미래사회
Journal of Future Society
2024. Vol. 15, No. 3, 231~244.
https://doi.org/10.22987/jifso.2024.15.3.231

지속 가능한 블록체인 소액 결제 시스템

신 영 아* **천 지 영**** **노 건 태*****

고려대학교 **서울사이버대학교**

본 논문에서는 시스템의 지속성을 보장하는 블록체인 기반 다자간 소액 결제 시스템을 제안한다. 기존 블록체인 기반 다자간 소액 결제 시스템의 경우 시스템 참여자로 하여금 블록체인 외부에서 발생하는 중간 거래 내역을 검증하기 위해 주기 내 최소 한번 이상 온라인 상태이어야 함을 요구한다. 그러나, 블록체인 기반 소액 결제 시스템은 본질적으로 소액 거래 당사자 혹은 사물인터넷 기기와 같은 저사양 기기를 참여 노드로 전제하므로, 연속적인 온라인 상태 유지는 시스템 참여의 제한 요인이 될 수 있다. 본 논문에서는 이에 주목하여 온라인 부담 의무를 경감시키는 새로운 참여개체인 모니터링 참여자를 도입하였으며, 이로 인해 블록체인 환경에서도 거래 수수료의 부담없이 소액 결제를 실현할 수 있도록 설계하였다. 제안하는 시스템은 안전성 측면에서 시스템 참여자의 잔액 안전성과 시스템 지속성을 보장한다.

주요어 : 블록체인, 확장성, 오프체인, 소액 결제 시스템

* 주저자: 신영아/고려대학교 정보보호대학원 정보보호학과 대학원생/서울시 성북구 안암로 145 로봇융합관 404호
/Tel: 02-3290-4258/E-mail: yashin95@korea.ac.kr
** 공동저자: 천지영/서울사이버대학교 인공지능학과 조교수/서울시 강북구 솔매로 49길 60
/Tel: 02-944-5543/E-mail: jychun@iscu.ac.kr
*** 교신저자: 노건태/서울사이버대학교 빅데이터·정보보호학과 부교수/서울시 강북구 솔매로 49길 60
/Tel: 02-944-5542/E-mail: gnoh@iscu.ac.kr

Ⅰ. 서론

4차 산업혁명의 핵심 기술인 블록체인은 비트코인, 이더리움 등의 암호화폐를 기반으로 한 가상자산 시장의 근본 기술이다. 블록체인 기술은 모든 거래 내역이 동일한 원장에 기록되며, 그 원장은 투명하게 공개된다. 동일한 원장은 시스템 참여자 모두가 확인할 수 있어 접근성 측면에서 가용성이 높다고 평가된다. 특히, 동일한 원장을 공유하기 위해 모든 참여자는 합의(Consensus) 과정에 참여할 수 있으므로 원장 결정의 권한이 탈중앙화되어 시스템의 신뢰도도 높다고 말할 수 있다.

이와 같은 이유로 블록체인은 미래 금융 산업의 혁신을 주도하는 전망 높은 기술임에도 불구하고(경정익, 2021), 확장성의 한계로 상용화 문제에 봉착하고 있다. 확장성 문제란, 처리 단위인 트랜잭션의 발행량이 증가할수록 처리 속도가 저하되는 문제를 주로 일컫는다. 또한, 확장성 문제는 거래 수수료에 의해서도 발생된다. 트랜잭션마다 요구되는 거래 수수료는 사용자의 비용 부담으로 인해 블록체인 기술 상용화의 장애 요인이 될 수 있다. 이는 소액 거래를 빈번히 실현하는 소액 거래 당사자 및 사물인터넷(IoT, Internet of Things) 기기에 특히 적용된다. 일례로, 매월 결제하는 OTT(Over The Top) 서비스나 사물인터넷 환경에서 기기 간 데이터 거래가 빈번하게 발생할 경우가 해당한다.

최근까지 블록체인 분야에서 다양한 관점에서 확장성 문제를 해결하기 위해 많은 연구가 진행되고 있다. 특히 2015년에는 블록체인 시스템에서 소액 거래를 실현하고자 하는 사용자들의 거래 수수료 부담을 없애고자, 블록체인 기반 소액 결제 기술(Payment Channel)이 제안되었다. 거래 초기에 거래 당사자 간 블록체인 트랜잭션을 발생하고, 블록체인 외부(오프체인)에서 소액 거래를 다수 실현한 뒤, 거래 당사자의 최종 잔액만 블록체인 트랜잭션으로 저장하는 원리를 따른다. 이를 통해 소액 거래 당사자는 거래 건수마다 실거래 금액보다 더 많이 발생하는 블록체인 거래 수수료를 최소화할 수 있으므로 거래 수수료 관점에서 확장성의 장점을 갖는다.

그러나, 블록체인 기반 소액 결제 기술 및 시스템은 오프체인에서 다수의 중간 거래를 실현하기 때문에 참여자는 연속적으로 중간 거래 내용들을 확인하기 위해 온라인 상태이어야 함을 전제한다. 그러나, 해당 기술은 본질적으로 시스템 참여 개체를 저비용 거래 대상자 및 경량화된 기기를 가정하고 있어, 연속적인 온라인 참여는 부담될 수 있으며, 궁극적으로 시스템 지속성을 저하하는 요인이 된다.

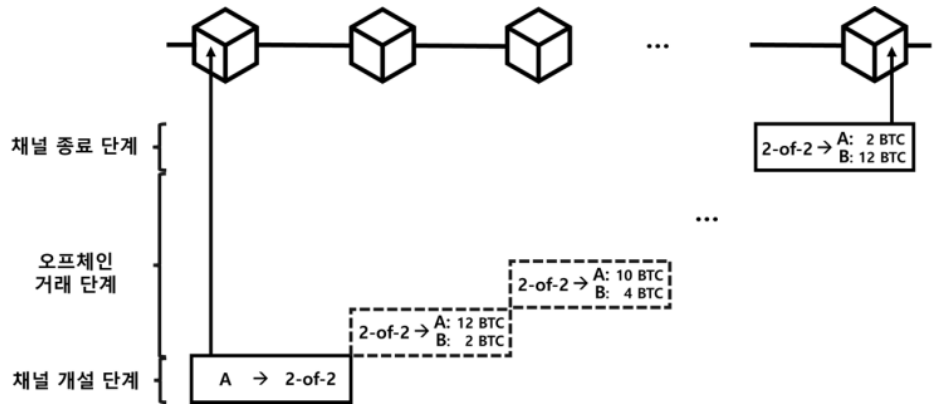
이에 따라, 본 연구는 블록체인 기반 소액 결제 기술 및 시스템 관련 선행연구에서 본연적으로 내재하던 참여자의 온라인 부담 문제를 해결하는 새로운 시스템을 제안한다. 제안하는 시스템은 소액 거래 당사자 및 저사양 기기들의 온라인 부담을 경감시킬 수 있는 새로운 참여 개체를 도입하여 블록체인 기반 금융 시장의 활성화를 확장성 문제없이 도모하고자 한다. 새롭게 참여하는 개체는 기존 참여자를 대신하여 중간 거래 내역들을 지속적으로 관찰(모니터링)하며, 모니터링을 하는 대가로 일정 보상을 시스템 이용자로부터 받아 시스템 참여 동기를 확보한다.

Ⅱ. 선행연구

본 장에서는 제안 시스템의 배경 기술인 블록체인 기반 소액 결제 기술 및 시스템에 관해 설명하며, 이미 선행연구에서 내재하는 한계점에 대해 분석한다. 이후, 본 시스템에서 사용하는 다중 서명 기법에 대해서도 살펴본다.

1. 블록체인 기반 양자 간 소액 결제 기술

블록체인 기반 소액 결제 기술(Payment Channel)

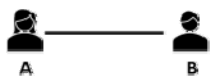
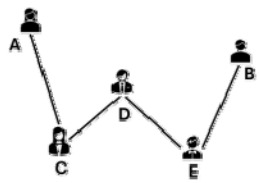
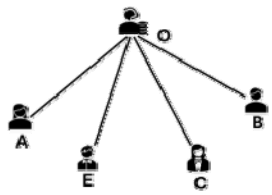


[그림 1] 지불 채널 기술 작동 단계

은 참여자의 수에 따라 양자 간 및 다자간으로 분류 가능하며, 양자 간 기술로부터 기술이 발전되기 시작하였다. 블록체인 기반 양자 간 소액 결제 기술은 비트코인 암호화폐 시스템에서 처음으로 제안되었다(C. Decker, 2015, J. Poon, 2016). 블록체인 시스템의 경우 처리량(Throughput) 및 거래 수수료(Transaction Fee)의 관점에서 확장성의 한계가 존재한다. 특히, 블록체인 기술의 이점으로 암호화폐를 사용하려는 일반 사용자의 경우 거래 금액이 소액일 경우 하나의 트랜잭션을 발행할 때 요구되는 거래 수수료가 거래 금액보다 크게 발생하여, 블록체인 시스템의 활용 의사가 저해될 수 있다. 소액 결제 기술은 이러한 한계점을 인식하여 지속적으로 소액 거래를 실현하려는 사용자의 거래 수수료 발생을 최소화함으로써 블록체인 확장성 문제를 해결하고자 한다. 사용자는 블록체인 시스템에 거래 초기와 마지막 시점에만 블록체인 트랜잭션을 발생시켜, 거래 완료 후 최종적인 잔액 정보만 블록체인 시스템에 저장하여 거래 수수료를 절감한다.

블록체인 기반 양자 간 소액 결제 기술은 [그림 1]과 같이 초기에 양자 간 거래 금액을 예치하는 채널 개설(Channel Open) 단계와 오프체인에서 수행하는 거래(Trading) 단계, 블록체인 외부에서 소액 거래를 실현한 후 최종 거래 결과 내역을 저장하는 채널 종료(Channel Close) 단계로 구성된다. 채널 개설 단계에서는 송신자가 자신과 수신자의 공개키를 바탕으로 생성한 2-of-2 다중서명(Multisig) 주소에 블록체인 외부인 오프체인 거래 단계에서 사용할 금액을 송신하는 트랜잭션을 생성하여 블록체인에 배포한다. 이후 거래 단계에서는 일정 시간 동안 오프체인 환경에서 2-of-2 다중 서명 주소로부터 매 거래 내역을 바탕으로 송신자와 수신자의 주소의 잔액을 지속적으로 업데이트 한다. 일정 시간이 지난 후, 거래가 완료되면 가장 마지막으로 생성한 트랜잭션을 블록체인에 저장함으로써 채널을 종료한다. 지불 채널 기술은 송신자와 수신자의 잔액에 대한 안전성을 보장하기 위해 오프체인 거래를 수행하기 전 수신자가 서명을 진행하지 않을 경우의 상황을 대비하여 환불(Refund) 트랜잭션을 먼저 생성 및 서명한다.

양자 간 소액 결제 기술을 확장하면 하나의 네트워크를 구성할 수 있다. 소액 결제 네트워크(Payment Channel Network)는 [그림 2]와 같이 거래 송신자 A와 수신자 B가 직접적으로 연결되어 있지 않더라도, 구축된 채널들을 활용하여 거래를 수행할 수 있다. 그러나, 소액 결제 네트워크의 경우, 중간자 노드(사용자)를 거쳐 거래를 실현하기 때문에 중간자 노드에 대한 거래 수수료가 발생한다는 단점이 존재한다.

구분	블록체인 기반 양자간 소액 결제 기술	블록체인 기반 양자간 소액 결제 네트워크	블록체인 기반 다자간 소액 결제 시스템
아키텍처			
온라인 요구사항	O	O	O
온라인 시간	연속적	연속적	주기 별 최소 1회

[그림 2] 선행연구 기술 비교

2. 블록체인 기반 다자간 소액 결제 시스템

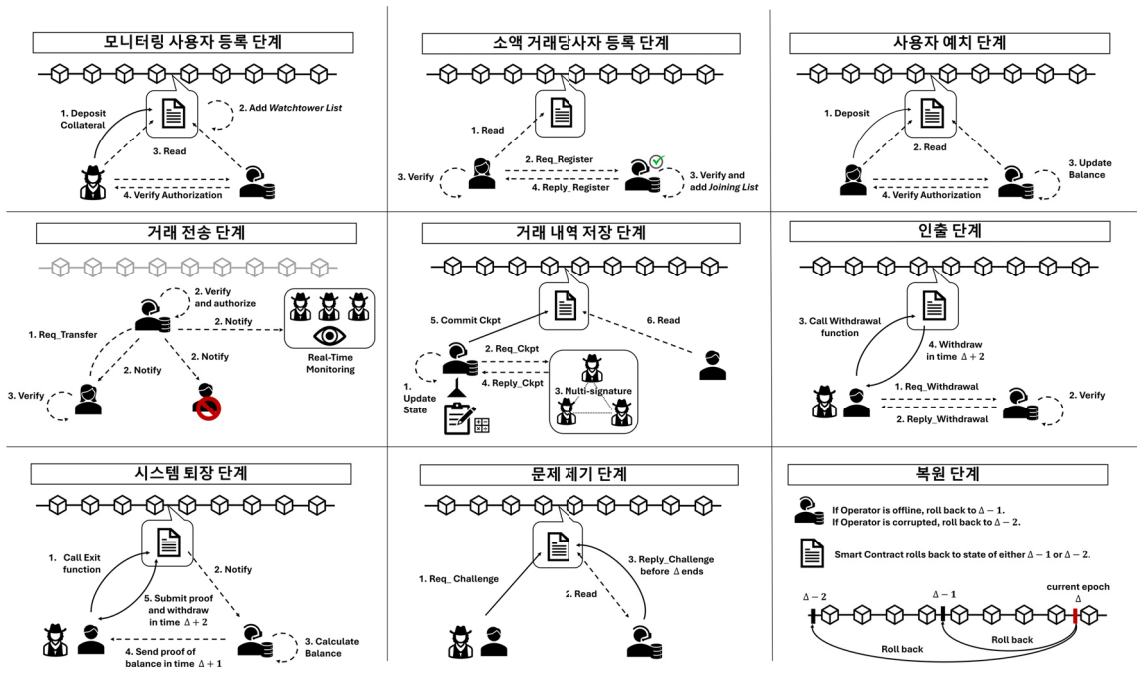
블록체인 기반 다자간 소액 결제 시스템은 양자간 소액 결제 기술 및 네트워크의 단점을 개선하여 확장된 시스템이다. 본 연구의 바탕이 되는 다자간 소액 결제 시스템은 하나의 중앙화된 노드를 바탕으로 다수의 노드가 연결하여 하나의 채널을 구축한다. 이 시스템은 주로 이더리움 환경에서 다수 활용되고 있으며 Commit-Chains라는 개념으로 제안되었다 (R. Khalil, 2018). 기존 양자간 소액 결제 기술 및 네트워크와 달리 동일 중앙화 노드에 연결된 참여자는 중간자 노드에 대한 별도의 거래 수수료 지출 없이 연결된 모든 참여자에게 거래 금액을 전송할 수 있으므로 효율적이다. 이후 최근까지 시스템의 효율성 및 중앙화 문제를 개선하기 위해 다수의 연구가 지속적으로 제안되고 있다 (Y. Ye, 2021, Z. Ge, 2023, J. He, 2024)

한편, 블록체인 기반 양자 간 및 다자간 소액 결제 시스템은 모두 시스템 참여자가 모두 블록체인 외부에서 실행한 거래 내역에 대해 확인하기 위해 최소 한 번 이상 온라인이어야 한다는 요구사항이 존재한다. 그러나, 해당 시스템을 이용하는 사용자는 대게 소액 거래 당사자이며, 경량화된 기기를 사용하여 블록체인 기반 시스템을 참여할 가능성이 높다. 이를 미루어 보아 본 연구는 참여자에게 요구되는 온라인 부담을 최소화하는 것이 선행기술의 사용성을 높일 수 있을 것으로 예측한다. 이에 따라, 온라인 부담을 경감할 수 있는 새로운 블록체인 기반 다자간 소액 결제 시스템을 제안한다.

3. 다중 서명 기법

본 연구는 소액 거래 당사자의 온라인 부담을 경감하기 위해 모니터링 참여자를 도입하여 새로운 시스템을 제안한다. 모니터링 참여자는 일정 수(최소 3명) 이상으로 구성되어야만 거래 내역의 진위성을 검증할 수 있으므로, 본 연구에서는 모니터링 참여자를 대상으로 다중 서명 기법을 활용한다.

다중 서명 기법은 다음과 같은 알고리즘으로 구성된다.



[그림 3] 제안하는 블록체인 기반 다자간 소액 결제 시스템

- 시스템 설정 단계(Setup): 보안 파라미터 1^k를 입력받아 다중 서명 값을 생성할 때 필요한 시스템 파라미터인 pp를 출력한다.
- 키 생성 단계(KeyGen): 시스템 파라미터 pp를 입력받아 사용자 $i(1 \leqq i \leqq n)$의 개인키 sk_i와 공개키 pk_i를 생성한다.
- 다중 서명 생성 단계(Sign): 각 사용자는 자신의 키 쌍과 모든 참여자의 공개키 정보가 포함된 공개키 리스트 L, 동일 메시지 m를 입력하여 부분 서명 값 σ_i를 생성하고, 참여자 간 상호작용을 통해 최종적인 다중 서명 값인 σ를 출력한다.
- 다중 서명 검증 단계(Verify): 시스템 파라미터 pp, 공개키 리스트 L, 메시지 m, 다중 서명 값 σ을 입력받아 누구나 검증을 수행하여 검증이 통과하면 1 또는 0을 출력한다.

Ⅲ. 제안 시스템

본 장에서는 일반적인 사용자 혹은 소형 기기들도 블록체인 시스템을 사용하면서도 거래 수수료 부담 없이 소액 거래를 지속적으로 수행할 수 있는 결제 시스템을 제시한다. 제안하는 시스템은 일반적인 인터넷 결제 시스템과 비교하여 전체 시스템의 신뢰성을 확보한다. 모든 참여자가 발행한 거래 내역을 누구나 확인할 수 있으며, 그 내역은 모든 사람으로부터 검증되었기 때문이다. 제안하는 시스템은 일반적인 블록체인 시스템을 활용할 때 요구되는 거래 수수료 부담 문제 또한 해결한다. 모든 소액결제를 블록체인 시스템에서 실현하는 대신, 초기 거래 내역과 최종적인 거래 내역만을 블록체인 시스템에 저장함으로써 전체 거래 횟수에 따른 총 거래 수수료보다 현저히 적게 발생한다. 이에 따라, 단순 블록체인 기술을 활용했을 경우와 비교하여

비용 효율적이다. 마지막으로, 제안하는 시스템은 기존 블록체인 시스템을 활용한 소액 결제 시스템과 비교하여 시스템 지속가능성의 이점을 갖는다. 현재까지 제안된 블록체인 기반의 소액 결제 시스템은 거래 당사자가 반드시 한 주기 내에 최소한 한 번 이상은 온라인이어야 함을 요구한다. 이는 한 주기 동안 자신에게 발생한 거래 내역들을 최소한 한 번은 확인해야 다음 주기에 거래 내역을 바탕으로 최종적인 잔액 정보를 갱신할 수 있기 때문이다. 본 시스템은 이러한 모니터링 서비스를 제공하는 참여자를 새로이 도입하여 온라인 의무 부담 역시 제거하고, 궁극적으로 시스템 전체의 지속 가능성을 확보하고자 한다. 특히, 모바일 디바이스, 저사양 기기 등을 다수 사용하는 일반적인 사용자도 시스템을 지속적으로 사용할 수 있다.

제안하는 블록체인 기반 다자간 소액 결제 시스템은 참여 개체의 유형은 네 가지로 분류된다.

- 운영자(Operator): 일반 사용자 또는 기기에 서비스를 제공하는 개체이다. 모든 소액 거래 당사자가 거래 전송 단계에서 실시간으로 생성하는 거래를 주도하여 처리한 후 이를 바탕으로 참여자의 최종적인 잔액 정보를 계산한다. 운영자는 중앙화된 개체지만, 시스템 참여자들에 의해 반드시 신뢰받는 개체는 아니다. 만약, 악의적인 행동을 수행할 경우, 해당 사실이 적발된다면 전체 시스템의 복원 과정을 수행한다.
- 소액 거래 당사자(Transacting Party): 전체 시스템을 참여하는 일반 사용자 또는 기기이며, 운영자의 주도로 블록체인 외부에서 소액 거래를 다수 실현한다. 일반 사용자 또는 기기는 언제든지 주기 단위로 참여 및 탈퇴할 수 있으며, 운영자가 올바르지 않은 행동을 수행할 시 블록체인 스마트 컨트랙트를 통해 문제를 제기할 수 있다.
- 스마트 컨트랙트(Smart Contract): 블록체인 시스템인 이더리움 환경에서 다양한 계약(프로그래밍)을 할 수 있는 코드이다. 어떠한 입력 값이 주어졌을 때, 스마트 컨트랙트는 사전에 배포된 계약 조건에 의해 실행되고, 결과를 출력한다.
- 모니터링 사용자(Monitoring Party): 블록체인 기반 다자간 소액 결제 시스템에서 소액 거래 당사자를 대신하여 거래 사실을 해당 주기 동안 지속적으로 확인하는 개체이며, 검증의 신뢰 확보를 위해 주기마다 일정 수 이상의 인원이 참여해야 한다. 모니터링 사용자는 모니터링의 역할을 적절히 수행할 시 이에 대한 보상을 모든 참여자들의 제공한 시스템 이용료로부터 수령한다. 또한, 모니터링 사용자가 악의적인 행동을 수행할 가능성을 고려하기 위해 초기 시스템을 참여할 시 일종의 담보물(금액)을 스마트 컨트랙트에 사전 예치하고, 발각될 시 그 금액을 일반 사용자 또는 운영자에게 전송한다.

전체 시스템은 대표적으로 블록체인 프로토콜과 블록체인 외부 네트워크에서 동작하는 오프체인 프로토콜로 구성된다. 블록체인 시스템 네트워크는 비동기식 네트워크(Asynchronous Network) 환경이며, 블록체인 시스템에는 사용자의 등록 및 탈퇴, 금액 예치, 시스템 상태 복원을 수행하는 기능이 기술된 스마트 컨트랙트가 배포된다. 본 연구에서는 이더리움과 같이 튜링 완전성(Turing Completeness)을 보장하는 블록체인 시스템 위에서 동작하며, 사용되는 암호 기술은 모두 암호학적으로 안전(Cryptographically Secure)하다고 가정한다. 또한, 제안하는 시스템은 블록체인 시스템 내부 프로토콜의 수정 없이 동작할 수 있으므로, 본 연구의 안전성은 블록체인 시스템에 종속된다.

블록체인 외부 네트워크인 오프체인 프로토콜은 동기식 네트워크(Synchronous Network) 환경이며, 동일 간격의 시간 주기(Δ)를 바탕으로 동작한다.

이에 따라, 모든 사용자는 공유된 시간 값과 현재 속한 주기 정보를 알고 있다고 가정한다. 또한, 통신 지연에 대해서는 지연 시간의 상한값(δ)을 정의하여 오프체인에서 메시지를 전송하는 시간과 실제 블록체인 시스템에 해당 메시지가 저장되는 지연 시간을 고려한다.

본 논문에서 제안하는 블록체인 기반 다자간 소액 결제 시스템은 다음과 같은 안전성 목표를 가진다.

- 잔액 안전성(Balance Security): 악의적인 시스템 참여자가 존재하더라도 정당한 참여자의 잔액은 탈취 혹은 손실되지 말아야 함을 뜻한다. 본 시스템은 모든 참여자들이 시스템 참여를 위해 사용 금액 혹은 담보물을 예치하는 과정을 사전에 요구되나, 해당 금액 또는 송수신 금액에 대한 안전성을 보장하는 것을 목표로 한다.
- 시스템 지속성(System Liveness): 시스템 참여자 중 악의적인 사용자가 있어도, 해당 시스템이 정상적으로 운영되어야 한다는 것을 의미한다. 본 시스템은 주기마다 반복되며, 주기가 끝난 후에는 운영자가 거래 결과를 집계하여 참여자의 잔액 정보를 갱신한다. 이 과정에서 참여자가 응답이 없거나, 잘못된 정보를 운영자에게 전달한다면 시스템의 동작이 멈추고, 일정 시간 동안 시스템이 진행되지 않을 수 있는 위협이 존재한다. 본 연구에서는 시스템이 지속적으로 정상적인 운영을 수행할 수 있도록, 모니터링 참여자들을 새로이 도입한다.

다음으로, 전체적인 시스템 동작 과정을 설명한다. 본 시스템은 크게 등록 단계, 예치 단계, 거래 전송 단계, 거래 내역 저장 단계, 인출 단계, 시스템 퇴장 단계, 문제 제기 단계, 복원 단계로 구성된다. [그림 3]은 전체 동작 과정을 도식화한 그림이다. 제안 시스템은 선행 연구인 NOCUST (R. Khali, 2018)의 동작 과정을 바탕으로 모니터링 개체들을

<표 1> 제안 시스템에서의 기호 설명

기호	설명
$\rightarrow$	블록체인 통신
$\dashrightarrow$	오프체인 통신
$SC_{Deposit}$	예치 컨트랙트
$SC_{Withdraw/Exit}$	인출 컨트랙트
$SC_{Challenge}$	문제 제기 컨트랙트
$SC_{Recovery}$	거래 복원 컨트랙트
e	주기 정보
$\boldsymbol{P(e)}=\{P_1(e),...,P_n(e)\}$	주기 e에서의 참여자 집합
$\boldsymbol{M(e)}=$ $M_1(e),...,M_m(e)\}$ $(m \geq 3)$	주기 e에서의 모니터링 참여자 집합
O	운영자
$collateral_{P_i}(e)$, $collateral_{M_j}(e)$	주기 e에서의 각 참여자의 담보액
$bal_{P_i}(e)$	주기 e에서의 각 소액 거래 당사자의 잔액
$penalty_O(e)$, $penalty_{M_j}(e)$, $penalty_{P_i}(e)$	주기 e에서의 각 참여자의 벌금
$deposit_{P_i}(e)$	주기 e에서의 각 소액 거래 당사자의 초기 예치금
$t_{root}(e)$	O에 의해 계산되는 주기 e의 잔액 정보 업데이트
$\sigma_{M_j}(e)$	주기 e 내 잔액 정보 업데이트에 대한 j번째 모니터링 참여자의 서명 값
$\sigma_{\boldsymbol{M}}(e)$	주기 e 내 잔액 정보 업데이트에 대한 모든 모니터링 참여자의 서명 값
$withdraw_{P_i}(e)$, $withdraw_{M_j}(e)$	각 참여자가 $SC_{Withdraw/Exit}$에 요청하는 인출 요청 메시지
$exit_{P_i}(e)$, $exit_{M_j}(e)$	각 참여자가 $SC_{Withdraw/Exit}$에 요청하는 퇴장 요청 메시지
$challenge_{P_i}(e)$, $challenge_{M_j}(e)$	각 참여자가 $SC_{challenge}$에 요청하는 문제 제기 요청 메시지

새롭게 정의하였으며, 모니터링 사용자로 하여금 오프라인 사용자 대신 거래 사실들을 확인하게 함으로써 주기 내 최종 거래 결과의 정당성을 부여하고자 한다. 전체 시스템에서 사용하는 수식에 대한 설명은 <표 1>과 같다.

1. 시스템 설정 단계

본 시스템의 서비스 제공자인 운영자는 블록체인 시스템에 사용될 스마트 컨트랙트를 배포한다. 이때 배포되는 스마트 컨트랙트는 크게 예치 컨트랙트 $SC_{Deposit}$, 인출 및 퇴장 컨트랙트 $SC_{Withdraw/Exit}$, 문제 제기 컨트랙트 $SC_{Challenge}$, 거래 복원 컨트랙트 $SC_{Recovery}$가 존재한다. 이후 운영자는 충분한 담보액 $collateral_O(e)$을 예치 컨트랙트 $SC_{Deposit}$에 예치한 후 온라인 또는 오프라인 방식으로 스마트 컨트랙트 주소 및 설정 완료 사실을 공표한다. 그리고 소액 거래당사자 혹은 모니터링 참여자의 참여를 대기한다.

2. 등록(Register) 단계

등록단계는 소액 거래 당사자의 등록 단계와 일반 사용자인 거래 당사자 등록 단계로 분류된다. 먼저, 모니터링 사용자의 등록 단계에서는 모니터링 역할을 수행하고자 하는 j번째 참여자 $M_j(e)$가 블록체인 시스템의 스마트 컨트랙트에 일정 금액을 $collateral_{M_j}(e)$로 예치함으로써 시작된다. 모니터링 사용자의 담보액 $collateral_{M_j}(e)$은 추후 악의적으로 행동할 시 해당 사실이 스마트 컨트랙트로부터 판정되면 벌금 납부 금액으로 활용된다. 벌금액이 반영될 경우 다음 주기에서의 담보 잔액은 $collateral_{M_j}(e+1) = collateral_{M_j}(e) - penalty_{M_j}(e)$가 된다. 이후, 스마트 컨트랙트는 참여 순서대로 컨트랙트 내에 리스트 $M(e) = \{M_1(e),...,M_m(e)\}$에 저장되어, 고유 인덱스를 가지게 된다. 담보물 예치 및 리스트 저장 사실을 블록체인 시스템으로부터 확인(Read)된 시스템 운영자 O는 이후 새롭게 참여한 거래 당사자와 통신 과정을 거쳐 해당 사실에 대해 검증(Verify Authorization)한다.

소액 거래 당사자의 등록 단계는 모니터링 사용자의 등록 단계와 달리 운영자와의 상호과정을 통해 먼저 등록 과정을 시작한다. 스마트 컨트랙트에서 모니터링 참여자가 일정 수만큼 이상(최소 3명 이상)이 참여된 사실이 확인(Read)될 시 소액 거래 당사자는 오프체인 환경에서 운영자에게 등록 요청 메시지(Req_Register)를 전송한다. 등록 요청 메시지에는 참여자의 아이디와 참여 의사 등이 포함되며, 메시지에 대한 사용자의 서명도 함께 전송된다. 이를 수신한 운영자는 신규 참여자의 메시지, 서명값에 대한 검증이 완료(Verify)되면, 참여 리스트(Joining List)에 아이디를 추가한 후 응답 메시지(Reply_Register)로써 운영자의 서명값과 함께 소액 거래 당사자에게 전송한다. 운영자의 메시지 및 서명이 검증된 신규 참여자는 다음 단계인 예치 단계를 수행한다.

3. 예치(Deposit) 단계

예치 단계는 신규 참여한 소액 거래 당사자가 특정 주기에 사용할 금액을 스마트 컨트랙트에 예치하는 과정을 의미한다. 일례로, 정기적으로 거래 상점으로부터 물품을 구매해야 하거나, 넷플릭스 등의 OTT 구독 서비스를 정기적으로 이용하고 있는 신규 참여자는 송신 금액과 일정 수수료 금액을 납부할 수 있는 충분한 금액 $bal_{P_i}(e)$을 스마트 컨트랙트 $SC_{Deposit}$에 예치한다.

예치 사실을 스마트 컨트랙트로부터 확인한 시스

템 운영자 O는 예치 금액 정보를 관리 중인 오프체인 장부에 업데이트한다. 운영자의 장부에는 참여자의 블록체인 시스템 주소 $addr_{M_i}$, ID, 예치 금액 $bal_{P_i}(e)$, 현재까지 수행된 거래 내역 등을 포함한다. 정보 관리 모델은 기존 연구인 NOCUST의 Merkleized Interval Tree-Structure를 따른다(R. Khali, 2018). 이후 운영자는 새롭게 업데이트한 머클 트리 루트 해시 $t_{root}(e)$에 대해 서명하여 신규 참여자에게 전송한다. 서명자는 운영자의 서명이 올바르고, 머클 루트 증명 값이 정당하면 예치가 완료되었음을 확인한다.

4. 거래 전송(Off-Chain Transfer) 단계

본 주기에 참여 중인 소액 거래 당사자는 운영자의 도움으로 오프체인을 통해서 소액 거래를 거래 수수료 부담없이 실현할 수 있다. 등록 및 예치가 완료된 소액 거래 당사자 중 금액을 송신하려는 자 $P_i(e)$는 예치한 금액 중 일부의 금액과 수신자 정보를 바탕으로 거래 요청 메시지(Req_Transfer)에 $tx(e)$를 포함하여 생성 후 이를 서명하여 운영자 O에게 전송한다. 오프체인 거래 메시지 $tx(e)$의 형태는 다음과 같다. 해당 주기 e에서의 $sender$는 송신자의 ID, $receiver$는 수신자의 ID를 의미하며, $nonce$는 오프체인 거래의 이중 지불 방지 및 거래 내역 간의 순서를 유지하기 위하여 생성하는 고유 값을 의미한다. amt는 송신 금액, $offset$은 운영자 O가 관리하는 정보 모델인 머클 트리 구조에서 각 참여자의 잔액 시작 위치를 의미한다. 일례로, 오프체인 초기 단계에서 $bal_1(e)=5$, $bal_2(e)=9$, $bal_3(e)=3$일 때, $P_3(e)$의 $offset_{P_3}(e)$는 14, $P_4(e)$의 $offset_{P_4}(e)$는 17이다. 이후, 거래가 진행될때마다 $offset_{P_i}(e)$은 송수신 amt금액을 바탕으로 업데이트된다. 마지막으로, fee는 거래 건수마다 운영자 O에게 부담하는 거래 수수료를 의미한다.

$$tx(e)= \{e, sender, receiver, nonce, amt, offset, fee\}$$

운영자 O는 수신한 메시지를 바탕으로 송신자의 보내려는 금액이 실행될 수 있을 만큼 잔액 정보가 충분한지, 수신자의 정보가 올바르게 기입되어 있는지 등을 검증(Verify)한 후 서명을 진행하여 참여자의 잔액 정보(State)를 갱신한다. 운영자는 거래 실행 완료 및 갱신된 잔액 정보를 거래 송신자, 거래 수신자, 모니터링 참여자를 포함한 모든 시스템 참여 개체에 전파(Notify)한다. 여기서 주목해야 할 점은 제안하는 시스템에서 기존 연구인 NOCUST와 달리 모니터링 참여자 $M_j(e)$가 포함되어 있다는 것이다. 이는 실행된 오프체인 거래를 확인하기 위해 모든 참여자가 한 주기 내에 최소 한 번 이상 온라인이어야 하는 참여자의 요구사항을 완화하기 위한 것이며, 주기마다 실행된 거래의 확인 및 검증은 참여자뿐만 아니라 모니터링 개체가 대신하여 수행할 수 있다. 이러한 이유로 제안하는 시스템은 소액 거래를 실현하는 거래 당사는 일반 대중적인 사용자 또는 저사양 기기에서도 충분히 이용할 수 있는 장점이 존재한다.

5. 거래 내역 저장(State Update) 단계

본 주기에서 오프체인 거래가 모두 완료되면 시스템 운영자 O는 수행된 모든 거래 내역들을 바탕으로 모든 참여자의 잔액 정보를 업데이트(Update State) 한다. 이때, 운영자 O는 기존 연구인 NOCUST의 Merkleized Interval Tree-Structure를 활용하여 일부 거래 내역의 누락이 발생하지 않도록 머클 트리에 결합하여 저장한다. 머클 트리의 증명

값인 최종 루트 해시 값(Checkpoint, ckpt) $t_{root}(e)$를 계산한 운영자 O는 스마트 컨트랙트에 바로 저장하는 대신 모니터링 참여자에게 전송하여 내역의 검증을 요청(Req_Ckpt)한다. 기존 연구와 달리 본 연구에서 모니터링 참여자 $M_j(e)$로부터 검증 작업을 요청하는 이유는 스마트 컨트랙트에 저장된 이후 거래 내역이 유효화(Finalize)되기까지 최소 2번 이상의 주기가 지나야 하는데, 그 이전까지 허용되는 문제 제기(Challenge) 현상을 감소시키기 위함이다. 거래 전송 단계에서 운영자로부터 수신한 거래 완료 메시지를 연속적으로 확인하고 있던 모니터링 참여자 $M_j(e)$는 운영자 O가 잘못된 머클 트리 증명 값을 계산한 것이 확인되면 모든 모니터링 참여자 $M_j(e)$와의 다중 서명을 진행하지 않고, 요청의 거절 메시지(Reply_Ckpt)로 운영자에게 응답한다. 이와 반대로, 증명 값이 올바르게 계산되었음이 운영자의 증명 값에 대해 모든 모니터링 참여자 $\boldsymbol{M}$이 각각 생성한 서명 값 $\sigma_{M_j}(e)$을 바탕으로 협력하여 다중 서명 $\sigma_{\boldsymbol{M}}(e)$을 생성한다. 다중 서명은 하나의 개체로부터 받는 서명에 비해 메시지의 진위성을 신뢰성 높게 확인할 수 있다. 이는 블록체인 암호화폐에서 트랜잭션을 생성할 때 사용자가 여러 지갑을 통해서 다중 서명을 진행하는 이유와 유사하다.

일반적인 다자간 소액 결제 시스템은 블록체인에 저장되는 거래 내역의 유효화를 위해서 낙관론적인(Optimistic) 방식을 따른다. 그러나, 문제 제기를 허용하되, 사전에 모니터링 사용자로부터 추가적인 검증을 받고 거래 내역을 블록체인에 저장한다면 효율적으로 거래의 유효화(Finalization)에 기여할 수 있다.

6. 인출(Withdrawal) 단계

본 시스템에 참여하고 있던 소액 거래 당사자 $P_i(e)$ 혹은 모니터링 사용자 $M_j(e)$는 참여하는 주기 내에서 언제든지 인출 신청 $withdraw_{P_i}(e)$ 또는 $withdraw_{M_j}(e)$을 생성하여 운영자 O에게 요청할 수 있다(Req_Withdrawal). 인출 요청 메시지를 수신한 운영자는 인출 메시지 및 잔액 정보를 검증한 후 응답 메시지(Reply_Withdrawal)를 송신한다. 실제 인출은 현재 주기($\triangle$)와 다음 주기($\triangle+1$)동안 별도의 문제 제기가 없으면 그다음 주기($\triangle+2$)에 스마트 컨트랙트를 통해 실행된다. 만약 운영자의 잔액이 충분하고, 사용자가 빠른 인출을 원할 시 다음 주기($\triangle+1$) 내에 운영자의 예치된 잔액으로 사전에 인출 과정을 진행할 수 있다.

7. 시스템 퇴장(Exit) 단계

현 시스템에 참여 중인 사용자는 스마트 컨트랙트를 통해 퇴장을 진행할 수 있다. 소액 거래 당사자 $P_i(e)$ 혹은 모니터링 참여자 $M_j(e)$는 스마트 컨트랙트에 퇴장 요청 함수 $exit_{P_i}(e)$ 또는 $exit_{M_j}(e)$을 통해 호출하면(Exit), 해당 사실을 블록체인 시스템을 통해 운영자가 확인한다. 이후, 운영자 O는 탈퇴 요청을 한 사용자의 상태 정보를 확인한 후 검증 사실을 머클 트리 증명 값 $t_{root}(e)$과 함께 요청한 사용자에게 오프체인을 통해 전송한다. 운영자의 증명 값이 올바르다는 것이 확인된 사용자는 문제 제기 허용 단계가 지나고, 거래 유효화가 된 주기($\triangle+2$)에 완전히 퇴장 가능하다.

8. 문제 제기(Chanllenge) 단계

거래가 유효화되기 전에 시스템 참여자(소액 거래 당사자 $P_i(e)$ 또는 모니터링 사용자 $M_j(e)$)는 계산된 최종 잔액 정보 또는 모든 거래 내역이 저장된 머클 트리의 증명 값이 잘못 계산된 경우 블

록체인 시스템에 배포된 스마트 컨트랙트를 통해 문제 제기 $challenge_{P_i}(e)$ 또는 $challenge_{M_j}(e)$를 실행할 수 있다. 문제 제기 요청 사실(Req_Challenge)을 스마트 컨트랙트로부터 확인한 운영자는 해당 주기에 대한 증명 값을 주기 내에 스마트 컨트랙트에 저장하여 문제 제기에 대해 응답(Reply_Challenge)을 해야 한다. 만약 운영자가 제한된 시간 내에 증명 값을 저장하지 않거나, 잘못된 증명 값을 저장하거나, 응답이 없을 시 복원 단계가 진행된다. 여기서 주목해야 할 사실은 운영자 O는 반드시 신뢰하는 개체가 아니라는 것이다. 참여자는 시스템 운영자 O의 행동에 대해서 반드시 신뢰할 필요성이 없으며, 만약 운영자 O가 오프라인이거나 악의적인 행동을 수행하면 문제 제기를 통해 운영자 O에게 패널티 $penalty_O(e)$를 부과할 수 있다. 또한, 문제 제기 $challenge_{P_i}(e)$ 또는 $challenge_{M_j}(e)$를 성공한 참여자는 $penalty_O(e)$로부터 일정액의 보상 $reward_{P_i}(e)$ 또는 $reward_{M_j}(e)$을 받을 수 있다.

9. 복원(Recovery) 단계

시스템 복원 단계는 운영자 O가 오프라인이거나, 문제 제기에 대해 올바른 증명 값을 제출하지 않거나, 잘못된 거래 내역을 바탕으로 최종 잔액 정보를 업데이트할 가능성을 고려하여 해당 주기에서 갱신된 모든 거래 내역을 무효화하고, 가장 최근에 유효화된 잔액 정보로 복원(Roll Back)할 수 있다. 만약, 운영자가 오프라인인 상태로 응답이 없을 경우에는 직전 주기($\triangle+1$)의 상태(State)로 복원하게 되며, 운영자 O가 악의적인 행동을 수행했다고 판단될 시에는 가장 최근에 유효화된 상태로 복원한다. 이때, 스마트 컨트랙트는 해당 주기에 수행된 모든 거래 내역들을 무효화하므로, 이는 정당한 사용자가 수행한 거래 내역 역시 무효화될 수 있음을 뜻한다. 즉, 시스템 복원 단계는 전체 시스템 지속성(Liveness)을 보장하기 위해 가장 마지막으로 수행되어야 한다. 다시 말하면, 악의적인 참여자가 많을수록 시스템의 복원 단계가 빈번히 발생하여 지속성을 보장할 수 없다는 것을 의미한다. 본 연구는 모니터링 참여자의 개체를 추가함으로써 해당 단계의 발생 가능성을 최소화하고자 하였다.

Ⅳ. 분석

본 연구에서 제안하는 블록체인 기반 다자간 소액 결제 시스템은 시스템의 안전성(Security)과 효율성(Efficiency)의 측면에서 선행연구인 NOCUST와 비교하여 분석하고자 한다.

1. 안전성 분석

본 연구에서는 안전성(Security)의 개념을 크게 사용자 잔액 안전성(Balance Security)과 시스템 지속성(Liveness)으로 정의한다.

정의 5.1.1. 잔액 안정성(Balance Security)이란, 악의적인 시스템 참여자가 존재하더라도 정직한 참여자의 잔액은 탈취 또는 소실되지 않아야 함을 말한다.

정의 5.1.2. 시스템 지속성(Liveness)이란, 악의적인 시스템 참여자가 존재하더라도 정당한 사용자의 채널 운영이 방해받지 않아야 함을 말한다.

각 안전성 정의에 따라 분석한 결과는 다음과 같다.

정리 5.1.1. Ⅲ절에 제시된 블록체인 기반 다자간 소액 결제 시스템은 시스템 참여자의 잔액 안전성(Balance Security)을 보장한다.

증명. 제안하는 시스템은 악의적인 시스템 참여자는 정직한 참여자의 신원을 위조할 수 없음을 전제하며, 모든 참여자는 합리적인 개체임을 가정한

다. 공격자는 소액 거래 당사자 $P_i(e)$이거나, 모니터링 참여자 $M_j(e)$이거나, 운영자 O가 될 수 있다. 먼저, 소액 거래 당사자 $P_i(e)$일 경우 정직한 참여자의 잔액을 탈취하기 위해 오프체인 거래 단계에서 거래 내역을 위조하여 발행할 수 있다. 이러한 경우 연속적으로 관찰하던 모니터링 참여자는 초기 잔액 정보와 거래 전송 단계 내 운영자의 거래 완료 메시지를 통해 거래 사실을 검증할 수 있다. 또한, 공격자의 거래 당사자가 잘못된 거래 내용을 확인하면 거래 내역 저장 단계 이후 문제 제기 단계에서 거래 사실의 진위성에 대해 검증을 요청할 수 있다.

두 번째로, 모니터링 참여자 $M_j(e)$가 공격자일 경우 거래 내역 저장 단계에서 다중 서명 과정을 거부하거나, 문제 제기 단계에서 최종 상태의 진위성의 검증을 요청할 수 있다. 먼저, 거래 내역 저장 단계에서는 모니터링 참여자 $M_j(e)$가 다중 서명을 거부할 시 보상의 기회를 놓치게 된다. 이러한 경우 합리적인 참여자는 역할을 거부할 동기를 잃게 된다. 또한, 문제 제기 단계에서는 운영자 O가 올바른 증명 값을 제출하면 스마트 컨트랙트가 진위를 판단하게 되므로, 거짓된 거래 내역으로 인한 정당한 사용자의 잔액 소실은 발생하지 않는다.

마지막으로, 공격자가 운영자 O일 경우 올바르지 않은 checkpoint를 계산할 수 있다. 이러한 경우 거래 내역 저장 단계에서 모니터링 참여자 $\boldsymbol{M}$로부터 checkpoint $t_{root}(e)$에 대한 다중 서명 $\sigma_{\boldsymbol{M}}(e)$을 받을 시 거부당할 수 있으므로, 일정 시간 동안 checkpoint와 증명 값을 스마트 컨트랙트에 저장하지 못하면 이전 상태로 복원하는 단계가 수행된다. 이외에도 기타 가능성에 의해 악의적인 행동을 수행하거나, 응답하지 않을 경우 일정 시간이 지나면 이전 상태로 복원하게 되므로, 궁극적으로 시스템 참여자의 잔액 안전성이 보장된다.

정리 5.1.2. Ⅲ절에 제시된 블록체인 기반 다자간 소액 결제 시스템은 NOCUST와 비교하여 시스템 지속성(Liveness)를 보장한다.

증명. 제안하는 시스템은 기반이 되는 블록체인 시스템의 안전성에 기반하며, 모니터링 참여자 $M_j(e)$의 개체를 시스템 참여자 중에서 새롭게 정의하였다. 선행연구인 NOCUST에서는 시스템 참여자가 주기 내 온라인 상태가 아니라면 스마트 컨트랙트에 의해 이전 주기로 잔액 정보를 복원한다. 이와 달리 본 시스템은 시스템 참여자가 온라인이 아니더라도 모니터링 참여자 $M_j(e)$에 의해 참여자의 중간 거래 사실을 검증할 수 있으며, 모니터링 참여자 $M_j(e)$는 정직하게 모니터링 임무를 수행할 경우 일정 보상도 지급받게 되므로 이윤을 추구할 동기가 발생한다. 이에 따라, 궁극적으로 시스템 복원 단계의 발생 가능성을 NOCUST와 비교하여 감소시킬 수 있으므로, 본 연구는 시스템 지속성을 보장한다.

2. 효율성 분석

제안하는 시스템에서의 효율성 분석 결과는 <표 2>과 같다. <표 2>는 시스템 단계별로 발생해야 하는 블록체인 트랜잭션 개수와 오프체인 메시지 개수를 통신 복잡도 측면에서 분석한 결과이다. 표 내 n은 소액 거래 당사자 수를 뜻하며, m은 모니터링 참여자 수를 의미한다. 거래 내역 저장 단계에서는 모니터링 참여자 간 수행되어야 하는 다중 서명 값 생성 과정으로 인하여 오프체인 메시지 전송 횟수가 $3m$으로 분석된다. 이는 다중 서명 알고리즘 자체에서 Sign 단계에서 요구되는 통신 횟수를 의미하며, 초기 난수에 대한 Commitment 값을 생성 및 전파하는 과정, 부분 다중 서명 값을 전송하는 과정, 최종 다중 서명 값을 전파하는 과정을 포함한다.

효율성 분석 결과에 따르면, 궁극적으로 본 연구

<표 2> 단계별 통신 복잡도

	블록체인 트랜잭션 수	오프체인 메시지 수
모니터링 사용자 등록 단계	1	2
소액 거래 당사자 등록 단계	0	2
예치 단계	1	2
거래 전송 단계	0	$1+n+m$
거래 내역 저장 단계	1	$2+3m$
인출 단계	2	2
퇴장 단계	2	1
문제 제기 단계	2	0

에서는 일반적인 블록체인 시스템에서 결제를 수행하는 것과 비교하여 발행하는 블록체인 트랜잭션 수를 최소화하여 비용 효율성의 이점을 갖는다. 또한, 이와 동시에 모니터링 참여자가 존재하더라도 블록체인 트랜잭션 수의 증가에 큰 영향을 미치지 않는다는 것을 확인할 수 있다.

V. 결론

본 연구는 블록체인 기반 다자간 소액 결제 시스템을 제안하여 블록체인 환경에서도 거래 수수료 부담 없이 소액 거래 당사자의 시스템 이용을 활성화하고자 새로운 시스템을 제안하였다. 또한, 제안하는 시스템은 모니터링 참여자라는 새로운 개체를 도입하여 선행연구에서 존재하던 참여자의 온라인 부담 문제를 해결하고자 하였다. 또한, 기존 블록체인 시스템에서의 거래 환경과 선행연구와 비교하여 통신 복잡도 측면에서 효율성을 분석하였으며, 안전성 측면에서는 시스템 참여자의 잔액 안전성과 지속성을 보장할 수 있음을 보였다.

참고문헌

경정익, 이재웅 (2021). 제4차 산업혁명시대 부동산 분야 블록체인 수용의도에 미치는 영향요인에 관한 연구. 미래사회, 12(1), 1 - 22.

C.Deckerd & R. Wattenhofer, (2015) A fast and scalable payment network with bitcoin duplexmicropayment channels, in Proc. Symp. Stabilization, Saf., Secur. *Distrib. Syst.*, 3 - 18.

J. Poon & T. Dryja, (2016) The bitcoin lightning network: Scalable off-chain instant payments,[Online]. Available: https://lightning.network/lightning-network-paper.pdf

R. Khalil, A. Zamyatin, G. Felley, P. Moreno-Sanchez, & A. Gervais, (2018) Commit-chains: Secure, scalable off-chain payments, [Online]. Available: https://eprint.iacr.org/2018/642

Y. Ye, Z. Ren, X. Luo & J. Zhang,W. Wu, (2021) Garou: An efficient and secure off-blockchain multi-party payment hub, IEEE Transactions on. *Networking and Service Management, 18, 4.*

Z. Ge, Y. Zhang, Y. Long & D. Gu, (2023) Magma: Robust and flexiblemulti-party payment channel, *IEEE Transactions on Dependable andSecure Computing, 99,* 1 - 18.

J. He et al., (2024) An Efficient Multi-Party Payment Protocol for IoT Micro-Payments, *in IEEE Internet of Things Journal.*

투고일자: 2024. 8. 31.
심사일자: 2024. 9. 23.
게재확정일자: 2024. 9. 30.

미래사회
Journal of Future Society
2024. Vol. 15, No. 3, 231~244.
https://doi.org/10.22987/jifso.2024.15.3.231

Sustainable Blockchain-Based Multi-Party Micropayment System

Young Ah Shin Ji Young Chun Geontae Noh

Korea University Seoul Cyber University

This paper proposes a blockchain-based multiparty micropayment system that ensures the liveness of the system. Existing blockchain-based multiparty micropayment systems require participants to be online at least once per cycle to verify offchain transaction records that occur outside the blockchain. However, since blockchain-based micropayment systems inherently involve low-specification devices, such as micropayment participants or Internet of Things (IoT) devices, maintaining a constant online presence can be a limiting factor for system participation. To address this issue, this paper introduces a new type of participating entity, the monitoring participant, to reduce the burden of being constantly online. This design facilitates the realization of micropayments without having much burden of transaction fees, even in a blockchain environment. We demostrate that our proposed system provides balance security while ensuring system liveness.

Keywords: Blockchain, Scalability, Offchain, Micropayment