Person-to-Person 결제 환경에 적합한 블록체인 기반의 안전한 금융 거래 시스템 연구

박병주*, 곽진**
*아주대학교 컴퓨터공학과 정보보호응용및보증연구실
**아주대학교 사이버보안학과
e-mail:bjpark.isaa@gmail.com*, security@ajou.ac.kr**

A Study on Blockchain Based Secure Financial Transaction System for Person-to-Person Payment Environment

Byeong-ju Park*, Jin Kwak**
*ISAA Lab., Department of Computer Engineering, Ajou University
**Department of Cyber Security, Ajou University

요 약

최근 모바일 결제 시장의 규모가 2015년 45억 달러에서, 2016년 62억 달러로 성장하며, P2P 거래량도 함께 증가하고 있다. 또한, P2P 결제 시장에 페이팔, 비자와 같은 온라인 결제 업체와 대형은행 뿐만 아니라, 페이스북, 구글, 애플, 삼성 등 IT회사들도 참여하고 있다. 안전하고 편리한 P2P 결제를 위해 다양한 거래 방식이 연구되고 있지만, 다양한 기업 및 은행들의 참여로 인해 서로 다른 방식으로 사용자들이 불편을 겪고 있으며, 모바일 환경의 특성으로 인해 많은 보안위협들이 발생하고 있는 실정이다. 이에 따라, 모바일 환경에서의 P2P 결제를 고려한 통합적인 보안 기술이 개발되어야 하며, 민감 정보라고 할 수 있는 사용자의 계좌번호, 금융거래 관련 정보 등을 보호하기 위한 기술이 필수적이다.

따라서 기존 은행권의 P2P 거래 방법의 문제점을 분석하고 블록체인 시스템과 DHT에 대해 분석한 후, P2P 결제 환경에 적합한 안전한 블록체인 기반 금융 거래 시스템을 연구함으로써, P2P 거래 환경의 안전성을 향상시키고자 한다.

1. 서론

최근 모바일 결제 시장이 크게 성장하며, 해당 결제 시장과 관련된 다양한 기술들이 주목받고 있다. 그 중 P2P(Person-to-Person) 결제 시장은 사용자-사용자 간의 거래라는 점에서 주목받고 있으며, 기존의 은행권 외에도 페이팔(Paypal), 비자(Visa)와 같은 온라인 결제 업체, 페이스북(Facebook), 구글(Google), 애플(Apple), 삼성 등 IT 회사들도 참여하고 있다. 하지만 다양한 기업 및 은행들의 독자적인 거래 방식으로 인해 사용자들이 불편을 겪고 있다. 또한, 모바일이라는 환경의 특성으로 인해 기존 모바일 보안 위협을 비롯해 새로운 보안 위협들이 발생하고 있다. 따라서, 다양한 P2P 결제 환경에 적합한 보안 기술이 필요하다. 또한 금융거래라는 측면에서 사용자의 계좌번호, 금융거래 관련 정보 등 민감한 개인정보들을 보호하기 위한 기술이 필요하다[1].

금융권에서 주목하고 있는 블록체인(Blockchain) 기술은 네트워크 내 모든 참여자가 공동으로 거래 정보를 검증·기록·보관하는 기술로, 거래 장부를 분산 저장해 조작이 어렵다. 또한, 분산 해시 테이블(DHT: Distributed Hash Table) 기술은 데이터와 서버를 동일한 주소 공간에 배치하는 기술로, 중앙 서버 없이도 데이터를 관리하는 서버를 찾는 룩업에 성능이 좋으며, 부하가 집중되지 않고 분산시키는 장점으로 인해, 극단적으로 큰 규모의 노드들도 관리할 수 있다. 이에 따라 본 논문에서는 기존의 P2P 거래 방식의 문제점을 고려하여 블록체인과 분산 해시 테이블을 통해 가용성이 높고 안전한 P2P 거래 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구를 분석한 후, 3장에서 P2P 거래 방식과 문제점에 대해 분석하고, 4장에서 P2P 결제 환경에 적합한 안전한 블록체인 기반 거래 시스템을 제안한 후, 5장에서 안전성을 분석하고, 6장에서 결론으로 끝을 맺는다.

2. 관련연구

2.1 블록체인

블록체인 기술은 비트코인(Bitcoin)을 위해 개발된 기반 기술로, 가상 화폐로 거래할 때 발생 가능한 공격을 막기 위한 기술이다. 블록체인은 거래 정보가 기록되어 있는 원장을 중앙 서버가 아닌 P2P 네트워크에 분산하여 참가자가 공동으로 기록하고 관리하며, 블록 체이닝을 통해 거래 기록에 대한 위·변조 여부를 검증할 수 있다. 현재에는 사용처에 따라 다양한 형태로 변형되어 사용되고 있으나 기본적인 구조는 유사하다[2,3,4].

• 블록체인의 종류와 개념 및 특징

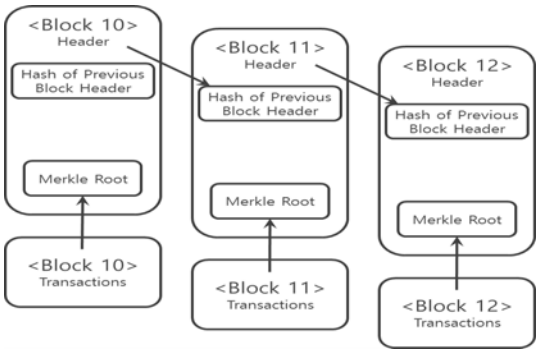
블록체인은 아래 <표 1>과 같이 분류할 수 있으며, 특징에 따라 사용처가 나누어진다[5,6].

<표 1> 블록체인의 종류와 개념 및 특징

구 분	개념 및 특징
퍼블릭 블록체인 (Public Blockchain)	- 인터넷을 통해 모두에게 공개, 운용 가능한 거래 장부 - 컴퓨팅 파워를 네트워크에 제공 - 네트워크 확장이 어렵고 거래 속도가 느림
프라이빗 블록체인 (Private Blockchain)	- 개인형 블록체인 - 1개의 주체가 내부 전산망을 블록체인으로 관리
컨소시엄 블록체인 (Consortium Blockchain)	- 반중앙형 블록체인 - 미리 선정된 주체들만 참여 가능 - 합의된 룰을 통해 공증 참여 - 네트워크 확장이 용이하고 거래속도가 빠름

• 블록체인 기본 구조

블록체인은 이전 블록헤더의 해시값, Merkle root, 전자서명, 현재 블록의 해시값, 타임스탬프 등으로 이루어진 블록헤더와 Merkle Root, 트랜잭션 등으로 이루어진 블록 데이터로 구성되어 있다. 블록체인의 기본 구조는 아래 (그림 1)과 같다.



(그림 1) 블록체인 기본 구조

• 거래 기록 및 확정 메커니즘

블록체인 기술에서는 공개성과 분산성이라는 특성으로 인해 위·변조에 대응하는 거래 기록 및 확정 메커니즘이 존재한다. 거래 기록 및 확정 메커니즘은 proof-of-work, proof-of-stake 등 다섯 가지가 있다[7].

2.2 분산 해시 테이블

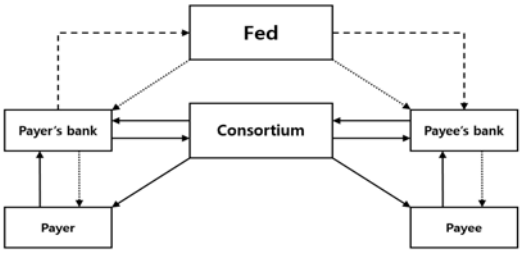
분산 해시 테이블은 해싱을 통하여 생성된 킷값과 ID의 쌍들을 시스템을 구성하는 전체 노드들에 균일하게 분산하기 위해 제안된 lookup 방식이다. 데이터의 킷값과 ID를 이용하여 모든 노드들과 데이터들을 동일한 주소 공간에 할당하는 방식으로 데이터 및 노드 관리 등의 장점이 있다[8,9]. 대표적인 DHT 알고리즘에는 Chord, Pastry, CAN 등이 있다.

3. 기존 거래 방식의 문제점

기존 P2P 결제 방식은 참여하는 엔티티의 종류에 따라 NONBANK-CENTRIC, BANK-CENTRIC, BANK-CENTRIC(Consortium)으로 분류할 수 있다[10]. 본 논문에서 제안하는 시스템은 BANK-CENTRIC(Consortium)과 유사한 형태를 취하므로 본 장에서는 해당 모델에 대해 분석한다.

3.1 BANK-CENTRIC P2P(Consortium Model)

BANK-CENTRIC P2P(이하 컨소시엄 모델)은 결제 요청자, 피결제 요청자, 결제 요청자의 은행, 피결제 요청자의 은행, 컨소시엄, 정부 기관과 같은 엔티티로 구성되며 자세한 프로토콜은 아래 (그림 3)과 같다.



(그림 2) BANK-CENTRIC P2P 프로토콜

컨소시엄 모델은 위와 같이 Payer, Payee, Consortium, Payer's bank, Payee's bank, Fed로 구성된다. 해당 프로토콜은 사용자-은행, 은행-컨소시엄, 은행-Fed 등 데이터 송수신이 발생하게 되고 이에 따라 거래의 속도가 늦어질 수 있으며, 내부자에 의한 거래 기록 데이터 위·변조가 발생할 수 있다. 또한, 모든 기존 P2P 거래 모델에서 금융거래는 중앙 집중화된 장부 시스템에 따라 이루어지고, 모든 거래기록 및 중요 정보들이 중앙 데이터베이스에 저장되어 있어, 중앙 데이터베이스가 공격을 받게 될 경우 가용성이 떨어질 수 있다. 아래 <표 2>는 P2P 거래 과정 중 일어날 수 있는 공격에 대한 설명이다.

<표 2> P2P 거래 중 발생 가능한 공격

공격 유형	설 명
데이터 위·변조	- 내부자에 의한 데이터 위·변조
서비스 거부 공격	- 은행 데이터베이스, 웹사이트 등을 마비시켜 가용성을 떨어뜨림

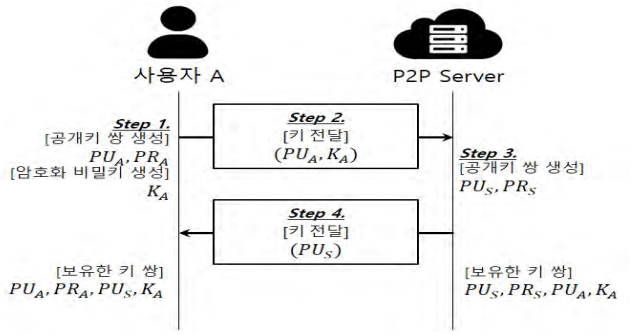
4. 제안 시스템

본 장에서는 DHT와 블록체인을 활용한 P2P 결제 시스템을 제안한다. 참여하는 엔티티는 사용자, P2P서버, DHT 노드이며, 다음 <표 3>은 제안 시스템에서 사용된 요소들의 표기법을 나타낸다.

<표 3> 제안 시스템에 사용된 표기법

표기법	설 명
PR_x	x의 개인키
PU_x	x의 공개키
K_x	x와 서버 간 대칭키
ID_x	x의 식별자
Sig_x	x의 서명
Tx_x	트랜잭션 x
T_x	타임스탬프 x
$Parse()$	역직렬화
$Compare(A,B)$	A,B 비교 검증
C_x	x의 직렬화된 거래 요청 정보
c_x	x의 송금·입금 정보
$account_x$	x의 계좌정보
PD	처리된 데이터
$L[]$	블록체인 메모리 공간
$ds[]$	데이터 저장

본 논문에서 제안하는 결제 시스템을 이용하기 위해 사용자는 P2P 서버와 사전에 블록체인에 사용될 전자서명 키와 암호화키를 교환하는 초기 과정을 거쳐야 한다. 다음 (그림 3)은 초기 과정을 나타낸 그림이다.

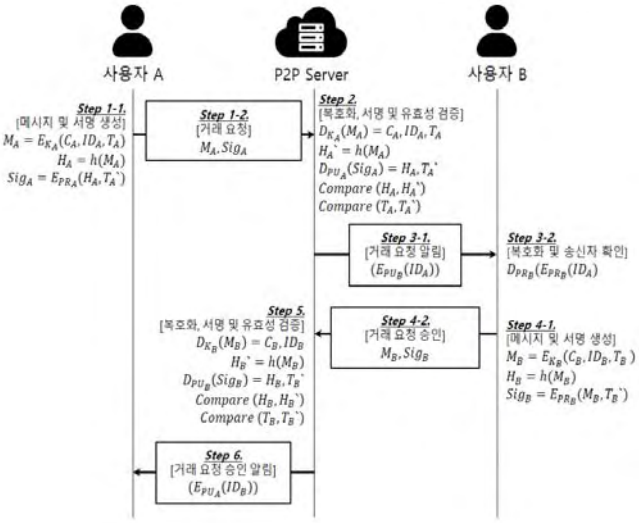


(그림 3) 초기 과정

Step 1. 사용자 A는 공개키 쌍과 암호화 비밀키 생성
Step 2. 사용자 A는 P2P서버에 암호화 비밀키와 전자서명 공개키 전송
Step 3. P2P 서버는 공개키 쌍을 생성
Step 4. P2P 서버는 공개키를 사용자 A에게 전송

위의 키 교환 절차는 사용자가 서비스를 이용하기 위해 P2P 서버의 웹사이트에 로그인을 한 후 이루어진다. 로그인을 한 후에 이루어지는 모든 통신은 SSL을 통해 이루어진다. 키 교환을 거치게 되면 사용자와 P2P서버는 전자서명 키 쌍과 사용자 또는 P2P서버의 전자서명 공개키, 암호화 비밀키를 보유하게 된다.

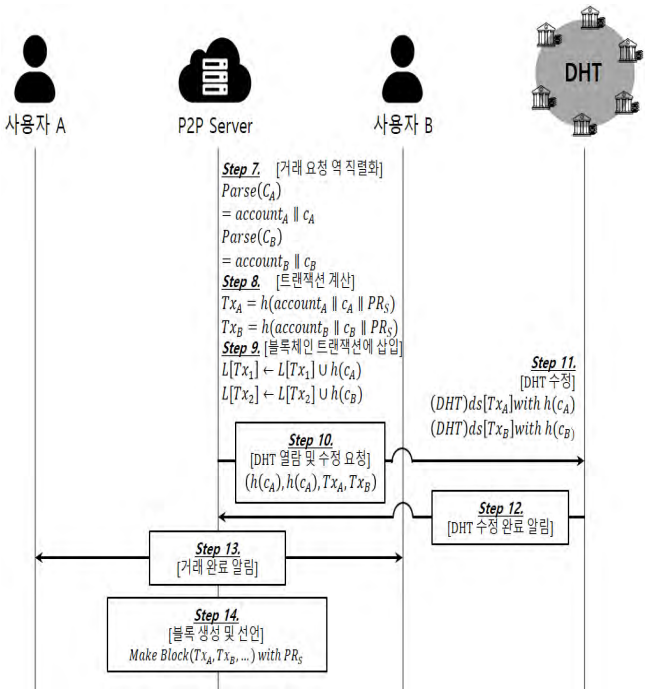
제안하는 시스템은 DHT 및 블록체인을 구성하는 은행권에서 공동으로 운영하는 P2P 서비스에 사용자가 로그인 한 후에 이루어진다. 프로토콜 중 상호 사용자 인증 및 거래 승인 단계는 다음 (그림 4)와 같으며, 각각의 스텝은 아래와 같다.



(그림 4) 상호 사용자 인증 및 거래 승인 단계

Step 1. 사용자 A는 자신의 은행 및 계좌 정보와 ID_A, 타임스탬프 T_A를 대칭키로 암호화한 후, 개인키로 전자서명을 생성해 서버로 전송
Step 2. P2P 서버는 사용자 A로부터 전송받은 M_A를 복호화해 ID_A를 얻고, 전자서명 및 타임스탬프 유효성 검증을 수행
Step 3. P2P 서버는 사용자 A의 식별자를 사용자 B의 공개키로 암호화해 전송하고 사용자 B는 전송받은 메시지를 복호화해 송금요청자 확인
Step 4. 사용자 B는 자신의 은행 및 계좌 정보와 ID_B, 타임스탬프 T_B를 대칭키로 암호화한 후, 개인키로 전자서명을 생성해 서버로 전송
Step 5. P2P 서버는 사용자 A로부터 전송받은 M_B를 복호화해 ID_B를 얻고, 전자서명 및 타임스탬프 유효성 검증을 수행
Step 6. P2P 서버는 사용자 B의 식별자를 사용자 A의 공개키로 암호화해 전송하고 사용자 A는 전송받은 메시지를 복호화해 송금대상자 확인

사용자들과 서버 간의 상호 사용자 인증 및 거래 요청 승인이 성공하면, 서버는 사용자들로부터 전송받은 거래 요청 메시지를 통해 거래를 진행한다. 거래 정보는 DHT에 저장되며 블록체인 블록으로 생성되어 선언된다. 상세한 프로토콜 및 절차는 다음 (그림 5)와 같다.



(그림 5) 거래 진행·완료, DHT 수정 및 블록 생성 절차

Step 7. P2P 서버는 사용자들로부터 전송받은 거래 요청 정보를 역직렬화해 사용자들의 정보를 얻음

Step 8. 역직렬화를 통해 얻은 사용자 A, B의 계좌정보와 자신의 공개키의 해시값을 계산하여 트랜잭션 생성

Step 9. 송금·입금 정보를 해시화해 Step 8에서 계산한 블록체인 해시값과 함께 계산한 후, 블록체인 트랜잭션에 삽입

Step 10. P2P 서버는 해시화된 계좌정보를 통해 DHT 열람 및 트랜잭션 저장을 요청

Step 11. DHT는 전송받은 사용자 계좌정보의 해시값을 통해 DHT 테이블에 트랜잭션 저장

Step 12. P2P 서버에게 DHT 내부 테이블 수정 완료 알림

Step 13. P2P 서버는 사용자 A, B에게 거래 완료 알림

Step 14. Step 8.에서 생성한 트랜잭션과 자신의 개인키를 통해 블록 생성

5. 안전성 분석

• 데이터 위·변조 방지

금융 거래 도중 데이터 위·변조가 발생할 수 있다. 공격자는 금융 거래 정보를 중간에 탈취해, 수신 계좌를 변경하거나, 금액을 바꿀 수 있다. 또한, 내부자가 데이터베이스에 저장된 정보를 위·변조할 위험이 있다. 하지만, 제안하는 시스템에서는 금융 거래 정보를 대칭키를 통해 암호화해 전송하며, 금융거래 정보는 블록체인에 저장해 선언한다. 블록체인에 저장된 정보는 이전의 복수의 블록들까지 모두 계산할 수 있으면 변조가 가능하나 해시 계산의 어려움으로 인해 불가능하다. 이에 따라, 공격자는 데이터를 위·변조할 수 없어 안전하다.

• 서비스 거부 공격 방어

일반적인 금융거래는 중앙 DB를 통해 이루어져 DDoS 공격이 발생할 경우, 가용성에 침해를 받는다. 본 논문에서 제안하는 시스템의 경우, 각각의 은행들이 폐쇄된 컨소시엄 블록체인의 노드들이 되며, DHT 노드 역할을 수행한다. 따라서 블록체인 생성과 DHT를 구성하는 은행들이 모두 분산 장부와 DHT를 가지고 있어, 서비스 거부 공격이 발생한다 해도 가용성의 침해 없이 지속적으로 블록을 생성해 위변조 검증을 수행하고 금융거래 서비스를 이용할 수 있다.

6. 결론

P2P 거래 시장이 빠르게 성장하고 있으며, 모바일을 통해 이루어지는 P2P 거래에 대한 연구가 활발하다. 다양한 은행 및 기업이 참여함에 따라, 다양한 서비스 및 플랫폼들이 등장하고 있으며, 기존의 금융거래의 취약점이 P2P 거래에도 그대로 적용됨에 따라 보안 기술 연구를 통한 안전성 향상이 필요하다.

본 논문에서는 블록체인, DHT 등을 통해 중간자 공격, 서비스 거부 공격과 같은 기존의 P2P 금융거래의 취약점을 보완하고, 안전한 P2P 결제 시스템을 제안하였다. 제안하는 시스템은 데이터 위·변조 방지 등을 통한 무결성, 분산 DB를 통한 가용성을 확보할 수 있어, 컨소시엄 P2P 거래 환경의 활성화를 촉진시킬 수 있으며, 해당 환경의 안전성을 높일 수 있다.

참고문헌

[01] 금융보안원, "주요 간편결제 서비스의 보안성 비교 분석", 2015.10.

[02] KORBIT, "블록체인의 기술적 이해 및 도입을 위한 첫걸음", 2016.03.

[03] World Economic Forum, "The Future of Financial Infrastructure", 2016.08.

[04] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

[05] 금융보안원, "국내외 금융분야 블록체인(Blockchain) 활용 동향", 2015.11.

[06] 금융보안원 보안연구부 기술팀, "블록체인 및 비트코인 보안 기술", 2015.11.

[07] 금융보안원 핀테크보안팀, "비트코인 신뢰 구조와 이중 지불 위협", 2016.01.

[08] 한국전자통신연구원, "주요 간편결제 서비스의 보안성 비교 분석", 2015.10.

[09] Ion Stoica, Rober Morris, David Karger, M.Frans Kaashoek, Hari Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications", Proc. of the 2001 ACM SIGCOMM Conf., 2001.08.

[10] Terri Bradford, William R. Keeton, "New Person-to-Person Payment Methods: Have Checks Met Their Match?", 2012.11.