Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.5, Oct. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.5.1021

신뢰실행환경(TEE) 기반의 블록체인 오프라인 결제 프로토콜

정 동 현,[1†] 김 범 중,[1] 이 중 희[2‡]
[1,2]고려대학교 (대학원생, 교수)

Trusted Execution Environment (TEE)-Based Blockchain Offline Payment Protocol

Donghyun Jeong,[1†] Beomjoong Kim,[1] Junghee Lee[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

본 논문에서는 블록체인 기반 오프라인 결제를 위한 TEE-BOP(Trusted Execution Environment-Based Blockchain Offline Payment) 프로토콜을 제안한다. TEE-BOP는 신뢰실행환경(TEE) 내에서 오프라인 잔액을 안전하게 관리하고, 머클 트리를 활용해 블록체인에 기록된 초기 입금 증명을 효율적으로 검증한다. 또한, TEE Attestation을 통해 생성된 키와 시스템의 신뢰성을 보장함으로써, 오프라인 환경에서도 안전하고 무결한 거래를 가능하게 한다. 기존 연구와 달리, TEE-BOP는 중앙 기관에 대한 의존성을 제거하고 이상적인 모델을 가정하지 않음으로써, 실제 환경에서의 적용 가능성을 높였다. 본 프로토콜은 다층적 방어 메커니즘으로 이중 지불 문제를 해결하고, 수취인이 TEE와 블록체인 간의 데이터 일치를 직접 검증하는 방식으로 위조 방지 문제를 해결한다. 이를 통해 네트워크 인프라가 불안정한 지역에서도 신뢰성 있는 블록체인 기반 오프라인 결제를 가능하게 한다. 이는 본 연구가 블록체인 기술의 적용 범위를 확장하고, 개발도상국이나 재난 상황에서의 금융 서비스 접근성 향상에 기여할 수 있음을 보여준다.

ABSTRACT

This paper proposes the TEE-BOP (Trusted Execution Environment-Based Blockchain Offline Payment) protocol for blockchain-based offline payments. TEE-BOP securely manages offline balances within a Trusted Execution Environment (TEE) and efficiently verifies initial deposit proofs recorded on the blockchain using Merkle trees. Additionally, it ensures secure and tamper-proof transactions in offline environments by guaranteeing the reliability of keys and the system through TEE Attestation. Unlike previous studies, TEE-BOP enhances real-world applicability by eliminating dependence on central authorities and avoiding assumptions of ideal models. The protocol solves the double-spending problem through multi-layered defense mechanisms and addresses forgery prevention by allowing recipients to directly verify data consistency between the TEE and the blockchain. This enables reliable blockchain-based offline payments in areas with unstable network infrastructure. It demonstrates that this research can expand the application of blockchain technology and contribute to improving access to financial services in developing countries or disaster situations.

Keywords: Blockchain, Offline Payment, Trusted Execution Environment (TEE)

Received(08. 28. 2024), Modified(09. 11. 2024), Accepted(09. 11. 2024)

† 주저자, jeongdh@korea.ac.kr
‡ 교신저자, j_lee@korea.ac.kr(Corresponding author)

I. 서 론

블록체인 기술의 등장은 금융 시스템의 탈중앙화를 가능하게 하며, 전통적인 중앙화된 금융 기관의 역할을 재정의하고 있다[1]. 이 혁신적인 기술은 투명성, 보안성, 그리고 중개자 없는 거래를 제공함으로써 금융 시스템의 새로운 패러다임을 제시한다. 그러나 대부분의 블록체인 기반 시스템은 실시간 온라인 연결을 전제로 하고 있어, 인터넷 접속이 제한된 환경에서의 적용에 한계가 있다.

이와 같은 제약은 특히 개발도상국이나 농촌 지역 등 인터넷 인프라가 충분히 발달하지 않은 곳에서 블록체인 기술의 혜택을 제한하는 요인으로 작용한다[2]. 전 세계적으로 수십억 명의 사람들이 여전히 안정적인 인터넷 접속을 누리지 못하고 있으며, 이는 디지털 금융 서비스에 대한 접근성 격차를 더욱 심화시키는 원인이 된다.

이러한 맥락에서 CBDC(Central Bank Digital Currency)의 개발 동향에도 주목할 필요가 있다. 많은 중앙은행들이 CBDC 구현에 있어 블록체인 기술을 고려하고 있으며, 특히 현금과 유사한 오프라인 결제 기능을 핵심 요구사항으로 인식하고 있다[18]. 따라서, CBDC의 이러한 요구사항을 충족시키고, 동시에 인터넷 인프라가 제한된 환경에서도 안전하고 효율적으로 작동할 수 있는 블록체인 기반 오프라인 결제 시스템의 개발이 시급한 과제로 대두되고 있다.

오프라인 결제 시스템은 이러한 문제를 해결할 수 있는 잠재력을 가지고 있지만, 기존의 솔루션들은 대부분 중앙화된 신뢰 기관에 의존하고 있다[3]. 이는 블록체인의 핵심 가치인 탈중앙화와 상충하며, 중앙 기관의 단일 실패 지점(single point of failure) 문제를 내포하고 있다[4]. 중앙화된 시스템은 보안, 프라이버시, 그리고 시스템의 복원력 측면에서 취약점을 가질 수 있으며, 이는 사용자들의 신뢰를 저해할 수 있는 요소가 된다.

본 논문에서 제안하는 TEE-BOP(Trusted Execution Environment-Based Offline Payment)는 이러한 문제들을 해결하기 위해 신뢰실행환경(TEE)의 보안성, 머클 트리의 효율성, 그리고 TEE Attestation 기술을 결합한 혁신적인 접근 방식을 제시한다. TEE는 하드웨어 수준의 격리된 실행 환경을 제공하여 민감한 데이터와 연산을 보호한다[5]. 이는 오프라인 환경에서도 높은 수준의 보안을 유지할 수 있게 한다. 머클 트리는 대규모 데이터 구조의 무결성을 효율적으로 검증할 수 있게 하여[6], 제한된 리소스를 가진 모바일 기기에서도 블록체인 데이터의 유효성을 확인할 수 있게 한다. TEE Attestation 기술은 TEE의 무결성을 검증하고 생성된 키의 신뢰성을 보장함으로써[16], 시스템 전반의 신뢰도를 높인다.

TEE-BOP의 핵심 아이디어는 TEE 내에서 안전하게 관리되는 오프라인 잔액과, 블록체인에 기록되는 초기 입금 증명, 그리고 TEE Attestation을 통한 키 신뢰성 보장을 결합하는 것이다. 이를 통해 오프라인 환경에서도 이중 지불을 방지하고, 거래의 무결성을 보장할 수 있다. 또한, 간소화된 검증 과정으로 제한된 리소스를 가진 모바일 기기에서도 효율적으로 동작할 수 있다. 이는 블록체인 기술의 혜택을 더 넓은 범위의 사용자들에게 확장할 수 있는 가능성을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 살펴보고, 기존 접근 방식들의 장단점을 분석한다. 3장에서는 TEE-BOP 프로토콜의 상세 설계를 제시하며, 각 구성 요소의 역할과 상호작용에 관해 설명한다. 4장에서는 프로토콜의 보안성을 형식적으로 분석하고, 다양한 공격 시나리오에 대한 대응 방안을 논의한다. 5장에서는 향후 연구 방향을 논의하며, 마지막 6장에서는 본 연구의 의의와 기여점을 요약하며 결론을 맺는다.

II. 관련 연구

블록체인 기반의 오프라인 결제 시스템 개발은 금융 기술 분야에서 중요한 연구 주제로 부상하고 있다. 본 장에서는 블록체인 기반 결제 시스템과 오프라인 결제 연구의 현황을 심도 있게 살펴보고, 각 접근 방식의 장단점을 분석한다. 특히, (1) 전자 현금 시스템, (2) 블록체인 기반 결제 시스템, (3) TEE를 활용한 보안 시스템, (4) 오프라인 결제 연구, (5) 블록체인 기반 오프라인 결제 연구의 다섯 가지 카테고리로 나누어 관련 연구를 살펴본다. 이후 본 연구의 접근을 소개하며 탈중앙화, 스마트 컨트랙트 지원, 오프라인 결제 가능성, 이중 지불 문제 해결, 그리고 위조 방지 측면에서 각 연구를 비교 평가한다.

2.1 전자 현금 시스템

전자 현금 시스템의 개념은 Chaum et al.[3]에 의해 처음 제안되었다. 이들의 연구는 중앙화된 은행을 통해 익명성을 보장하는 전자 화폐 시스템을 구현하였다. Camenisch et al.[7]은 이를 발전시켜 오프라인 환경에서도 사용 가능한 익명 e-cash 시스템을 제안했다. 그러나 이러한 초기 시스템들은 여전히 중앙 기관에 의존적이었으며, 이중 지불 문제를 완전히 해결하지 못했다.

Brands[8]는 일회용 블라인드 서명을 사용하여 더욱 효율적인 전자 현금 시스템을 제안했다. 이 시스템은 사용자의 프라이버시를 보호하면서도 이중 지불을 탐지할 수 있는 메커니즘을 제공했다. 그러나 이 접근법 역시 중앙화된 은행의 존재를 전제로 하고 있다.

2.2 블록체인 기반 결제 시스템

Bitcoin[1]의 등장으로 중앙화된 기관 없이도 안전한 디지털 거래가 가능해졌다. 그러나 Bitcoin은 실시간 온라인 연결을 필요로 하며, 거래 확인에 대략 10분이 소요되어 즉각적인 결제에 한계가 있다. 이러한 문제를 해결하기 위해 Lightning Network[9]와 같은 Layer-2 솔루션이 제안되었다.

Lightning Network는 오프체인 결제 채널을 통해 즉각적인 소액 결제를 가능하게 한다. 그러나 이 접근법은 여전히 온라인 연결에 의존적이다. 채널 설정과 유지에 주기적인 온라인 연결이 필요할 뿐만 아니라, 채널이 사전에 설정되지 않으면 오프라인 결제가 불가능하다. 따라서 Lightning Network는 실제로 온라인 환경에서 주로 사용되는 방식이다.

Ethereum[10]의 등장으로 스마트 컨트랙트를 통한 복잡한 금융 로직 구현이 가능해졌지만, Ethereum 또한 실시간 온라인 연결을 전제로 하고 있다. 이는 오프라인 환경에서의 사용에 제약이 있으며, 스마트 컨트랙트를 활용한 다양한 응용 프로그램들도 네트워크에 계속 연결되어 있어야만 정상적으로 동작할 수 있다.

2.3 TEE를 활용한 보안 시스템

TEE(Trusted Execution Environment)는

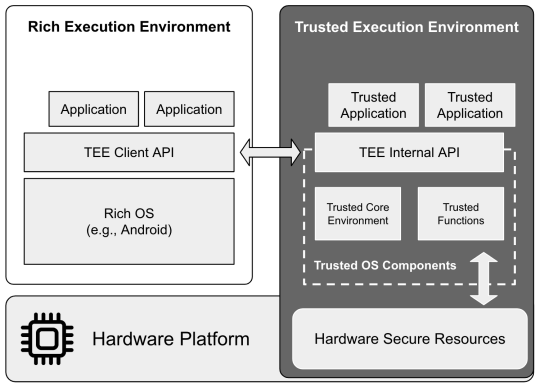

Fig. 1. Architecture of the TEE[27]

하드웨어 수준에서 격리된 실행 환경을 제공하여 민감한 데이터와 연산을 보호하는 기술이다.

Intel SGX[5]와 ARM TrustZone[12]이 대표적인 TEE 구현 기술이다. TEE는 격리 실행, 암호화된 메모리, TEE Attestation, 보안 키 관리 등의 주요 특징을 가지고 있으며, 이를 통해 외부의 간섭이나 관찰로부터 보호된 안전한 연산 환경을 제공한다.

블록체인 시스템에서 TEE를 활용한 연구들은 주로 프라이빗 스마트 컨트랙트, 오프체인 연산, 안전한 키 관리, 오프라인 거래 등의 목적으로 진행되고 있다. 이러한 기술을 블록체인과 결합한 연구들이 최근 활발히 진행되고 있으며, 블록체인의 보안성과 신뢰성을 향상시키는 데 중요한 역할을 하고 있다.

본 논문의 4장에서 언급한바와 같이, TEE 기술은 현재 높은 수준의 보안을 제공하고 있으며, 공격에 대한 비용이 매우 높아 현실적으로 공격이 쉽지 않다. 실제로 ApplePay, SamsungPay 등 많은 결제 시스템에서 TEE가 광범위하게 사용되고 있다[25]. 이러한 TEE의 안전성에 기반하여, 본 논문을 포함한 많은 연구는 TEE를 활용한 프로토콜을 설계하고 있다.

2.4 오프라인 결제 연구

Christodorescu et al.[13]은 CBDC를 위한 오프라인 결제 시스템 연구에서 중앙화된 서버를 사용하는 접근 방식을 제안했다. 이 방식은 서버가 '입금 확인' 서명을 생성해 TEE에 제공하며, 이를 통해 TEE는 서버와 실제 잔액 상태를 안전하게 주고받을 수 있다. 이 접근법은 중앙화된 시스템의 장점

을 활용하여 구현이 상대적으로 용이하고 효율적인 관리가 가능하지만, 단일 실패 지점 문제와 중앙 기관에 대한 의존성 등 블록체인이 해결하고자 했던 중앙화의 한계를 여전히 내포하고 있다.

2.5 블록체인 기반 오프라인 결제 연구

블록체인 기술은 분산화된 신뢰 모델을 통해 중앙 기관의 필요성을 제거하고 투명성을 제공하지만, 실시간 네트워크 연결에 의존한다는 본질적인 한계가 존재한다. 오프라인 결제 기능은 이러한 한계를 극복하고 블록체인 기술의 적용 범위를 확장하기 위해 중요하다. 특히 인터넷 연결이 불안정한 지역이나 재난 상황에서 블록체인 기반 결제 시스템의 실용성을 크게 향상시킬 수 있다.

그러나 블록체인 환경에서의 오프라인 결제 구현은 중앙화된 서버 기반 시스템에 비해 상당한 기술적 도전을 수반한다. 중앙 권위체가 부재한 상황에서 오프라인 거래의 유효성을 검증하고 이중 지불을 방지하는 것이 핵심 과제이다. 블록체인 기반 오프라인 결제는 사용자의 악의적 행위에 취약하며, 이중 지불 문제와 위조 방지 문제를 근본적으로 해결하기 어렵다. 현재까지의 연구에서 가장 유망한 접근법은 TEE와 같은 안전한 하드웨어를 활용하여 이 두 가지 핵심 문제를 해결하는 방식이다.

Dmitrienko et al.[14]은 비트코인 네트워크에서의 오프라인 결제 방법을 제안했다. 이 연구도 TEE를 활용하는 방식을 채택하였으며, 분산화된 지갑 취소(Distributed Wallet Revocation) 메커니즘을 도입하여 이중 지불 문제에 대응하고, 확률적 보안 모델을 통해 위조 방지를 시도했다. 그러나 이 방법은 이중 지불 문제를 사전에 완전히 방지하지 못하고 사후 대응에 초점을 맞추며, 이중 지불 발생 시 피해자의 손실을 완전히 보상하지 못한다는 한계를 가진다. 또한, TEE에 의존하는 보안 이외에도 위조 방지에 대한 확률적 접근으로 인해 완전한 보안을 보장하지 못한다는 문제점이 있다.

Jie et al.[15]의 연구는 TEE와 스마트 컨트랙트를 결합한 접근법을 제시했다. 이 프로토콜은 TEE를 활용하여 오프라인 상태에서 안전한 연산을 수행하고, 스마트 컨트랙트를 통해 복잡한 금융 로직을 구현할 수 있으며, 오프라인 결제와 온라인 동기화를 결합하여 유연성을 제공한다. 그러나 이 접근법은 블록체인의 실제 상태를 TEE가 독립적으로 검증할 수 있는 구체적인 방법이 부재하여, 이상적인 채널 모델을 가정하므로 실용 가능성이 낮다는 한계점이 존재한다.

2.6 기존 연구의 한계 및 본 연구의 접근

기존 연구들은 블록체인 기반 오프라인 결제 시스템 구현에 있어 여러 한계점을 드러냈다. 중앙화된 접근법은 단일 실패 지점 문제와 중앙 기관 의존성을 해결하지 못했으며, 분산화된 접근법은 이중 지불과 위조 방지 문제에 대한 완전한 해결책을 제시하지 못했다.

본 논문에서 제안하는 프로토콜은 이러한 기존 연구의 한계를 극복하고자 한다. 우리의 접근법은 TEE 보안을 활용하면서도 이상적인 모델에 의존하지 않는 실용 가능한 설계를 제시한다. 특히, 머클 트리를 활용한 로컬 검증 메커니즘을 통해 수취인이 블록체인의 실제 상태를 직접 확인할 수 있게 하여,

Table 1. Comparison of related papers

Approach	Decentralized (No central server)	Smart contract support	Offline Payments	No double spending	Unforgeability
Christodorescu et al.[13]	x	x	o	TEE-based	o (Centralized Verification)
Dmitrienko et al.[14]	o	x	o	Vulnerable	Probabilistic vulnerable
Jie et al.[15]	o	o	o	TEE-based	Impractical (Ideal Model)
Our protocol	o	o	o	TEE-based	o (MT local verification)

지불자의 TEE 내의 상태를 신뢰할 수 있는 구체적인 방법론을 제공한다. 이중 지불 문제는 TEE의 안전성에 기반하여 해결하며, 이를 통해 오프라인 환경에서의 유연한 사용성을 보장한다.

Table 1.은 기존 연구들과 본 논문에서 제안하는 프로토콜의 주요 특성을 비교한 것이다.

이 비교 표를 통해 본 연구에서 제안하는 프로토콜이 기존 접근법들의 한계를 극복하고, 탈중앙화, 스마트 컨트랙트 지원, 오프라인 결제 기능, 그리고 강화된 보안 메커니즘을 동시에 제공하는 것을 알 수 있다. 특히, 머클 트리를 이용한 로컬 검증 메커니즘은 많은 컴퓨팅 파워를 요구하지 않고 수취인이 직접 위조 방지 문제를 검증할 수 있는 방식으로, 위조 방지 문제에 대한 혁신적인 해결책을 제시한다. 이는 기존 연구가 해결하지 못한 문제들을 해결함으로써, 블록체인 기반 오프라인 결제 시스템의 실용화에 실질적인 진전을 이룰 수 있게 한다.

III. TEE기반의 블록체인 오프라인 결제 프로토콜

본 장에서는 TEE-BOP라는 새로운 프로토콜을 제안한다. TEE-BOP는 TEE의 하드웨어 수준 보안성과 블록체인의 분산 검증 메커니즘을 결합하여 안전하고 효율적인 오프라인 결제를 실현한다. 이 프로토콜은 기존 연구의 한계를 극복하고, 탈중앙화된 환경에서 신뢰성 있는 오프라인 결제를 가능하게 한다.

3.1 시스템 모델

TEE-BOP 프로토콜은 다음과 같은 주요 구성요소로 이루어진다:

1. Payer: TEE가 탑재된 디바이스를 소유한 오프라인 결제 개시자(지불자)
2. Payee: 결제의 유효성을 검증하는 수취인 (TEE 미탑재 가능)
3. Trusted Execution Environment (TEE): Payer의 디바이스에 내장된 격리된 실행 환경
4. Global On-chain Contract (GOC): 블록체인 상에 배포된 스마트 컨트랙트
5. Merkle Tree (MT): GOC에서 관리되는 초기 입금 기록 자료구조

이러한 구성 요소들은 상호 작용을 통해 안전한 오프라인 결제 시스템을 구현한다. Payer의 TEE는 오프라인 결제의 핵심 보안 요소로 작용하며, GOC는 온체인 상태 관리와 최종 정산을 담당한다. 머클 트리(MT)는 효율적인 데이터 검증을 위해 사용된다.

3.2 암호화 기본 요소

TEE-BOP 프로토콜은 다음과 같은 암호화 기본 요소를 사용한다:

- $H(\cdot)$: 충돌 저항성을 가진 암호학적 해시 함수 (예: SHA-256)
- $KeyGen(1^\lambda) \rightarrow (pk, sk)$: 보안 매개변수 λ를 입력으로 받아 공개키 pk와 비밀키 sk를 생성하는 키 생성 알고리즘. 여기서 1^λ는 λ비트의 1로 이루어진 문자열을 의미하며, 이는 알고리즘의 보안 수준을 결정한다.
- $sign(m, sk) \rightarrow \sigma$: 메시지 m과 비밀키 sk를 입력으로 받아 서명 σ를 생성하는 서명 알고리즘
- $verify(m, \sigma, pk) \rightarrow \{0, 1\}$: 메시지 m, 서명 σ, 공개키 pk를 입력으로 받아 서명의 유효성을 검증하는 알고리즘

이러한 암호화 요소들은 프로토콜의 각 단계에서 데이터의 무결성, 인증, 그리고 부인 방지를 보장하는 데 사용된다.

3.3 TEE Attestation

TEE Attestation은 TEE의 신뢰성을 보장하기 위한 중요한 메커니즘으로, TEE가 실행 중인 코드와 데이터의 무결성을 외부 엔티티가 검증할 수 있도록 하는 역할을 한다. 이 과정은 TEE 내부에서 독립적으로 수행되며, TEE가 물리적 공격에 노출된 환경에서도 내부의 무결성을 유지할 수 있도록 설계되어 있다.

TEE Attestation은 다음과 같은 정보를 포함하는 서명된 데이터를 생성한다:

$$TA = (ID_{TEE}, Ver_{HW}, Ver_{FW}, M_{code}, pk_i, \sigma_{TA})$$

여기서 ID_{TEE}는 TEE 제조사 식별자, Ver_{HW}

와 Ver_{FW}는 각각 하드웨어와 펌웨어 버전, M_{code}는 TEE 내부 코드에서 실행 중인 코드의 측정값(해시), pk_i는 TEE가 오프라인 금액 초기 입금 요청을 받고 생성한 공개키, σ_{TA}은 TEE 제조사의 비밀키로 생성된 디지털 서명이다.

TEE Attestation의 생성 및 검증 과정은 다음과 같이 이루어진다. TEE는 제조 과정에서 미리 프로비저닝된 비밀키(SK_{TEE})를 사용하여 자신의 상태를 나타내는 데이터에 서명한다. 이 서명된 Attestation 데이터는 외부 엔티티로 전송되며, 외부 엔티티는 TEE 제조사로부터 사전에 배포된 공개키(PK_{TEE})를 통해 서명의 유효성을 검증할 수 있다[16]. 이를 통해 TEE가 신뢰할 수 있는 환경에서 동작하고 있으며, 내부 코드와 데이터가 변조되지 않았음을 확인할 수 있다.

TEE-BOP 프로토콜에서는 TEE Attestation이 Payer의 입금 요청 단계에서 생성되어 GOC에 제출된다. GOC는 이를 통해 TEE의 신뢰성을 검증하며, 이후의 오프라인 거래에 대한 보안 기반을 마련하게 된다. 따라서 TEE Attestation은 TEE-BOP 시스템의 전반적인 보안성을 강화하는 중요한 구성 요소이다.

3.4 프로토콜 설명

Fig. 2.는 제안된 TEE-BOP 프로토콜의 아키텍처 개요를 도식화한 것이다. $Addr_{Payer}$와 $Addr_{Payee}$는 각각 Payer와 Payee의 블록체인 주소를 나타내고 sk_{Payer}와 sk_{Payee}는 그에 대응하는 비밀키를 나타낸다. 사용자는 이러한 키 쌍을 사용하여 블록체인과의 상호작용 시 트랜잭션에 서명한다.

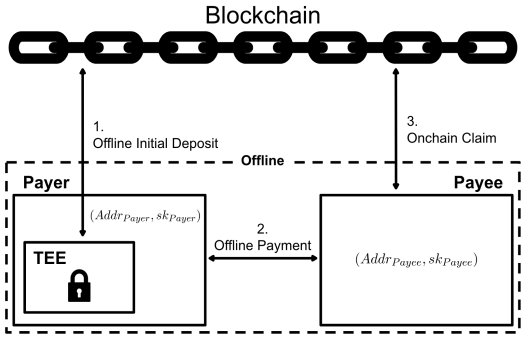

Fig. 2. TEE-BOP protocol overview

본 프로토콜은 오프라인 금액 초기 입금, 오프라인 결제, 정산의 3단계로 구성된다. 각 단계의 상세한 설명은 다음과 같다.

3.4.1 오프라인 금액 초기 입금

본 절에서는 TEE-BOP 프로토콜의 첫 번째 단계인 오프라인 금액 초기 입금 과정을 상세히 기술한다. 이 단계는 Payer가 오프라인 결제에 사용할 금액을 자신의 TEE에 안전하게 할당하고 이를 블록체인에 입금하는 과정을 포함한다. 이 과정은 TEE의 보안 기능과 블록체인의 투명성 및 불변성을 결합하여 안전하고 검증 가능한 입금 메커니즘을 제공한다.

오프라인 금액 초기 입금 프로토콜의 세부 단계는 Fig. 3.에 명시되어 있다.

Algorithm 1 Offline Initial Amount Deposit Process

Payer sends $\texttt{DepositRequest}(amount_{offline})$ to TEE

TEE:
- $(pk_i, sk_i) \leftarrow \texttt{KeyGen}(1^\lambda)$
- $balance_{offline} = amount_{offline}$
- $M_{code} = \texttt{H}(TEE_{code})$
- $TA = (ID_{TEE}, Ver_{HW}, Ver_{FW}, M_{code}, pk_i)$
- $\sigma_{TA} = \texttt{Sign}(TA, SK_{TEE})$
- $m_{init} = (amount_{offline} \| pk_i)$
- $\sigma_{deposit} = \texttt{Sign}(m_{init}, sk_i)$
- Send $(m_{init}, pk_i, \sigma_{deposit}, TA, \sigma_{TA})$ to Payer

Payer sends $T(m_{init}, pk_i, \sigma_{deposit}, TA, \sigma_{TA}, amount_{onchain})$ to GOC

GOC:
- **assert** $\texttt{Verify}(TA, \sigma_{TA}, PK_{TEE})$
- **assert** $\texttt{Verify}(m_{init}, \sigma_{deposit}, pk_i)$
- **assert** $amount_{offline} == amount_{onchain}$
- $balance[pk_i] = amount_{onchain}$
- $\texttt{MT.add}(\sigma_{deposit})$
- Send **Receipt** to Payer

Fig. 3. Offline Initial Amount Deposit Process

프로토콜은 Payer의 입금 요청으로부터 시작된다. TEE는 이 요청을 받아 일련의 중요한 작업을 수행한다. 먼저 KeyGen(1^λ) 함수를 통해 안전한 키 쌍을 생성하고, 요청된 금액을 TEE의 오프라인 잔액에 할당한다. 이 과정에서 생성되는 공개키 pk_i는 충분히 큰 키 공간에서 무작위로 선택되며, 현대 암호 표준에 따라 생성된다. 이러한 방식으로, 서로 다른 TEE 간에 동일한 pk_i가 생성될 확률은 극히 낮아, 실질적으로 각 TEE의 $\sigma_{deposit}$의 고유성이 보장된다[17].

그다음, TEE가 수행하는 코드의 해시값을 계산하고, 이를 포함한 TEE Attestation(TA)을 생성

한다. TA는 TEE의 식별자, 하드웨어 및 펌웨어 버전, 코드 해시, 그리고 생성된 공개키를 포함한다. 이 TA는 TEE 제조사의 키로 서명되어 σ_{TA}가 생성된다. 마지막으로, TEE는 입금 금액과 공개키에 대한 서명 $\sigma_{deposit}$을 생성하고, 이 모든 정보를 Payer에게 반환한다.

Payer는 TEE로부터 받은 정보를 바탕으로 트랜잭션 T를 구성하여 GOC에 전송한다. 이 트랜잭션에는 입금 서명, 온체인 입금 금액, TA 등이 포함된다.

GOC는 받은 정보를 철저하게 검증한다. 먼저 TA의 유효성을 확인한다. 이 과정에서 GOC는 TEE 제조사가 공개적으로 제공한 공개키(PK_{TEE})를 사용하여 TA의 서명을 검증한다. TA 검증이 성공적으로 완료되면, GOC는 다음으로 입금 서명을 검증한다. 그다음, 오프라인 입금 요청 금액과 실제 온체인 입금 금액의 일치 여부를 확인한다. 모든 검증이 성공적으로 완료되면, GOC는 총 입금액을 업데이트하고 입금 서명을 머클 트리에 추가한 후, Payer에게 입금 영수증을 전송한다.

이 프로토콜은 무결성, 기밀성, 검증 가능성 등의 주요 보안 속성을 제공한다. TA를 통해 플랫폼의 무결성이 검증되며, 비밀키(sk_i)는 TEE 내부에서만 접근 가능하여 기밀성이 보장된다. 또한, 입금 서명($\sigma_{deposit}$)은 블록체인에 기록되어, 추후 오프라인 결제 과정에서 Payee가 직접 GOC에 기록된 정보를 검증할 수 있게 한다.

오프라인 금액 초기 입금 단계는 TEE의 보안 기능과 블록체인의 투명성을 결합하여 안전하고 검증 가능한 자금 입금 메커니즘을 제공한다. 이는 후속 오프라인 거래의 기반이 되며, TEE-BOP 프로토콜의 전체적인 보안성을 강화한다. 특히, GOC에 입금된 금액은 TEE의 유효한 서명 없이는 이체될 수 없도록 설계되어 있다. 이러한 메커니즘은 TEE를 우회한 악의적인 행동을 원천적으로 방지한다.

결과적으로, 본 프로토콜은 TEE와 블록체인 기술의 장점을 효과적으로 결합하여 안전하고 신뢰할 수 있는 오프라인 결제 환경을 구축한다.

3.4.2 오프라인 결제

본 절에서는 TEE-BOP 프로토콜의 핵심인 오프라인 결제 과정을 상세히 기술한다. 이 과정에서는 Payer와 Payee는 네트워크 연결 없이 직접 거래를 수행한다. 구체적으로, 이는 NFC(Near Field Communication)[23] 또는 BLE(Bluetooth Low Energy)[28]와 같은 단거리 무선 통신 기술을 활용하여 이루어진다. 이러한 기술들은 두 기기 간의 근접한 거리에서 안전하고 효율적인 데이터 교환을 가능하게 한다.

TEE-BOP 프로토콜의 주요 특징은 GOC에 기록된 초기 입금 데이터의 무결성을 머클 트리를 통해 효율적으로 검증한다는 점이다. 특히, 머클 트리에는 초기 입금 기록만이 존재하며, Payee가 이를 간단히 검증함으로써 효율적인 위조 방지 메커니즘을 구현한다. 이 방식은 전체 블록체인 데이터를 검증할 필요 없이 특정 거래의 유효성을 빠르게 확인할 수 있게 한다. 머클 트리에 저장된 리프노드($\sigma_{deposit}$)의 불변성을 활용함으로써 프로토콜의 보안성이 크게 향상되며, 이는 TEE의 안전성과 결합하여 높은 수준의 신뢰성을 제공한다.

3.4.2.1 오프라인 결제 사전 준비

오프라인 결제를 위한 사전 준비 단계는 Payer와 Payee 모두에게 필수적이며, 이는 오프라인 환경에서의 안전하고 효율적인 거래를 보장하기 위한 핵심 요소이다. 이 준비 과정은 Payer와 Payee 각각에 대해 다르게 적용되며, 다음과 같이 상세히 설명될 수 있다.

Payer의 사전 준비는 주기적인 머클 증명(Merkle Proof) 업데이트를 중심으로 이루어진다. Payer는 t_{payer}라는 주기(예: 약 1주일)마다 최소 한 번 현재 블록의 GOC에서 관리되는 머클 트리 상태를 확인한다. 이 과정에서 Payer는 자신의 초기 입금 서명인 $\sigma_{deposit}$에 대한 머클 증명을 생성하고, 이를 자신의 디바이스에 저장한다. 이러한 과정은 주기적인 간단한 네트워크 요청과 로컬 저장 작업으로 구성되어 있어, 큰 오버헤드 없이 수행할 수 있다는 장점이 있다.

머클 증명의 크기는 머클 트리의 깊이에 비례한다. 머클 트리의 깊이는 $\log_2 n$ (여기서 n은 리프노드의 수)이므로, 머클 증명의 저장 공간 요구사항은 $O(\log_2 n)$으로 매우 효율적이다. 이는 블록체인의 전체 상태를 저장하는 것에 비해 현저히 적은 저장 공간을 요구하며, 이를 통해 제한된 저장 공간을

가진 모바일 기기나 IoT 디바이스에서도 적용 가능한 수준의 효율성을 제공한다.

한편, Payee의 사전 준비는 머클 루트(root)의 주기적인 저장에 초점을 맞춘다. Payee는 t_{payee}기간 동안 (예: 약 1주일) 생성되는 모든 블록의 GOC 머클 루트를 자신의 디바이스에 저장한다. 각 머클 루트는 고정된 크기(예: 32바이트)를 가지므로, 저장 공간의 예측과 관리가 용이하다. 이렇게 저장된 머클 루트는 후에 Payer로부터 받은 머클 증명의 유효성을 검증하는 데 사용된다.

Payer와 Payee의 주기 차이로 인해 발생할 수 있는 문제를 방지하기 위해, 두 주체는 서로 다른 방식으로 데이터를 관리한다. Payer는 t_{payer}주기마다 최소 한 번씩 머클 증명을 업데이트하고, Payee는 t_{payee}기간 동안의 모든 머클 루트를 저장한다. 이는 매 블록에서의 머클 루트를 저장하되, 최소 t_{payee}기간 동안의 데이터를 저장공간에 유지함을 의미한다. 이러한 접근 방식은 Payer와 Payee 간의 시간적 불일치를 최소화하고, 오프라인 거래 시 즉각적인 검증을 가능하게 한다.

실제 적용을 위해 이더리움 네트워크를 예로 들면, 2024년 8월 기준으로 지난 1년간 일일 평균 7,031개의 블록이 생성되었다는 Etherscan의 데이터를 활용할 수 있다[24]. 이를 바탕으로 계산하면 일주일 동안 약 49,217개의 블록이 생성된다 (7,031 블록/일 * 7일 ≈ 49,217 블록/주).

따라서, t_{payer}와 t_{payee}를 모두 49,217 블록(약 1주일)으로 설정할 경우, Payer는 49,217 블록마다 최소 한 번씩 머클 증명을 업데이트하고, Payee는 49,217개의 연속된 블록에 대한 머클 루트를 항상 저장하고 있게 된다.

이러한 설정에서 Payee의 저장 공간 요구사항은 약 1.57MB (32바이트 * 49,217 블록)로 계산된다. 이는 현대의 모바일 기기나 IoT 디바이스에서도 충분히 관리 가능한 수준으로, 제안된 프로토콜의 실용성을 뒷받침한다.

이러한 방식으로, Payer가 제공하는 머클 증명에 대응하는 머클 루트를 Payee가 항상 가지고 있을 수 있게 되어, 오프라인 거래 시 즉시 검증이 가능하다. 설령 Payer가 최신 블록에서 머클 증명을 업데이트하고, Payee가 최신 블록까지 업데이트를 못했다면, Payer의 업데이트 이전 머클 증명을 통해서 자신의 초기 입금을 증명할 수 있다.

3.4.2.2 오프라인 결제 프로세스

오프라인 결제 프로토콜의 세부 단계는 Fig. 4.에 명시되어 있다.

오프라인 결제 프로토콜은 Payee가 Payer에게 머클 증명 요청을 전송하면서 시작된다. Payer는 이에 응답하여 자신이 저장한 최신 머클 증명을 Payee에게 제공한다. 이 증명은 Payer의 초기 입금이 유효함을 증명하는 데 사용된다.

Payee는 먼저 수신한 머클 증명의 머클 루트가 자신이 보유한 유효한 머클 루트 집합에 포함되는지 확인한다. 일치하는 머클 루트가 발견되면, Payee는 해당 머클 증명의 유효성을 검증한다. 이 과정은 $O(\log_2 n)$의 계산 복잡도를 가진다. 검증이 성공하면 Payee는 결제 요청을 Payer에게 전송한다. 이 요청에는 Payee의 블록체인 주소와 요청 금액이 포함된다.

Payer는 받은 결제 요청을 자신의 TEE로 전달한다. TEE는 내부적으로 중요한 보안 작업을 수행한다. 먼저 오프라인 잔액이 충분한지 확인하고, 요청된 금액만큼 잔액을 차감한다. 그다음, TEE 내부의 단조증가 카운터[12]를 활용해 Nonce를 설정한 뒤, 결제 서명을 생성한다. 이 서명에는 Payee의 블록체인 주소, 결제 금액, 그리고 이중 지불을 방지하기 위한 Nonce가 포함된다.

TEE가 생성한 결제 서명은 Payer를 거쳐 Payee에게 전달된다. Payee는 이 서명의 유효성을 검증한다. 검증이 성공하면 Payee는 거래 완료 메시지를 Payer에게 전송하여 거래를 종료한다.

Algorithm 2 Offline Payment Process

Payee sends `MerkleProofRequest` to Payer
Payer sends `MerkleProof`($\sigma_{deposit}$) to Payee

Payee:
  assert Verify(`MerkleProof`($\sigma_{deposit}$))
  Send `PaymentRequest`($Addr_{Payee}, amount_{pay}$) to Payer

Payer sends `PaymentRequest`($Addr_{Payee}, amount_{pay}$) to TEE

TEE:
  assert ($balance_{offline} \geq amount_{pay}$)
  $balance_{offline} -= amount_{pay}$
  $Nonce \leftarrow$ TEE's monotonic counter
  $m_{payment} = (Addr_{Payee} \| amount_{pay} \| Nonce)$
  $\sigma_{payment} = \texttt{Sign}(m_{payment}, sk_i)$
  Send $(m_{payment}, \sigma_{payment})$ to Payer

Payer sends $(m_{payment}, \sigma_{payment})$ to Payee

Payee:
  assert Verify($m_{payment}, \sigma_{payment}, pk_i$)
  Send `OK` to Payer

Fig. 4. Offline Payment Process

3.4.3 온체인 정산

TEE-BOP 프로토콜의 마지막 단계인 온체인 정산 과정은 오프라인에서 수행된 거래를 블록체인 상에서 검증하고 최종적으로 정산하는 중요한 역할을 수행한다. 이 단계는 Payee가 온라인 연결을 회복했을 때 시작되며, 이전 단계에서 보장된 거래의 무결성을 블록체인에 반영하고 이중 지불을 방지하는 메커니즘을 포함한다. Fig. 5.은 이 정산 과정의 세부 절차를 나타낸다.

정산 과정은 Payee가 메시지와 결제 서명을 가지고 GOC에 정산 요청을 전송하면서 시작된다. 여기서 GOC에 보내는 메시지($m_{payment}$)는 Payee의 블록체인 주소, 결제 금액, Nonce의 정보를 담고 있는 메시지이다. 결제 서명($\sigma_{payment}$)은 오프라인 거래시 TEE가 생성한 결제 서명이다. GOC는 이 요청을 받아 일련의 검증 및 처리 작업을 수행한다.

먼저, GOC는 결제 서명의 유효성을 확인한다. 이 과정을 통해 오프라인 거래가 실제로 유효한 Payer의 TEE에 의해 생성되었음을 보장한다.

다음으로, GOC는 공개키(pk_i)와 Nonce를 사용하여 이 거래가 이미 처리되었는지 확인한다. 이 과정은 동일한 오프라인 거래가 여러 번 청구되는 것을 방지하는 중요한 단계이다. 이중 지불 확인 후, GOC는 해당 공개키의 Nonce를 사용됨으로 표시한다. 이는 향후 동일한 Nonce를 사용한 청구를 방지하기 위한 조치이다.

검증 과정이 성공적으로 완료되면, GOC는 정산된 금액만큼 Payer의 온체인 잔액을 감소시킨다. 마지막으로, GOC는 정산된 금액을 Payee의 블록체인 주소로 이체한다. 이로써 오프라인 거래의 온체인 정산 과정이 완료된다.

이 정산 과정을 통해 오프라인에서 이루어진 거래가 블록체인 상에서 안전하게 검증되고 처리된다.

Algorithm 3 Onchain Claim Process

Payee sends `Claim`($m_{payment}, \sigma_{payment}$) to GOC

GOC:

assert Verify($m_{payment}, \sigma_{payment}, pk_i$)
assert !IsDoubleSpent($pk_i, Nonce$)
MarkAsSpent($pk_i, Nonce$)
$balance[pk_i] -= amount_{pay}$
Transfer $amount_{pay}$ to $Addr_{Payee}$

Fig. 5. Onchain Claim Process

GOC의 철저한 검증 과정은 거래의 유효성을 보장하며, Nonce의 사용은 이중 지불을 효과적으로 방지한다. 또한, 모든 정산 과정이 블록체인에 기록되어 투명성과 감사 가능성을 제공한다.

IV. 보안성 분석

본 장에서는 TEE-BOP 프로토콜의 보안성을 체계적으로 분석한다. 주요 보안 목표인 이중 지불 방지, 위조 방지, 부인 방지, 그리고 다양한 공격 시나리오에 대한 저항성을 중심으로 평가를 수행한다.

4.1 이중 지불 방지

TEE-BOP 프로토콜은 다층적 방어 메커니즘을 통해 이중 지불을 효과적으로 방지한다:

a) TEE 내부 잔액 관리:
Payer의 잔액은 TEE 내부에서 엄격하게 관리된다. 모든 거래는 TEE 내에서 검증되며, 잔액 변경 연산은 원자적으로 수행된다. 이는 오프라인 환경에서 동일 금액의 중복 사용을 원천적으로 차단한다. TEE의 격리된 실행 환경은 외부로부터의 무단 접근과 조작을 방지하여, 잔액 관리의 무결성을 보장한다[16].

b) Nonce 활용:
각 오프라인 거래마다 고유한 Nonce가 사용되어 거래의 유일성을 보장한다. Nonce는 정산 단계에서 GOC에 의해 검증되며, 사용된 Nonce의 재사용은 불가능하다. 이는 동일한 거래가 여러 번 처리되는 것을 방지하며, 온체인 정산 과정에서의 이중 지불 시도를 차단한다.

이러한 다층적 방어 메커니즘의 조합으로 인해, 이중 지불을 시도하기 위해 공격자는 TEE의 보안을 무력화하고, Nonce의 중복을 GOC가 탐지하지 못하도록 해야 한다. 이는 하드웨어와 소프트웨어 수준에서 각기 다른 보안 계층을 형성한다. 이는 현재의 기술 수준에서 상당히 어려운 수준의 보안을 제공한다.

4.2 위조 방지

TEE-BOP 프로토콜은 다음과 같은 방법으로 거래 위조를 방지한다:

a) 머클 트리 기반 검증:
초기 입금 기록은 블록체인의 머클 트리에 저장되며, 이는 오프라인 거래의 기반이 된다. Payee는 거래 전 머클 증명을 검증하여 Payer의 자금 보유를 확인한다. 머클 트리의 암호학적 특성상, 머클 루트 해시의 변조 없이 개별 거래 기록을 수정하는 것은 계산적으로 매우 어렵다[11]. 이 메커니즘은 초기 자금의 유효성을 보장하며, 허위 자금으로의 지불을 방지한다.

b) TEE 기반 안전한 키 관리 및 서명 생성:
TEE-BOP 프로토콜은 모든 오프라인 거래에 사용되는 비밀키를 TEE 내부에서 생성 및 관리한다. TEE의 격리된 실행 환경은 비밀키에 대한 무단 접근을 원천적으로 차단한다[16]. 거래 데이터 생성 및 서명 과정이 이 보안 환경에서 수행되어, 거래 위조 시도를 효과적으로 방지한다.

본 프로토콜은 전체 메시지에 대해 직접 서명을 수행한다. 이 방식은 거래 데이터의 무결성을 보장하며, TEE에서 생성된 디지털 서명은 거래의 출처 신뢰성을 확립한다. 서명 검증 과정을 통해 Payee는 거래의 진위를 확인할 수 있다.
이러한 보안 메커니즘으로 인해, 거래 위조 공격 시도는 TEE의 보안, 머클 트리의 구조적 특성, 그리고 디지털 서명 체계를 동시에 무력화해야 한다. 현재의 기술 수준에서 이는 계산적으로 실현 불가능하므로, 거래 위조에 대해 강력한 보안성을 제공한다고 볼 수 있다.

4.3 부인 방지

TEE-BOP 프로토콜은 다음 메커니즘을 통해 거래 부인을 효과적으로 방지한다:

a) 양방향 확인 프로세스:
거래 과정에서 Payee는 거래 수락 시 확인 메시지를 Payer에게 전송한다. 이 과정에서 생성된 기록들은 양측이 거래를 인정했음을 증명한다. 이 양방향 프로세스는 거래의 상호 인정을 보장하며, 추후 발생할 수 있는 분쟁을 해결하는 데 중요한 증거로 활용될 수 있다.

b) 정산 단계에서의 검증:
오프라인 거래는 최종적으로 정산 단계에서 GOC에 의해 검증된다. 이 과정에서 Nonce의 유효성이 확인되며, 이는 거래의 존재를 불변적으로 증명한다. Payee는 이 정산 과정을 통해 실제 금액을 받게 되므로, 거래를 부인할 동기가 존재하지 않는다.

거래의 무결성이 암호학적으로 보장되고, 양방향 확인 프로세스가 존재하며, 정산 과정에서 실제 금액을 수령하는 구조로 인해 거래 부인의 가능성은 극히 낮다. 이는 TEE-BOP 프로토콜이 부인 방지 메커니즘을 갖추고 있음을 보여준다.

4.4 TEE의 신뢰성 기반 보안 및 잠재적 공격 시나리오 분석

TEE-BOP 프로토콜은 TrustZone과 같은 TEE의 강력한 보안 특성을 기반으로 설계되었으며, TEE의 신뢰성 보장 메커니즘과 다양한 잠재적 공격 시나리오에 대한 저항성을 갖추고 있다. 본 절에서 이러한 보안 메커니즘과 공격 시나리오를 상세하게 분석한다.

4.4.1 TEE의 신뢰성 보장 메커니즘

TEE는 TEE Attestation을 통해 자신의 무결성과 신뢰성을 외부에 암호학적으로 증명한다. 이는 TEE의 현재 상태, 구성, 그리고 실행 중인 소프트웨어의 측정값을 포함하며, TEE 제조사의 비밀키로 서명된 디지털 서명을 통해 보호된다. TEE-BOP 프로토콜에서 TEE Attestation은 TEE 내에서 생성된 공개키가 실제로 신뢰할 수 있는 환경에서 생성되었음을 입증한다. 해당 공개키는 GOC에 저장되어 이후 오프라인 거래의 유효성 검증에 사용된다. 또한, TEE Attestation에 포함된 측정값을 통해 TEE의 현재 상태가 예상된 안전한 상태와 일치하는지 확인할 수 있어, TEE가 변조되지 않았음을 보장한다[16].
TEE는 또한 높은 수준의 물리적 보안을 제공한다. TEE의 물리적 보안은 하드웨어 수준의 격리,

암호화된 메모리, 그리고 보안 부팅 등 다양한 기술을 통해 구현된다[16]. 이러한 기술들은 물리적 공격에 대한 높은 수준의 저항성을 제공하여 TEE의 무결성과 기밀성을 보장한다.

TEE의 주요 물리적 보안 특성 중 하나는 하드웨어 격리로, 보안 영역과 비보안 영역을 물리적으로 분리하여 비인가된 접근을 차단한다[16]. 또한, 중요 데이터와 코드는 암호화된 형태로 저장 및 처리되어 메모리에 대한 직접적인 물리적 공격을 어렵게 만든다.

보안 부팅은 시스템 부팅 시 TEE의 무결성을 검증하여 부트 단계에서의 공격을 방지하는 또 다른 중요한 특성이다[19]. 더불어, 실행 중인 코드와 데이터의 무결성을 지속적으로 검증하여 런타임 공격을 탐지하는 메커니즘도 구현되어 있다[20].

TEE의 강력한 물리적 보안은 오프라인 환경에서의 안전한 거래를 가능하게 하는 TEE-BOP와 같은 프로토콜의 기반이 된다. 이러한 TEE 기술은 네트워크 연결이 불안정하거나 불가능한 상황에서도 높은 수준의 보안을 제공한다.

4.4.2 잠재적 공격 시나리오 분석

TEE-BOP 프로토콜은 TEE의 보안 특성을 기반으로 설계되었으나, 다양한 잠재적 공격 시나리오에 노출될 수 있다. 본 절에서는 주요 공격 유형과 TEE-BOP 프로토콜의 취약점, 그리고 이에 대한 잠재적 대응 방안을 분석한다.

4.4.2.1 Side-Channel 공격

Side-Channel 공격은 TEE의 비기능적 특성(전력 소비, 전자기 방출, 실행 시간 등)을 분석하여 내부 데이터나 연산 과정을 유추하는 공격 기법이다[29]. TEE의 격리된 실행 환경은 기본적인 방어 체계를 제공하지만, 고도화된 공격 기법의 효과성이 입증되었다. 예를 들어, Bukasa et al.[26]의 연구에 따르면, TrustZone이 적용된 환경에서도 Side-Channel 공격이 성공적으로 수행될 수 있음이 실험적으로 입증되었다.

이러한 위험을 완화하기 위해 TEE-BOP 프로토콜에 다음과 같은 대응 방안을 적용할 수 있다. 상수 시간 암호화 알고리즘의 사용은 타이밍 공격 방지에 효과적일 수 있다. 이는 입력에 관계없이 일정한 시간이 소요되므로, 연산 시간을 통한 정보 유출을 차단할 수 있다[30].

TEE-BOP 프로토콜은 구조적으로 키 노출의 영향을 제한하는 특성을 가지고 있다. 구체적으로, 오프라인 잔액을 추가할 때마다 사용자는 초기 입금 프로세스를 다시 거치게 되며, 이 과정에서 새로운 키 쌍이 생성되어 사용된다. 이는 각 입금 세션마다 고유한 키를 사용하는 것을 의미하며, 이전 세션의 키가 노출되더라도 새로운 새션의 보안에는 영향을 미치지 않는다. 이러한 방식은 키의 수명을 제한하고, 공격자가 단일 키를 장기간 공격하는 것을 방지하여 전체적인 시스템 보안을 강화한다.

4.4.2.2 Fault Injection 공격

Fault Injection 공격은 TEE 하드웨어에 의도적인 오류를 주입하여 비정상적인 동작을 유도하고 보안 메커니즘을 우회하려는 공격 기법이다[29]. TEE-BOP 프로토콜에서는 특히 거래 서명 생성 과정이나 잔액 검증 로직이 해당 공격의 대상이 될 수 있다.

TEE는 기본적으로 전압 및 클록 모니터링, 센서를 통한 물리적 변조 감지 등의 기능을 제공하여 많은 Fault Injection 시도를 탐지하고 방어할 수 있다. 이에 대응책으로 중요 연산의 중복 수행 및 결과 비교, 오류 감지 및 정정 코드 적용, 그리고 TEE 내부 상태의 무결성 검사등을 고려할 수 있다[29].

4.4.2.3 상태 롤백 공격

상태 롤백 공격은 TEE의 내부 상태를 이전 시점으로 되돌려 거래를 무효화하려는 시도이다[31]. TEE-BOP 프로토콜에서는 이는 특히 오프라인 거래 후 잔액 상태를 롤백하려는 시도로 나타날 수 있다.

TEE-BOP 프로토콜은 Nonce와 단조증가 카운터를 결합한 방식을 통해 롤백 공격을 방지한다. 각 거래마다 고유한 Nonce를 생성하고, 이를 TEE 내부의 보안 단조증가 카운터와 연동함으로써 거래의 순서와 유일성을 보장하는 방식이다. 추가적인 대응 방안으로, TEE 내부에 각 거래의 해시 체인을 유지하고, 신뢰할 수 있는 시계 구현을 통해 오프라인 거래를 제한함으로써 롤백 공격의 위험을 더욱 감소시킬 수 있다.

이러한 종합적인 보안 분석을 통해, TEE-BOP 프로토콜이 오프라인 블록체인 거래의 보안 요구사항을 효과적으로 충족시키며, 실제 환경에서의 안전한

구현이 가능함을 확인할 수 있다. TEE의 물리적 보안과 암호학적 기법을 결합한 이 프로토콜은 이중 지불 방지, 거래 무결성 보장, 부인 방지와 같은 핵심 보안 요구사항을 충족시키며, 다양한 잠재적 공격 시나리오를 분석하고 이에 대한 대응 방안을 제시한다.

특히, TEE의 물리적 보안 특성과 경제적 요인을 고려할 때, TEE의 안전성을 해치는 공격은 현실적으로 매우 어려울 것으로 판단된다. 이러한 분석을 바탕으로, TEE-BOP 프로토콜은 오프라인 블록체인 거래 환경에서 요구되는 고수준의 보안 요구사항을 효과적으로 충족시키는 견고한 솔루션으로 평가될 수 있다.

V. 향후 연구 방향

본 연구에서 제안한 TEE-BOP 프로토콜은 블록체인 기반 오프라인 결제 시스템의 실용 가능성을 크게 향상시키고 그 보안성을 검증했다. 그러나 이 프로토콜의 잠재력을 더욱 확장하고 다양한 응용 분야에 적용하기 위해서는 추가적인 연구가 필요하다. 본 장에서는 TEE-BOP 프로토콜의 새로운 응용 분야를 위한 두 가지 주요 연구 방향을 제시한다.

5.1 영지식 증명을 통한 거래 프라이버시 강화

TEE-BOP 프로토콜의 프라이버시 보호 기능을 강화하기 위해 영지식 증명(Zero-Knowledge Proof, ZKP) 기술의 도입을 고려해볼 수 있다. 영지식 증명은 거래 당사자의 개인 정보를 노출하지 않으면서도 거래의 유효성을 증명할 수 있는 암호학적 기법이다. 특히, zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)[21]이나 Bulletproofs[22]와 같은 효율적인 영지식 증명 시스템은 TEE-BOP 프로토콜에 결합될 경우 거래의 프라이버시를 향상시킬 수 있다.

영지식 증명 기술의 도입은 TEE-BOP 프로토콜의 응용 범위를 넓히고, 특히 금융 프라이버시가 중요한 응용 분야에서의 활용도를 높이는 데 기여할 수 있다. 구체적으로, 영지식 증명을 통해 거래 금액, 참여자 신원 등의 민감한 정보를 보호하면서도 거래의 무결성을 유지할 수 있다.

그러나 영지식 증명 기술을 TEE-BOP에 효과적으로 통합하기 위해서는 몇 가지 중요한 도전 과제가 존재한다. 첫째, TEE의 제한된 컴퓨팅 자원 내에서 복잡한 영지식 증명 연산을 어떠한 방식으로 효율적으로 수행할 수 있을지에 대한 연구가 필요하다. zk-SNARK와 같은 기술은 고도의 계산 능력을 요구하므로, TEE의 환경 내에서 효율성을 유지하면서도 증명을 생성하고 검증할 수 있는 방법을 모색해야 한다. 둘째, 영지식 증명과 TEE의 보안 모델 간의 상호작용에 대한 심도 있는 연구가 필요하다. 영지식 증명을 도입함으로써 새로운 취약점이 발생하지 않도록 보안성을 충분히 검토하고, TEE-BOP 프로토콜의 전체적인 보안 모델을 강화해야 한다.

5.2 CBDC 시스템 적용 연구

TEE-BOP는 블록체인을 사용하는 CBDC 시스템의 오프라인 거래 메커니즘으로 적용될 수 있다. 현재 많은 국가에서 CBDC의 개발이 활발히 이루어지고 있으며, 이러한 디지털 화폐의 오프라인 사용 가능성은 다양한 환경에서 디지털 화폐의 활용도를 높이는 데 중요한 요소로 작용한다.

이를 위해서는 몇 가지 핵심적인 연구 방향이 요구된다. 첫째, 중앙은행의 정책적 요구사항과 규제 프레임워크에 부합하는 프로토콜 설계가 필수적이다. CBDC 시스템은 국가별로 다양한 규제와 정책을 따르므로, TEE-BOP 프로토콜을 이러한 요구사항에 맞추어 수정 및 보완해야 한다. 둘째, TEE-BOP 프로토콜을 기반으로 한 CBDC의 오프라인 거래가 실제 환경에서 어떻게 작동하는지를 검증하는 실증적으로 검토해야 한다. 특히 CBDC는 대규모 트래픽을 처리할 수 있어야 하므로, 다양한 시나리오에서의 테스트를 통해 시스템의 안정성과 보안성을 평가하고, 최적화된 프로토콜을 도출해야 한다.

VI. 결 론

본 논문에서는 신뢰실행환경 기반 블록체인 오프라인 결제 프로토콜 TEE-BOP를 제안하고, 보안성과 효율성을 체계적으로 분석하였다. 본 프로토콜은 네트워크 연결이 불안정한 상황에서도 안전하고 무결한 거래를 보장하기 위해 설계되었다. 이를 달성하기 위해, TEE를 활용한 지불자의 오프라인 잔액 관리와 블록체인과 데이터 일치를 수취인이 효율적으로 검증하는 방식으로 이중 지불 및 위조 방지 문제를 효과적으로 해결한다.

본 연구는 또한 다양한 공격 시나리오를 고려한 보안성 분석을 통해 TEE-BOP의 견고한 보안 메커니즘을 보였다. 이러한 분석 결과는 TEE-BOP가 실제 환경에서 실용적인 블록체인 오프라인 결제 솔루션으로 활용될 수 있음을 시사한다.

향후 연구에서는 영지식 증명 기술을 통한 거래 프라이버시 강화와 CBDC 시스템에 적용 방안을 탐구할 예정이다. 이를 통해 TEE-BOP의 개인정보 보호 기능과 실용성을 더욱 향상시킬 수 있을 것으로 기대된다.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Oct. 2008.

[2] World Bank, "Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution," World Bank Publications, May. 2018.

[3] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," Advances in Cryptology, CRYPTO '88, LNCS 403, pp. 319-327, 1990.

[4] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab "Blockchain for industry 4.0: A comprehensive review," IEEE Access, vol. 8, pp. 79764-79800, Apr. 2020.

[5] V. Costan and S. Devadas, "Intel SGX explained," Cryptology ePrint Archive, Paper 2016/086, Jan. 2016.

[6] R. C. Merkle, "A digital signature based on a conventional encryption function," Advances in Cryptology, CRYPTO '87, LNCS 293, pp. 369-378, 1988.

[7] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Compact e-cash," EUROCRYPT 2005, LNCS 3494, pp. 302-321, 2005.

[8] S. Brands, "Untraceable off-line cash in wallet with observers," Advances in Cryptology, CRYPTO '93, LNCS 773, pp. 302-318, 1993.

[9] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," Jan. 2016.

[10] V. Buterin, "A next-generation smart contract and decentralized application platform," Jan. 2014.

[11] National Institute of Standards and Technology, "Secure Hash Standard (SHS)," FIPS PUB 180-4, Aug. 2015.

[12] ARM Limited., "ARM security technology: Building a secure system using TrustZone technology," PRD29-GENC-009492C, Apr 2009.

[13] M. Christodorescu, W.C. Gu, R. Kumaresan, M. Minaei, M. Ozdayi, B. Price, S. Raghuraman, M. Saad, C. Sheffield, M. Xu, and M. Zamani, "Towards a two-tier hierarchical infrastructure: an offline payment system for central bank digital currencies," arXiv preprint arXiv:2012.08003, Dec. 2020.

[14] A. Dmitrienko, D. Noack, and M. Yung, "Secure wallet-assisted offline bitcoin payments with double-spender revocation," Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pp. 520-531, Apr. 2017.

[15] W. Jie, W. Qiu, A. S. Voundi Koe, J. Li, Y. Wang, Y. Wu, J. Li, and Z. Zheng, "A secure and flexible blockchain-based offline payment protocol," IEEE Transactions on Computers, vol. 73, no. 2, pp. 408-421, Feb. 2024.

[16] S. Pinto and N. Santos, "Demystifying arm trustzone: A comprehensive survey," ACM Computing Surveys, vol. 51, no. 6, pp. 1-36, Jan. 2019.

[17] N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, John Wiley & Sons, Feb. 2011.

[18] H. Armelius, C. A. Claussen, and I. Hull, "On the possibility of a cash-like CBDC," Sveriges Riksbank Staff memo, Feb. 2021.

[19] W. A. Arbaugh, D. J. Farber, and J. M. Smith, "A secure and reliable bootstrap architecture," Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097), pp. 65-71, May. 1997.

[20] A. M. Azab, P. Ning, J. Shah, Q. Chen, R. Bhutkar, G. Ganesh, J. Ma, and W. Shen, "Hypervision across worlds: Real-time kernel protection from the ARM TrustZone secure world," Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 90-102, Nov. 2014.

[21] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von Neumann architecture," 23rd USENIX Security Symposium, pp. 781-796, Aug. 2014.

[22] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," 2018 IEEE Symposium on Security and Privacy, pp. 315-334, May. 2018.

[23] P. Pourghomi and G. Ghinea, "A proposed NFC payment application," arXiv preprint arXiv:1312.2828, Dec. 2013.

[24] Etherscan, "Ethereum block count and rewards chart," https://etherscan.io/chart/blocks, Aug. 2024.

[25] W. Liu, X. Wang and W. Peng, "State of the Art: Secure Mobile Payment," IEEE Access, vol. 8, pp. 13898-13914, Jan. 2020.

[26] S.K. Bukasa, R. Lashermes, H. Le Bouder, J.L. Lanet, and A. Legay, "How TrustZone could be bypassed: Side-channel attacks on a modern system-on-chip," 11th IFIP International Conference on Information Security Theory and Practice, pp. 93-109, Sep. 2017.

[27] GlobalPlatform, "Introduction to trusted execution environments," GlobalPlatform, Inc., May. 2018.

[28] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of Bluetooth Low Energy: An emerging low-power wireless technology," Sensors, vol. 12, no. 9, pp. 11734-11753, Aug. 2012.

[29] A. Muñoz, R. Rios, R. Roman, and J. Lopez, "A survey on the (in)security of trusted execution environments," Computers & Security, vol. 129, Jun. 2023.

[30] Q. Ge, Y. Yarom, D. Cock, and G. Heiser, "A survey of microarchitectural timing attacks and countermeasures on contemporary hardware," Journal of Cryptographic Engineering, vol. 8, pp. 1-27, Apr. 2018.

[31] Y. Chen, Y. Zhang, Z. Wang, and T. Wei "Downgrade attack on trustzone," arXiv preprint arXiv:1707.05082, Jul. 2017.

〈저자소개〉

정 동 현 (Donghyun Jeong) 학생회원
2016년~2022년: 한국외국어대학교 컴퓨터공학과 졸업
2023년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 블록체인, 프라이버시, 암호

김 범 중 (Beomjoong Kim) 학생회원
2014년~2021년: 고려대학교 물리학과
2021년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석박사통합과정
〈관심분야〉 디지털 자산 보안, 블록체인, 프라이버시

이 중 희 (Junghee Lee) 종신회원
2000년 2월: 서울대학교 컴퓨터공학과 공학학사
2003년 2월: 서울대학교 컴퓨터공학과 공학석사
2003년~2008년: 삼성전자, 연구원
2013년 2월: 조지아공과대학교 전자공학과 공학박사
2014년~2019년: University of Texas at San Antonio 교수
2019년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 하드웨어 보안