보안성 강화를 위한 암호화폐 지갑 시스템의 현황과 발전 방향

고유민[1], 김미희[2]
[1]한경대학교 컴퓨터응용수학부 학부생
[2]한경대학교 컴퓨터응용수학부 (컴퓨터 시스템 연구소) 교수

goyoomin4206@hknu.ac.kr, mhkim@hknu.ac.kr(교신저자)

Current Status and Development Direction of Cryptocurrency Wallet System for Security Enhancemen

Yoo-min Go[1], Mi-hui Kim[2]
[1]School of Computer Engineering & Applied Mathematics, Hankyong National University
[2]School of Computer Engineering & Applied Mathematics, Hankyong National University

요 약

블록체인 기술의 급격한 발전은 비트코인과 이더리움 등 주요 암호화폐를 통해 디지털 자산 시장의 핵심 인프라를 구축하였으며, 이에 따라 사용자 자산을 안전하게 보관하고 거래를 지원하는 암호화폐 지갑의 중요성이 크게 부각되고 있다. 그러나 기존 지갑 시스템은 단일 프로세스 구조의 보안 취약성, 특정 네트워크에 대한 종속성, 복잡한 사용자 관리, 법적·제도적 미비와 같은 한계에 직면해 있다. 본 논문에서는 이러한 문제를 해결하기 위해 제안된 최신 기술 동향을 분석한다. 구체적으로 스마트 컨트랙트 기반 보호계좌 시스템, 다중 프로세스 구조 적용, 강화된 암호화 통신 및 합의 알고리즘 개선, 그리고 임계값 암호화·다자간 안전 계산·분산 키 생성과 같은 다중 노드 기반 암호화 기법을 고찰하고 향후 발전 방향을 제시한다. 이러한 보안 강화 방안들은 자산 회수 메커니즘의 안정성을 확보하고, 전반적인 시스템 보안성을 향상하며, 효율적인 성능을 유지에 기여할 수 있다. 나아가 향후 암호화폐 지갑은 보안 표준화와 법·제도적 기반 마련을 통해 신뢰성을 높이고, Web3 구현을 뒷받침하는 중심적인 기술 기반으로 확산될 것으로 예상한다.

1. 서론

최근 블록체인 기술은 비트코인과 이더리움 등 주요 암호화폐 거래의 기반 기술로 발전하며, 디지털 자산을 안전하게 관리하는 핵심 인프라로 자리잡았다. 그러나 현재 사용되고 있는 소프트웨어 지갑은 특정 블록체인 네트워크만 지원하며, 단일 프로세스 구조로 인해 하나의 침해가 전체 시스템으로 확산될 수 있는 위험을 내포하고 있다. 따라서 이러한 한계를 극복하기 위해 다중 블록체인을 지원하며 최신 기술 동향을 중심으로 보안성을 강화한 암호화폐 지갑 연구가 필수적으로 진행되고 있다. 본 논문은 암호화폐 지갑의 유형과 주요 문제점을 분석하고, 보안 강화를 위한 최신 연구 동향을 분석하여 효과적인 미래 발전 방안을 제시하는 데 목적이 있다.

2. 암호화폐 지갑의 유형과 특징

암호화폐 지갑은 사용자가 블록체인 네트워크에서 개인 키와 디지털 자산을 안전하게 보관하는 핵심 도구이다. 일반적으로 하드웨어 지갑과 소프트웨어 지갑으로 구분되며 구현 방식, 보안 수준, 편의성에서 서로 다른 특성을 지닌다[2]. 따라서 사용 목적과 환경에 따라 적합한 지갑 유형을 선택하는 것이 중요하다.

<표 1> 암호화폐 지갑의 유형과 특징

구분	장점	단점
하드웨어 지갑	- 높은 보안성 - 해킹 위험 최소화	- 높은 비용 - 낮은 사용 편의성
소프트웨어 지갑	- 우수한 접근성과 사용 편의성- 다양한 서비스 연계	- 해킹 공격 취약 - 개인 키 관리 위험 존재

3. 기존 화폐 지갑의 문제점

암호화폐 지갑은 블록체인 환경에서 디지털 자산을 관리하는 필수적인 요소이다. 그러나 기술의 빠른 확산에도 불구하고 여전히 여러 측면에서 다양한 한계를 지니고 있으며, 이러한 제약은 블록체인의 광범위한 활용을 저해하는 주요 과제로 작용한다. 주요 문제점을 정리하면 다음과 같다.

■ 보안 취약성 : 단일 프로세스로 인해 보안 침해 발생 시 전체 시스템 위험 노출 증가, 개인 키 분실·유출 시 자산 복구 불가
■ 관리 복잡성 : 다양한 블록체인 자산 관리를 위해 사용자는 여러 지갑을 운용해야 하는 단점
■ 법·제도 미비 : 국내외적으로 암호화폐 지갑 관련 법 기준과 정립이 미흡하여 신뢰성 부족
■ 네트워크 종속성 : 대부분 지갑이 특정 블록체인만 지원하여 범용성 부족

4. 최근 연구 동향 및 보안 강화 방안

블록체인 기반 암호화폐 지갑 시스템은 현재 보안 취약성, 사용자 관리의 복잡성, 네트워크 종속성 등 다양한 문제에 직면해 있다. 기존 지갑이 가진 문제를 해결하고 사용자 자산 보호를 위해 최신 기술 동향을 중심으로 암호화폐 지갑 시스템의 보안성 강화 방안을 고찰하고, 향후 발전 방향을 제시하고자 한다 특히, 제안하는 방안들은 [2]자산의 안전한 회수 메커니즘 확보, [1][3]시스템 보안성 향상, 그리고 [1]효율적인 성능유지에 중점을 두었다.

최근에는 여러 노드가 협력하여 암호화 연산을 수행하는 다중 노드 기반 보안 기법이 암호화폐 지갑의 신뢰성과 내구성을 강화하는 핵심 기술로 주목받고 있다. 대표적으로 첫째, 임계값 암호화(Threshold Cryptography) 기술은 하나의 비밀 키를 여러 노드에 분할하여 보관하고, 일정 수 이상이 협력해야 연산이 가능하도록 하여 단일 노드의 위험을 줄인다[2]. 둘째, 다자간 안전 계산(MPC, Multi-Party Computation 기술은 각 참여자가 자신의 입력값을 노출하지 않고도 공동 연산을 안전하게 수행할 수 있도록 하여 데이터 프라이버시를 강력하게 보호한다[2]. 셋째, 분산 키 생성(DKG, Distributed Key Generation) 기술은 중앙 기관의 개입 없이 여러 노드가 협력하여 키를 생성하고 보관하여 단일 실패 지점을 제거한다. 넷째, 멀티시그(Multi-Signature) 지갑의 성능 향상을 위한 연구도 진행되고 있다. 블룸 필터를 활용함으로써, 대규모 서명 검증 과정에서 저장 공간과 계산 비용을 줄이고 참여자의 프라이버시를 보호하는 방안이 제안되었다[2].

이처럼 혁신적인 다중 노드 기반 기법들은 암호화폐 지갑의 보안 수준을 한층 더 강화하는 핵심 기술로 폭넓게 활용할 수 있다.

5. 향후 발전 방향

향후 암호화폐 지갑 시스템의 발전은 여러 측면에서 이루어질 것으로 예상된다. 첫째, 사용자 경험(UX)의 향상이 요구된다. 다양한 환경에서도 사용자가 편리하게 이용할 수 있도록, 여러 플랫폼 간의 호환성과 직관적인 UI 설계를 갖추는 것이 중요하다[2]. 둘째, 지갑의 신뢰성과 안정성을 높이기 위해서는 국제적으로 인정받는 보안 인증 및 관리 기준을 수립하고 이를 표준화하는 작업이 필수적이다[3]. 마지막으로, 암호화폐 지갑은 단순히 자산을 관리하는 도구를 넘어, Web3 생태계의 주요 관문으로 자리잡을 것으로 예상된다. 이에 따라 지갑은 디지털 자산의 보관과 거래를 넘어, 분산 애플리케이션(DApp)과의 연동 및 탈중앙화 서비스의 확산을 지원하는 핵심 인프라로 발전할 것이다[1].

6. 결론

본 논문은 암호화폐 지갑의 기술적 진화와 기존 시스템의 한계점을 분석하고, 최근 연구 동향을 바탕으로 보안 강화 방안을 심층적으로 검토하였다. 결론적으로, 암호화폐 지갑의 신뢰성과 내구성을 확보하기 위해서는 [2]스마트 컨트랙트를 활용한 보호계좌 시스템, [1]다중 프로세스 구조의 적용, 그리고 [2]임계값 암호화·다자간 안전 계산(MPC)·분산 키 생성(DKG)과 같은 다중 노드 기반 보안 기법, [3]암호화 통신·합의 알고리즘 기반 보안 프레임워크가 핵심적인 요소로 작용한다. 이러한 기술들은 자산 회수 기능의 안정성 확보, 시스템 전반의 보안성 향상, 그리고 성능 효율성 유지에 실질적인 기여를 할 수 있다. 나아가 암호화폐 지갑은 단순한 디지털 자산 관리 도구를 넘어, [3]국제적 보안 표준의 도입과 법·제도적 기반 마련을 통해 사용자 보호를 강화하고, Web3 시대의 핵심 인프라로서 그 역할이 점차 확대될 것으로 예상된다. 이에 향후 연구에서는 다양한 블록체인 환경에서 제안 기법들의 성능 및 효율성을 실험적으로 검토하고, 최신 공격 기법에 대한 위협 모델링을 수행하며, 실제 사용자 데이터를 반영한 사용성 평가와 실증 연구를 진행할 계획이다.

사사 (Acknowledgement)
이 논문은 한경국립대학교 국립대학육성사업(2025) 지원을 받아 작성되었음

참고문헌

[1] 김혁수 외 3인,“보안성 강화된 다중 블록체인 지원 암호화폐 지갑 개발”, 한국정보통신학회논문지, 제29권 제1호, 2025, pp.99-107
[2] 이승석 외 2인,“이더리움 블록체인 기반 암호화폐 지갑 시스템 개발에 관한 연구”, 한국산업보안연구, 제12권 제2호, 2022, pp.69-88
[3] 유승재,“보안성 강화를 위한 블록체인기술의 활용과 개선방안 연구”, 융합보안논문지, 제23권 제1호, 2023, pp.63-80