

웨이브(Waves)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다.

WAVES 기술 백서



초록

WAVES는 맞춤형 블록체인 토큰 운영에 중점을 둔 탈중앙화 블록체인 플랫폼이다. 국가 통화의 전송은 규제 준수 게이트웨이 운영자를 통해 WAVES 블록체인에서 유지된다. 탈중앙화된 토큰 거래소는 블록체인 상에서 자금 조달,クラウド펀딩 및 금융 상품 거래를 용이하게 한다. 경량 클라이언트는 최종 사용자를 위해 간편한 설치 절차와 완전한 학습 곡선을 제공한다.

서론

‘가설: 블록체인 기술의 모든 가능한 응용은 시도될 것이지만, P2P 디지털 화폐는 여전히 가장 많이 사용되는 응용일 것이다.’

Ryan X Charles

‘블록체인 기술의 킬러 애플리케이션은 블록체인 그 자체이다.’

일반적 통념

출범 이후 블록체인 기술은 그 가장 자연스러운 응용, 즉 네트워크 토큰을 이용한 가치 전송을 둘러싸고 끊임 없는 논쟁에 휩싸여 왔다. 탈중앙화된 화폐는 혁신적인 발전이지만, 블록체인 기술을 이에만 한정할 수는 없다. 본질적으로 분산형 데이터베이스인 블록체인은 분산 원장 항목의 다양한 유형을 가능하게 하며, 그 성격은 블록체인 사용자의 해석에 따라 달라진다.

디지털 화폐의 기반으로서 블록체인을 도입한 것은 기술에 대한 큰 관심을 불러일으켰으며, 전 세계 규제 기관과 정부를 경계 태세로 만들었다. 비트코인이 유효한 통화 시스템으로 자리 잡을 것이라는 점은 의심의 여지가 없다. 그러나 현재 시점에서는 너무 많은 블록체인 토큰이 화폐로 사용되어서는 안 된다. 유동성 부족과 높은 변동성으로 인해 새로 등장한 블록체인을 안정적인 가치 저장 수단으로 사용하는 것을 방해하기 때문이다.

우리는 블록체인 기술이 제공할 수 있는 저수준 기능(예: 스마트 계약)보다는 종종 간과되는 블록체인 토큰의 다른 사용 사례에 초점을 맞출 것을 제안한다. 고전적인 컬러드 코인(colored coins) 접근법에는 매우 강력하지만 활용되지 않은 잠재력이 있으며, WAVES 플랫폼은 이를 최대한 실현하도록 설계되었다.

스마트 계약은 비트코인 스크립팅의 자연스러운 발전으로서 불가피하며, 블록체인 기술의 핵심 구성 요소 중 하나가 될 것이다. 반면, 특정 기능은 다른 접근 방식을 통해 훨씬 쉽게 구현할 수 있다. 블록체인 거래에 첨부된 형태로 실현된 맞춤형 토큰 운영은 매우 유연하며, 블록체인을 통한 국가 통화 전송에서 탈중앙화 거래에 이르기까지 다양한 응용에 사용할 수 있다. 이러한 운영에 초점을 맞추는 것은 Ethereum이 도입한 접근 방식을 잘 보완할 수 있을 것이다.[1]

이후 섹션에서는 WAVES 플랫폼 기능의 기술적 동기를 설명하고, 사례를 통해 이를 보여줄 것이다. 우리는 현재 블록체인 기술의 가장 “실제 생산에 즉시 적용 가능한” 측면을 규명하고 이를 현실 세계의 문제에 적용하는 것을 목표로 한다.

맞춤형 블록체인 토큰과 그 활용

기술적 동기

블록체인 자산과 컬러드 코인(colored coins) 접근법은 2013년경 등장했으며, 이때 비트코인 블록체인을 활용한 여러 프로토콜이 구현되었다. [4] [5] [6] 이와 별개로, 맞춤형 블록체인 토큰 플랫폼을 처음부터 구축하려는 시도도 여러 번 있었으며, 그중 가장 주목할 만한 것은 Nxt이다. [7]

우리는 Nxt가 구현한 접근법을 발전시켜, 블록체인 거래에 첨부된 추가 데이터(attachment)를 통해 맞춤형 토큰의 생성과 전송을 실현한다. 이 접근법은 새로운 거래 유형을 쉽게 구현할 수 있다는 명확한 장점이 있지만, 실제적인 관점에서는 필수적인 하드 포크 문제를 동반한다. 즉, 새로운 거래 유형을 추가할 때 네트워크 클라이언트 소프트웨어를 반드시 업데이트해야 하며, 이전 클라이언트는 새로운 거래 유형을 지원할 수 없기 때문이다.

WAVES는 핵심 소프트웨어 모듈에 포함되지 않고 그 위에 확장(extension) 형태로 설치되는 플러그인을 통해 새로운 거래 유형을 도입하는 확장 가능한 솔루션을 제공함으로써 이 문제에 접근한다. 관련 플러그인이 설치되어 있지 않은 클라이언트도 이러한 맞춤형 거래를 릴레이할 수 있다. 이 접근법은 서드파티 개발자가 새로운 거래 유형을 도입할 수 있도록 하며, 앱스토어(Appstore)와 유사한 생태계를 형성한다.

핵심 수준에서는 다음과 같은 가장 기본적인 거래 유형만 지원된다:

- 맞춤형 토큰의 생성, 삭제 및 전송
- 탈중앙화된 토큰 거래: 분산형 주문 매칭 엔진으로 구현되며, 네트워크 상의 Bid 및 Ask 거래가 서로 매칭된다
- 익명성 기능: 산업 수준의 거래 플랫폼에서는 익명 주문장이 반드시 필요하다

WAVES는 탈중앙화 블록체인 거래 측면에서 한 단계 도약하여, 하나의 맞춤형 토큰을 다른 맞춤형 토큰과 거래할 수 있는(자산 간 거래, asset-to-asset trading) 기능을 제공한다. 이를 통해 국가 통화와 연동된 토큰과의 거래를 포함한 새로운 기회를 열어주며, 전통적인 거래 인프라를 블록체인 상에서 재현할 수 있게 한다.

사용 사례

블록체인 상의 국가 통화

가치 전송을 위해 메인 네트워크 토큰을 사용하는 것은 매우 자연스러운 일이지만, 몇 가지 문제를 야기한다. 유동성이 낮고 변동성이 높은 토큰을 가치 전송에 사용하는 것은 상인들에게 명백한 단점을 가지며, 규제 기관과의 마찰을 초래한다. 그럼에도 불구하고 완전히 탈중앙화된 화폐는 실행 가능하며, 비트코인이 화폐로서 느리지만 꾸준히 채택되고 있다는 점이 이를 입증한다.

그러나 탈중앙화된 화폐가 가치 저장 수단으로 사용되는 것을 방해하는 변동성을 완화하고 충분한 유동성을 제공하기 위해서는, 화폐로 사용되는 토큰의 전체 수를 제한해야 한다(적어도 기술 개발의 초기 단계에서는). 이러한 이유로 우리는 화폐로서 비트코인만을 사용할 것을 강력히 권장한다.

외부 가치 전송 토큰 및 통화를 처리하는 우리의 접근 방식은 ‘Multigateway’ 접근법에서 비롯된다.[2] 비트코인의 경우, 비트코인을 해당 네트워크 토큰으로 교환하기 위한 입출금 절차를 유지하는 당사자(또는 다중 서명 당사자)가 존재한다. 따라서 우리는 WAVES 블록체인을 이용하여 비트코인 전송을 용이하게 한다.

이 접근 방식은 비트코인 자체의 한계로 인해 본질적으로 중앙화되어 있다. 이는 특정 시장 조성 절차를 통해 동적인 페깅을 제공하는 “시장 페그(market peg)” 접근 방식과는 대조적이다. 처음에는 시장 페그 방식이 금융 자산을 탈중앙화된 플랫폼에서 반영하는 데 적절한 방법처럼 보일 수 있지만, 자세히 살펴보면 숨겨진 중앙화 요소가 필연적으로 드러난다.

우리는 블록체인 기반 국가 통화와 BTC를 지원하는 과정에서 명시적으로 중앙화를 도입함으로써 기존 금융 기관에 새로운 기회를 열 수 있다. 그들의 역할은 법정화폐 자산에 대한 유동성 제공과 KYC/AML 절차 수행으로 축소될 수 있다. 결제 인프라의 유지 관리는 완전히 탈중앙화된 블록체인으로 아웃소싱된다.

이러한 블록체인 상의 국가 통화 제공 접근법은 Nxt 블록체인에서 CoinoUSD 토큰을 통해 처음 시도되었다. 이는 Ripple의 게이트웨이 방식과도 유사하다. 우리는 이러한 전략이 등장하고 있는 허가형(permissioned) 블록체인 접근법과 경쟁할 수 있으며, 오픈 블록체인 상에서 활동하기를 원하는 금융 기관을 유치할 수 있다고 믿는다.

클라우드펀딩, 탈중앙화 금융 상품 및 그 너머

우리는 블록체인이 금융적 요소에서 조직적 요소에 이르기까지 커뮤니티 기반 프로젝트의 대부분 측면을 관리하기 위한 효과적인 수단이라고 믿는다. 블록체인 기술은 본질적인 지연(latency) 특성으로 인해 고빈도 거래(high-frequency trading)를 지원할 수 없다. 아마도 밀리초 단위의 실행 시간을 요구하는 대규모 거래에서는 중앙화된 솔루션이 항상 더 선호될 것이다. 그러나 즉각적인 거래가 필요하지 않은 응용 분야에서는 블록체인이 매우 자연스러운 환경을 제공한다 — 예를 들어, 크라우드펀딩 토큰 발행이나 커뮤니티 내 금융 흐름 관리에 적합하다. 이러한 영역에서는 탈중앙화 솔루션의 활용이 유리하며, 중앙화는 특별한 이점을 제공하지 못한다.

향후 출시될 제품에 대한 대가로 일정 금액을 서약하는 킥스타터(Kickstarter)와 유사한 모델을 고려하면, 그 한계가 명확하다. 프로젝트 후원자는 자신의 프로젝트 “투자”를 다른 사용자에게 판매하여 빠져나올 수 없다. 반면 이러한 사용 사례는 블록체인 기반 시스템에서는 매우 자연스럽다. 여기서는 맞춤형 토큰이 설계 상 교환 및 전송될 수 있기 때문이다.

증권 발행은 대부분의 관할권에서 엄격히 규제된다. 일부 미래 토큰 가격에 대한 예측이 이루어지거나 토큰 발행자가 일정 배당금 지급을 약속하는 경우, 토큰은 증권과 연관될 수 있다. 그러나 블록체인은 규제에 무관한(regulation-agnostic) 도구이다. 블록체인을 증권 발행에 활용하고자 하는 법인이 현지 법률 및 규정을 준수한다면, 블록체인 상에서 증권을 발행하는 것은 주식 시장 상장과 마찬가지로 정당하다.

스타트업 자금 조달, 비공개 투자 배치(private placement) 및 벤처 단계 투자는 블록체인 기반 금융 상품이 가장 적합하게 활용될 수 있는 영역으로 보인다. 반면, 너무 높은 속도 요구 조건이 없는 한, 대규모 기업들도 청산(settlement)이나 결제(clearing)와 같은 특정 금융 업무에 이를 사용할 수 있다.

대부분의 관할권(미국 제외)에서는 일정 한도를 초과하지 않는 블록체인 기반 자금 조달이 완전히 합법적으로 수행될 수 있다. 미국의 지분 크라우드펀딩 법률은 간소화된 SEC 등록 절차를 통한 자금 조달을 허용한다.

엄격한 미국 증권법은 사기를 방지하기 위한 것이며, 이를 위해 미국 증권거래위원회(SEC)와 같은 강력한 중앙 감독 기관이 필요하다. 그러나 탈중앙화 기술의 발전은 커뮤니티 기반의 분산형 발행자 심사 메커니즘을 도입할 수 있으며, 이는 궁극적으로 중앙 집중식 규제 기관을 대체할 수도 있다.

WAVES 플랫폼의 주요 사용 사례 중 하나로 크라우드펀딩을 포함한다는 것은, 시스템 코어에 탈중앙화된 KYC/AML 형태가 통합되어야 함을 의미한다. 이를 위해 우리는 WAVES 블록체인 상에서 부정 행위자를 제거할 수 있는 탈중앙화 평판 시스템(decentralized reputation system)을 구현하고 있다.

경량 클라이언트, 이중 계층 아키텍처, 지분 증명(Proof of Stake), 그리고 사용성

기술적 동기

이중 계층 아키텍처와 경량 클라이언트

고전적인 비트코인 접근법은 본질적으로 공통 거래 로그를 통해 분산 시스템을 동기화하는 방식이다. 이 방식은 각 네트워크 노드가 전체 거래 내역의 복사본을 저장해야 하며, 이는 시간이 지남에 따라 확장성이 떨어진다는 결국 모든 노드가 전체 히스토리를 저장할 수 없게 되기 때문이다. 이를 완화하기 위한 다양한 방법이 존재한다 — 특정 노드에 필요한 데이터만 저장할 수 있도록 하는 단순 결제 검증(SPV) 절차, 오프체인 거래, 양방향 결제 채널, 블록체인 데이터 팽창 완화, 시스템 상태를 직접 다루는 방법 등이다. [8] 모든 노드가 체네시스 블록에서 동일한 조건으로 시작하는 가장 단순한 접근법에서는, 저장 용량이 낮은 노드가 전체 블록체인

을 저장할 수 있는 고성능 노드에 의존하게 되면서 사실상 중앙화가 발생할 수 있다. 결과적으로 이중 계층(two-tier) 아키텍처가 형성된다.

이것이 시스템을 본질적으로 중앙화시키는가? 그렇지 않다. 충분한 자원을 가진 새로운 노드는 언제든지 네트워크에 참여하여 전체 노드가 될 수 있기 때문이다.

물론 중앙화 경향이 나타나면 신뢰 문제가 발생한다. 경량 노드는 전체 노드를 신뢰해야 하며, 악의적인 전체 노드의 희생양이 될 가능성도 있다. 하지만 여러 노드에 대한 폴링(polling), 신뢰할 수 있는 노드 목록 유지 등의 방법을 통해 이를 완화할 수 있다.

WAVES 플랫폼은 전통적인 암호화폐 옹호자에게 다소 극단적으로 보일 수 있는 접근 방식을 채택한다. 경량 노드는 블록체인을 전혀 다운로드하지 않으며, 대신 전체 노드에 의존하여 결제 검증과 네트워크 상호작용을 수행한다. 이 접근 방식은 Nxt 플랫폼에서 1년 이상 성공적으로 운영된 SuperNET 라이트 클라이언트[3]에 기반한다.

WAVES는 Scorex 플랫폼[8] 위에 구축되어 있으며, 전체 거래 내역 대신 현재 네트워크 상태를 사용하는 접근법을 발전시키고 있다. 경량 노드용 단순 결제 검증(SPV) 절차가 구현되어 추가적인 보안 계층을 제공할 것이다. 시스템 상태는 경량 노드에 의해 다운로드될 수 있으며, 이를 기반으로 한 단순 결제 검증 절차가 수행된다.

지분 증명(Proof-of-Stake) 합의 및 스테이크 임대(Stake Leasing)

우리는 WAVES의 합의 알고리즘으로 지분 증명(Proof-of-Stake, PoS) 프로토콜을 선택했다. 이 선택은 Nxt에서의 성공적인 사용 사례와 이론적 근거에 기반한다. 동시에 우리는 거래 시간을 단축하고 거래 처리량을 높이기 위한 PoS 프로토콜의 향상된 형태인 임대 지분 증명(Leased Proof-of-Stake, LPoS)을 제안한다.

PoS 시스템에서 메인 네트워크 토큰 잔액을 보유한 각 노드는 해당 잔액에 비례하여 블록을 생성할 확률을 가진다. 이중 계층 아키텍처에서는 결제 처리를 전체 노드로만 이관하는 것이 논리적이다. 동시에, 잔액이 0이 아닌 모든 노드는 여전히 스테이킹 보상을 받을 자격이 있어야 한다.

스테이킹 노드 수 감소로 인한 보안 저하라는 이론적 문제는 경량 노드가 전체 노드에 명시적으로 잔액을 임대하는 방식으로 해결할 수 있다. 경량 노드는 신뢰할 수 있는 전체 노드에 잔액을 임대함으로써 온라인 상태를 유지하지 않아도 거래 수수료를 받을 가능성을 높이며, 전체 노드는 잔액 증가로 인해 블록을 생성할 확률이 높아진다.

계정 임대(account leasing)는 잔액 이전(balance transfer)과 동일하지 않다. 경량 노드는 여전히 자신의 잔액을 다른 노드로 전송하거나 다른 작업을 수행할 수 있다. 잔액을 임대함으로써 경량 노드는 실질적으로 네트워크의 결제 처리를 담당할 전체 노드를 선택하게 된다. 블록을 생성할 수 있는 노드의 수를 줄이면 확인 시간이 단축되고, 지연(latency)이 줄며, 시스템의 처리량이 향상된다.

경량 노드 구현과 브라우저 플러그인

경량 노드는 JavaScript로 작성된 브라우저 플러그인 형태로 구현된다. 이는 Scorex 기반의 전체 노드와 상호작용한다. 플러그인은 브라우저 앱 스토어에서 설치되며, 블록체인을 다운로드할 필요가 없기 때문에 사용자는 간단한 설치 절차 후 즉시 완전한 블록체인 기반 지갑을 사용할 수 있다.

지갑 인터페이스는 전통적인 온라인 बैं킹 또는 브로커리지 인터페이스와 유사하다. 통합된 국가 통화는 법정 화폐 단위로 표시된 본원적 가치 전송을 가능하게 한다. 블록체인과 법정화폐 간 교환은 신뢰할 수 있는 제공자에 의해 수행된다. 사용자가 국가 통화 토큰을 구매하면, 이를 다른 사용자에게 전송하거나 탈중앙화 거래소에서 거래할 수 있다.

자산 간 거래(asset-to-asset trading)는 USD, EUR, CNY 등과의 거래를 가능하게 함으로써 주식시장과 유사한 거래 인터페이스를 제공한다. 전반적으로 플랫폼의 인터페이스는 일반 암호화폐 클라이언트보다 전통적인 금융 인터페이스에 더 가깝다. 우리는 대부분의 사용자가 이미 익숙한 인터페이스를 제공하는 동시에, 블록체인 기술로 이를 강화하는 것이 중요하다고 본다. 사용자는 기존 금융 플랫폼으로는 할 수 없던 일을 수행할 수 있으며, 학습 곡선은 완만하게 유지되어 대중적 채택의 핵심 요인이 된다.

WAVES의 추가 핵심 기능

WAVES는 우선적으로 커뮤니티 기반 개발 및 프로젝트를 대상으로 한다. 이를 위해 탈중앙화된 투표 및 메시징 기능이 구현된다. 이를 통해 커뮤니티 프로젝트를 DAO와 유사한 방식으로 관리할 수 있으며, 기술적으로는 단순성을 유지한다.

WAVES는 맞춤형 토큰(자산)으로 네트워크 거래 수수료를 지불할 수 있도록 허용할 것이다. 관련 거래와 함께 자산을 메인 네트워크 토큰으로 교환하기 위한 주문이 탈중앙화 거래소로 전송되며, 그 주문이 실행된 이후에만 해당 거래가 다음 블록에 포함될 수 있다.

결론

WAVES 플랫폼은 초기 단계부터 대중적 채택(mass adoption)을 염두에 두고 구축되고 있다. 이 개요에서는 최종 사용자에게 이전에 없던 기회를 제공하고, 블록체인 기술의 빠른 도입을 위한 길을 닦을 수 있는 기술적 해결책을 제시하고자 했다.

참고문헌

[1] <https://github.com/ethereum/wiki/wiki/White-Paper>

[2] <http://multigateway.org/>

[3] <https://github.com/Tosch110/SuperNet-Lite>

[4] <https://github.com/CounterpartyXCP>

[5] <https://github.com/OpenAssets/open-assets-protocol>

[6] <https://github.com/OmniLayer/spec>

[7] <http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt>

[8] <http://arxiv.org/abs/1603.07926>