확장성을 고려한 오프라인 암호화폐 기반의 거래 시스템 설계 및 구현

이재현[1], 이재민[2], 김동성*
금오공과대학교 IT융복합공학과
{leejaehyun[1], ljmpaul[2], dskim*}@kumoh.ac.kr

Design and Implementation of Transaction System Based on Offline Cryptocurrency Considering Scalability

Jae-Hyun Lee, Jae-Min Lee, Dong-Seong Kim
Kumoh National Institude of Technology Dept. of IT Convergence Eng.

요 약

본 논문은 블록체인 밖에서 암호화폐를 관리할 때, 여러 디바이스의 호환성을 고려한 Peer-to-Peer 통신으로 암호화폐를 전송하는 방식을 제안한다. 현재 암호화폐의 탈중앙화, 오픈소스, 보안성 등의 강점으로, 암호화폐 거래횟수가 급증하는 추세이다. 하지만 그로 인해 거래 완료에 요구되는 시간과 비용이 증가함에 따라 정작 서비스의 질은 떨어지게 되었다. 이를 해결하고자 암호화폐의 네트워크인 mainnet의 암호화폐를 다른 블록체인 네트워크 또는 오프라인에서 토큰을 거래하고 이후 mainnet의 블록체인에 오프라인 거래 전후의 데이터에 연속성이 성립하도록 하는 Layer2 연구가 진행되었다. 하지만 이러한 연구에서는 mainnet 밖의 영역, off-chain영역에서 오프라인 토큰을 주고받는 시스템에 대한 연구가 미진하였고, 이에 대해 본 논문에서 off-chain영역에서 타 플랫폼 간의 통신 확장성을 고려한 오프라인 토큰 거래 시스템을 제안하고자 한다.

Ⅰ. 서 론

암호화폐는 블록체인 네트워크에서 원장의 구조인 블록을 생성하는 연산작업에 대한 보상으로 제공되기도 하며, 생산에 제한이 있어 희소성을 인정받아 가상화폐로 동작하고 있다. 또한, 블록체인 구조의 특성상 거래를 오픈된 코드를 통해 안전함을 보이고, 자동화하여, 중개하는 특정 기관 없이도 신뢰성 있는 전자거래를 가능하게 한다. 이러한 이점으로, 암호화폐 거래횟수는 급증하고 있다[1]. 하지만 이에 대한 부작용으로 거래가 완료되는데 걸리는 시간이나, 블록을 생성하는데 요구되는 비용인 gas fee 또한 증가함을 보였다. 블록체인에서 거래기록의 무결함과 기록의 연속성을 보장하기 위해 거래기록을 블록체인 구조로 만드는 연산작업을 하는데, 실제로 작업을 실행하는 Miner 노드들에게 과부하가 걸리면 블록 생성 마이너가 선택하는 거래 또한 계속해서 지연이 생기며, miner노드가 요구하는 gas fee가 급증하는 형태를 보인다. 또한 일정량 이하의 gas fee를 제한한 경우에는 어떠한 miner노드도 해당 거래를 블록화하는데 지속해서 후위의 우선순위를 지정하게 되는 starving 현상이 나타난다.

이러한 문제점을 해결하고자 실제 암호화폐 데이터가 거래되는 mainnet에서 일부 암호화폐를 mainnet 외부, off-chain에서 다룰 수 있도록 가공하여 서비스를 제공하는 연구가 진행되었다. mainnet인 on-chain에서는 많은 트래픽이 발생하는 만큼 블록체인 구조를 생성하는데 시간적, 금전적 비용이 많이 든다. 하지만 on-chain에서 필요한 정보들만을 off-chain 환경으로 추출하여 다룬다면 같은 블록체인의 구조를 가지므로 블록체인의 무결성, 보안성, 투명성 및 안정성 특징을 그대로 지니며, on-chain 보다 낮은 거래량을 가져 블록체인 구조를 운용하는 비용이 감소하게 된다. 그리고 향후 off-chain으로 가져온 데이터는 실제 가치를 위해 on-chain으로 다시 불러온다. off-chain에서는 이 시점만을 잘 고려한다면, on-chain에서 사용되는 합의 알고리즘, 블록 데이터 구조에서 안정성을 위해 속도나 비용을 희생한 부분을 off-chain에서는 on-chain보다 예측가능한 사용자들이 사용하는 네트워크이므로, 구조나 알고리즘 선정에 선택의 폭이 더 넓다. 또한 AI등 추가적인 알고리즘을 도입하는 등의 자유도가 너 넓다고 할수 있다.[2]

off-chain환경으로는 private 블록체인 네트워크를 구성하는 경우도 있었으며[3], 더 극한으로 가서 오프라인 환경에서 두 디바이스간의 데이터 통신으로 off-chain 환경을 구축하는 연구도 진행되었다[1]. 특히 오프라인에서 두 디바이스간의 통신으로 블록체인의 가상자산을 거래한다는 부분에서 지금까지는실제 현금이 카드 등 온라인 자산으로 이동하는 경우였다면, 이 접근은 온라인 자산이 오프라인으로 이동하는 방향의 접근법이다. 온라인 자산의 장점인 편리함을 유지하되, 네트워크 인프라가 없어도 거래가 가능한 오프라인 거래의 장점을 동시에 가지는 방법이라 할 수 있다. 하지만 이러한 연구들에서는 오프라인 거래하는 방식에 대해서는 실용성이 미진함을 보였다. 이를 본 논문에서 블록체인 자산을 오프라인에서 거래할 때 실용성 및 확장성에 초점을 둔 거래 시스템을 제안하고자 한다.

Ⅱ. offchain 환경으로 오프라인을 택하는 경우

그림1에서 offchain환경으로 오프라인을 채택하여 온라인 자산을 오프라인 토큰으로 생성하며 이를 거래하는 구조를 보인다. 기존의 논문들에서는 오프라인 토큰을 전달하는데 블루투스, NFC 및 와이파이 통신을 사용한 전달방식을 고려하여 토큰 전달 시스템을 제안했다. 하지만 기존 방식들의 경우에는 개발자가 IOS 기기의 NFC 자원에 접근이 어려운 점, IOS 기기와 Android기기간의 블루투스 호환이 힘들하는 점을 고려하지 않았

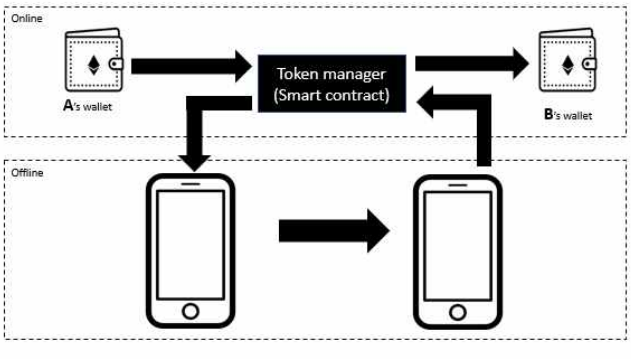

그림 1. 오프라인 토큰 생성 및 거래 구조도

다. 오프라인 환경에서 거래하는 만큼 해당 구조에서는 디바이스간의 통신의 중요성이 높다. 특히 오프라인 통신에서 데이터의 무결성과 보안성은 무엇보다 먼저 고려되어야 한다.

Ⅲ. 제안하는 오프라인 토큰 전달방법

기기에 저장되는 오프라인 토큰 정보는 오프라인 토큰을 소유한다 말할 수 있는 해시값, 해당 해시값에 연결된 암호화폐 값 그리고 on-chain에 저장할 때 정보의 연속성을 만족하기 위한 주소정보가 있다. 실제로 거래에서는 해당 데이터가 전송되며, 전송간에 데이터가 공격자에게 스니핑 공격에 대한 방비책으로, 간단한 암호화가 필요하며, 본 논문에서는 구현이 쉽고 대부분의 라이브러리에서 호환되는 AES-256 대칭키 알고리즘을 채택했다. 암호화키는 두 개로 나누어 관리하며, 암호화 및 복호화가 필요할 때 조합하여 사용함으로, 응용파일 역공학으로 키를 탈취 당하는것에 대해 일부 저항을 한다.

또한, 오프라인 토큰을 주고받을 때, 송신자는 수신자가 수신했음을 확인하고 자신의 디바이스에서 토큰정보를 제거 또는 무효화 해야하며, 수신자는 데이터를 수신하고 송신자의 디바이스에서 토큰 정보가 제거 또는 무효화됨을 확인 할 수 있어야 한다. 송수신자 중에 악의를 가지고 토큰정보가 송신함에도 토큰정보를 디바이스에 남겨두고 사용할 수도 있고, 수신을 완료했음에도 수신받지 못했다고 송신자에게 알리는 방식으로 공격할 수 있다.

이에 대한 방비책으로 TCP의 3-way Handshake를 응용하여 신뢰성 있는 토큰 전달 구조를 설계하였다.

Data(1)	Hex, 64bit		
	TH(Token Head), 32bit	AH(Address Head), 32bit	
Data(2)	Hex, 80bit		
	TH(Token Head), 32bit	AH(Address Head), 32bit	Salt code, 16bit
Data(3)	Hex, 80bit		
	TT(Token Tail), 32bit	AT(Address Tail), 32bit	Encoded Salt code, 16bit
Token	Hex, 64bit		
	TH(Token Head), 32bit	TT(Token Tail), 32bit	
Address	Hex, 64bit		
	AH(Address Head), 32bit	AT(Address Tail), 32bit	

표 1 오프라인 토큰값 전달에 생성되는 DATA1,2,3의 구조

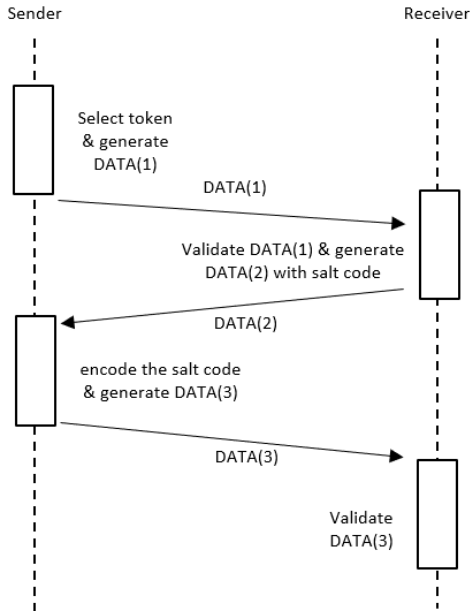

그림 2. TCP의 3-way HandShake를 응용한 오프라인 토큰 전달 방식

Ⅳ. 결론

본 논문에서는 확장성 및 실용성을 고려한 오프라인 환경에서 암호화폐를 거래하는 시스템을 설계하였다. 이를 통해 블루투스나 와이파이, NFC와 같이 설치된 통신규격이 맞지않는 디바이스간에서도 메시지 통신이나 QR코드와 같은 이미지 기반의 통신에서는 어떤 디바이스와도 오프라인 토큰교환이 가능하도록확장성에 고려하여 설계하였다. 또한 offchain에서 중요한 데이터의 연속성과 보안성을 고려하여 3-way handshake를 사용하여 적용해, 스니핑이나 스푸핑과 같은 악의적인 공격에 대처할 수 있는 구조를 설계하였다.

ACKNOWLEDGMENT

이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원사업 (2018R1A6A1A03024003), 정부(과학기술정보통신부)의 재원으로 한국연구재단 (NRF-2022R1I1A3071844), 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT연구센터지원사업의 연구결과로 수행되었음"(IITP-2023-2020-0-01612).

참 고 문 헌

[1] Ikechi Saviour Igboanusi, Kevin Putra Dirgantoro, Jae-Min Lee, Dong-Seong Kim, Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture, ICT Express, Volume 7, Issue 3, September 2021, Pages 327-334

[2] Prabhat Kumar, Govind P.Gupta, Rakesh Tripathi, "TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning",Journal of Systems Architecture, Volume 115, May 2021, 101954

[3] Lin Zhong, Qianhong Wu, Jan Xie, Jin Li, Bo Qin, "A secure versatile light payment system based on blockchain", Future Generation Computer Systems, Volume 93, April 2019, Pages 327-337