID는 r_addr에서 들어올 것으로 내역을 확인할 수 있다.

판별식은 아래의 식 (1)과 같으며, 이 식을 통과하는 것은 해당 주문들에 대해 사용자가 지정한 원래의 교환비보다 좋거나 같은 비율로 체결될 수 있음을 의미한다.

$$\prod \frac{ASK_t}{BID_t} = \frac{\prod ASK}{\prod BID} \geq 1 \quad (1)$$

FACCS는 사용자가 지갑 내에서 보유하고 있는 화폐의 일부를 다른 화폐로 교환하고자 하는 요구로부터 시작된다. (ASK, BID)쌍을 주문으로 LP에게 전송하고 LP는 이러한 주문들을 취합 후 판별식을 적용하여 주문들에 대한 결과를 전송한다. 체결된 주문들에 대한 결과는 ASK에 대한 수신자의 지갑 주소 및 화폐량, 그리고 BID에 대한 송신자의 지갑 주소 및 화폐량이며 체결되지 않은 주문들에 대한 결과는 모두 Null로 처리하여 교환할 수 있는 상대의 주문이 없음을 알린다. 아래는 LP를 이용하는 공격자에 대해 크게 세 가지 유형으로 분류한 것이다.

4.1.1 A_{LP}가 $User$에게 s_addr를 자신의 주소로 위조하여 보내는 경우

공격자 A_{LP}가 사용자 U_i(단, $i \in [1,n]$)에게 s_addr를 자신의 주소로 위조하여 보내기 위해 적어도 사용자가 보낸 질의에 합당하는 응답을 보내야 한다.

하지만 결과적으로 사용자들은 LP로부터 받는 응답에도 HTLC를 사용하여 서로 Swap을 수행하기 때문에 공격자가 중간에서 사용자들의 화폐를 갈취하는 것은 불가능하다. 이를 증명하기 위해 다음과 같이 강한 공격자를 가정한다.

- 공격자는 LP에서 사용하는 매칭 판별식을 수행할 수 있다.
- 공격자는 사용자가 LP로 질의하는 모든 내용을 도청할 수 있다.
- 공격자는 LP와 유사하거나 혹은 더 빠르게 응답을 사용자들에게 보낼 수 있다.

Fig. 5는 위와 같은 강한 공격자를 표현한 그림이다.

먼저 사용자들은 본인들의 질의에 여러 개의 응답이 도착할 경우 어떠한 것이 LP로부터 도착한 것인지 혹은 공격자로부터 도착한 것인지 구별 불가능하다. 이는 사용자가 수동적으로 선택하는 것이 아닌 시스템이 자동적으로 처리를 하는 것이기 때문이며, 따라서 도착한 응답들 중 먼저 도착한 응답에 대해 화폐 교환을 시도할 것이다.

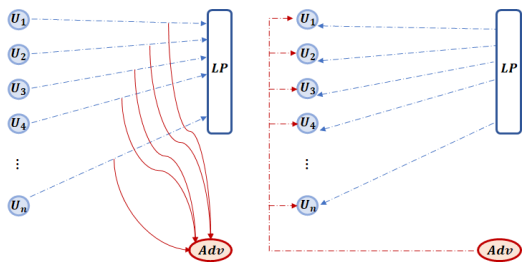

Fig. 5. Eavesdropping and trasacting forged address

하지만 본 논문에서는 이를 막기 위해 HTLC를 사용하며, HTLC의 본래 기능에 의해 양방향 거래가 발생하지 않는 경우 해당 주문을 취소하는 것으로 위와 같은 경우를 방지할 수 있다. 더 나아가 HTLC를 사용하는 것은 위와 같은 공격자뿐만 아니라 상대 사용자의 단순 변심에 의한 손해, 예를 들어 상대 사용자에게 화폐가 도달하는 순간 잠적하여 본인의 화폐 전송을 막는 경우,를 방지할 수 있다.

4.1.2 A_{LP}가 선행매매 공격자인 경우

앞서 설명한 매칭 판별식은 사용자의 화폐 교환 질의에 대해 수행된다. 하지만 본 논문에서 말하는

Table 5. Intervals of g according to risk levels for FACCS within coldwallet

Risk levels	Intervals of g
few	$0 \leq g \leq 0.03$
low	$0.03 < g \leq 0.07$
medium	$0.07 < g \leq 0.12$
high	$0.12 < g \leq 0.20$

사용자의 화폐 교환 질의는 실제 시장 가격을 반영한 질의이며, 이에 사용되는 실제 시장 가격은 CoinMarketCap[1)]을 참조한다.

본 논문에서는 각 사용자마다 교환하고자 하는 화폐들의 교환율을 가변적으로 수용하지만 현재 존재하는 거래소의 수수료보다 높지 않도록 조절하기 위해 아래와 같이 리스크 수준을 달리한다. (단, g는 실제 시장 가격에서 추가되는 교환율을 의미한다.)

리스크 수준에 따라 교환율을 제한하는 목적은 화폐 교환에 따른 거래 매칭의 유동성을 높이기 위함으로 리스크 수준이 높을수록 매칭 우선순위가 높아진다. 또한 위 Table 5에서 리스크 수준이 높은 g는 현재 운영되는 거래소에서 사용자에게 요구하는 수수료보다 저렴하다. 이와 같은 경우가 가능한 이유는 본 논문에서 제안하는 모델이 자동화 시스템으로 운영되기 때문이다. 해킹으로 인한 자산 손실 문제가 존재하는 거래소를 사용하지 않으면서 자동화 시스템으로 운영한다는 면에서 위 g의 범위는 합리적이라 말할 수 있다. 결과적으로 위와 같이 효율적이면서도 안정적으로 교환을 성사시키면서 교환율을 제한하며, 4.1.1절에서 설명한 것과 같이 HTLC를 통해 실제 교환이 이루어지기 때문에 공격자 A_{LP}가 선행매매 공격을 통해 이득을 취하기에 매우 어렵다.

4.1.3 A_{LP}가 masquerading 공격자인 경우

본 논문에서 LP에 대한 어플리케이션 업데이트는 물리적인 수동 업데이트를 제안한다. 따라서 어플리케이션에 원격으로 접근하여 프로그램을 변경하려는 시도는 기본적으로 차단하는 것으로 해당 공격을 방지한다. 또한 이러한 악의적인 접근이 발생할 경우 LP 시스템들은 해당 주소를 블랙리스트로 관리하여 이후 접근을 원천적으로 차단한다.

1) CoinMarketCap(Cryptocurrency Market Capitalizations)은 다양한 암호 화폐들의 전 세계적 실시간 시장 가격을 보여주는 사이트로 주간 암호 화폐 시세 변화에 따른 그래프도 확인할 수 있다. API가 공개되어 있어 사용자들이 사용하는 지갑에서 실시간 시장 가격을 보여주는 기능을 쉽게 적용할 수 있다.

4.2 유연한 차세대 암호 화폐 지갑 시스템

이 절에서는 4.1절 FACCS와 지갑 대 지갑 직송 기능을 포함하는 차세대 암호 화폐 지갑 시스템을 설명한다. Fig. 2(a)는 본 논문에서 제안하는 차세대 암호 화폐 지갑 시스템이며 하드웨어 기반의 콜드월렛을 거래 및 직송의 주체로 본다. Fig. 2(a)에서 하위 계층에 있는 주체들은 LP들이며, LP는 FACCS 서비스만을 제공하는 주체이다.

본 논문에서 제안하는 시스템은 스마트 컨트랙트로 작성되는 자동화 시스템으로 거래소에서 제공하지 못한 거래의 투명성을 제공할 수 있다. 또한 거래 및 직송의 주체는 하드웨어 기반의 콜드월렛이기 때문에 사용자의 개인키는 거래에서 사용되는 순간을 제외하고 항상 오프라인으로 안전하게 유지된다. 그 외에도 자동화 시스템으로 구축하기 때문에 사용자에게 많은 지식을 요구하지 않으며, 선행매매 등의 공격이 발생되기 매우 어렵다. 마지막으로 거래소를 이용함에 따라 높았던 거래 수수료가 필요하지 않게 되며, LP를 두고 유연한 거래가 가능하도록 판별식을 사용하여 전체적인 거래의 속도를 높이고자 하였다.

아래 Table 6은 중앙화 거래소를 개선한 탈중앙화 거래소와 본 논문에서 제안하는 시스템을 비교한 것이다.

앞서 설명한 바와 같이 탈중앙화 거래소는 중앙화 거래소에 존재하는 문제점을 개선한 시스템이다. 따라서 위 표에서는 이러한 탈중앙화 거래소와 본 논문에서 제안하는 모델을 비교하였다. 제안하는 모델은 거래소를 사용하지 않으며 LP를 통해 화폐 교환을 하더라도 실제 교환은 HTLC를 통해 수행한다. 또

Table 6. Comparison with DEX and Proposed.

	Decentralized	Proposed
Hack issue	high	very low
Knowledge requirements	high	very low
Transparency	no	yes
Early buy-in	possible	impossible
transaction fee	medium	very low
Speed	slow	medium

한 기본적으로 사용자의 개인키를 개인용 안전장치인 콜드월렛에 저장하기 때문에 해킹 가능성이 극히 드물다. 또한 콜드월렛은 개인키를 저장하면서 인증을 수행할 때에 서명 값을 생성하여 전송하기 때문에 별도의 사용자 인증과 같은 불편함이 없기 때문에 초기 지갑을 생성하는 과정을 수행한 이후에 사용자에 대한 지식 요구가 매우 낮다. 또한 본 논문에서 제안하는 모델은 사람이 관여하지 않는 자동화 시스템이기 때문에 사용자들은 투명한 거래를 보장받을 수 있다. 그 외에도 앞서 4.1절에서 설명한 바와 같이 선행매매 공격이 불가능하며, 전송 수수료[2] 또한 매우 낮다. 마지막으로 리스크 수준과 교환율 제한을 여러 단계로 두어 거래 속도를 저하시키지 않도록 하였다.

V. 결 론

본 논문에서는 블록체인 본래 취지와 가장 가까운 시스템을 제안하였다. 또한 스마트 컨트랙트로 자동화 시스템을 구축하는 것으로 기존에 제공하지 못했던 거래의 투명성을 제공하였고, FACCS를 사용하여 거래의 유동성을 확보하였다. 제안하는 시스템은 거래소없이 화폐 매수 및 매도가 가능하며 지갑 대 지갑으로 직송이 가능하다.

본 논문에서 제안하는 시스템은 암호 화폐를 통한 결제 시스템, 환전 시스템 등 다양한 분야에서 활용할 수 있으며 더 나아가 국경이 없어지는 매우 높은 수준의 사용자 편의성을 제공할 수 있다. 향후 제안하는 시스템에 대한 공격 모델을 설립하여 안전성 및 프라이버시를 분석하는 것이 중요하다.

References

[1] Iddo Bentov, Yan Ji, Fan Zhang, Yunqi Li, Xueyuan Zhao, Lorenz Breidenbach, Philip Daian, and Ari Juels, "Tesseract: Real-Time Cryptocurrency Exchange Using Trusted hardware," IACR Cryptology ePrint Archive, 2017.

[2] Maurice Herlihy, "Atomic Cross-Chain Swaps," arXiv preprint arXiv:1801.09515, 2018.

[3] Young-Seek Chung and Jae-Sang Cha, "The Security Risk and Countermeasures of Blockchain based Virtual Currency Trading," Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 11, No. 1, pp. 100-106, Feb. 2018.

[4] Financial Security Institute, "BlockChain Technology and Security Considerations", Aug. 2017.

[5] Seo-Gu Kang, Hyung-Joon Bae, Seong-Hyeon Lim, and Young-Sook Lee, "A Study on the Vulnerability and Countermeasures of Bitcoin," Proceedings of the Korean Society of Computer Information Conference, Vol. 25, No. 2, pp. 124-127, 2017.

[6] Will Warren and Amir Bandeali, "0x: An open protocol for decentralized exchange on the Ethereum blockchain," URI: https://github.com/0xProject/white-paper, 2017.

[7] Dr. Julian Hosp, Toby Hoenisch, and Paul Kittiwongsunthorn, "COMIT Cryptographically-secure Off-chain Multi-asset Instant Transaction network," arXiv preprint arXiv:1810.02174, 2018.

[8] Satoshi Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," URI: https://bitcoin.org/bitcoin.pdf, Oct. 2008.

[9] Abraham Othman, David M Pennock, Daniel M Reeves, and Tuomas Sandholm, "A practical liquidity-sensitive automated market maker," ACM Transactions on Economics and Computation, Vol. 1, No. 3, 2013.

[10] Wikipedia: Mt. Gox, https://en.wikipedia.org/wiki/Mt.Gox. AQccessed: 2017-02-016.

2) 제안하는 모델의 경우 일반 화폐 전송은 콜드월렛 간의 전송이므로 수수료가 없으며, 지갑 내에 화폐 교환을 하고자 할 경우에만 시장 가격보다 극히 적은 추가 금액이 발생할 수 있다.

〈저자소개〉

이 창 근 (Chang Keun Lee) 정회원
1992년 5월: IOWA State University Poli. Sci.학과 졸업
2007년 8월: 고려대학교 전문경영학 석사(MBA)
2013년 9월~현재: ㈜키페어 공동대표
2017년 3월~현재: 고려대학교 금융보안학과 석사과정
〈관심분야〉 정보보호, 전자금융보안, 블록체인

김 인 석 (In-Seok Kim) 정회원
1973년 2월: 홍익대학교 전자계산학과 졸업
2003년 2월: 동국대학교 정보보호학과 석사
2008년 2월: 고려대학교 정보경영공학과 박사
2009년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 정보보호, 전자금융보안, IT감사, 전자금융법규