AOK WHITEPAPER

AOK Group

V.1.0

목차

목차

1. Introduction

1.1. Early technology

미국 벨코어 연구소(Bell Communications Research, Inc., Bellcore) 소속의 암호학자 슈트어트 하버(Stuart Haber)와 스콧 스토네타(Scott Stornetta)는 암호학 저널(Journal of Cryptology)에 1991년 9월, '어떻게 디지털 서류에 타임 스탬프를 찍을 것인가(How to timestamp a digital document)' 라는 논문을 발표하였다. 이들은 논문에서 디지털 문서에 타임 스탬프를 찍어 신뢰성을 증명하는 '타임스탬프' 개념을 처음으로 기술하였다. 이들은 암호 해싱 알고리즘을 사용해 각 문서의 고유 ID를 생성하여 문서가 변경될 때 마다 ID 역시 변경되는 'Surety'라는 타임 스탬프 서비스를 소개했다. 또한 Surety는 풀이된 고객 인감으로 구성된 '범용 레지스트리 데이터베이스'를 호출하는 방식으로 모든 고객의 '위조 불가' 인감 원장을 발명했다. 또한 이들은 매주 새롭게 분류되는 해시 값을 미국 뉴욕타임스의 작은 광고 섹션에 게재하며 블록체인 기술의 첫 번째 사례를 완성했다.

그에 이어 1998년 엔지니어인 웨이 다이(Wei Dai)는 초기 단계의 암호화 거래시스템인 전자 분산원장 시스템에 기반한 B-money라는 최초의 전자거래 분산화 솔루션을 개발하게 되었다. B-money는 모든 암호화폐의 뿌리가 되는 기본 개념을 제안하였다. 중앙화된 기관을 통하지 않고 P2P방식으로 참여자들끼리 직접 거래를 할 수 있도록 한 점, 분산원장 개념을 도입해 거래 기록을 모든 참여자들이 공유하도록 한 점, 새로운 블록을 성공적으로 생성한 사용자에게 보상으로 코인을 지급하도록 한 점 등 현재의 암호화폐에서 사용되는 중요한 개념들을 제시하였으나 실제로 구현되지는 못하였다. 왜냐면 블록체인 기술을 기반으로 한 것이 아니라 블라인드 서명과 같은 암호화 기술을 접목한 전자화폐였기 때문이다. 따라서 Satoshi Nakamoto의 논문에서 참고될 정도로 기본적인 중요한 개념들을 제시한 것에 의미가 있다.

> The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

Excerpts of How To Time-Stamp a Digital Document

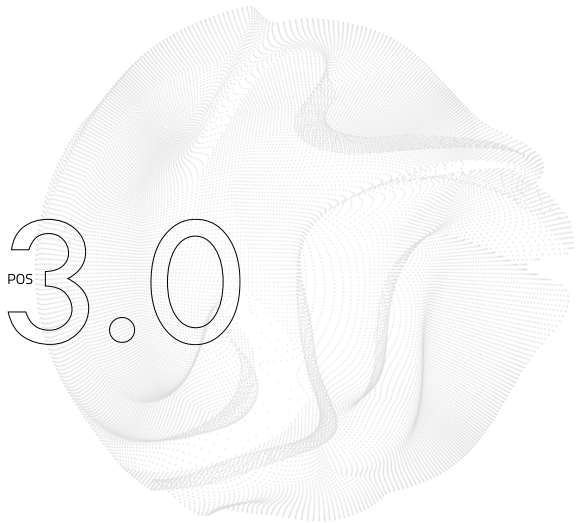
1. Introduction

1.2. Implementation and Development

블록체인 기술은 '분산원장'의 기본적인 개념을 구현한 비트코인의 1세대를 넘어 원장 속에서 계약의 기능을 더한 스마트 컨트랙트(Smart contract)기능을 특징으로 하는 이더리움의 2세대로 진화하였다. 1세대로 불리우는 대표적인 블록체인인 비트코인은 합의제의 거버넌스로 구성되어 시스템 업그레이드가 어려운 구조이다. 또한 작업증명(PoW: Proof of Work) 방식이기 때문에 채굴 이익과 관련하여 채굴업자들의 이해관계에 좌우되어 탈중앙화 개념이 손상받는 문제도 발생하였다.

컴퓨팅 파워를 제공하는 업자들의 힘이 강해지면서 발생한 일이었다. 이더리움은 데이터 처리 용량 증가에 따른 속도지연이 큰 문제로 대두되었고 전송수수료인 가스비(Gas Fee)의 증가로 인한 거래 비용 증가 문제가 대두되었다.

이러한 1, 2세대 메인넷은 모두 PoW방식으로 블록생성을 하므로 근본적으로 컴퓨팅 파워와 전기자원의 과도한 소비 문제를 안고 있을 수 밖에 없게 되었다. 따라서 이더리움 2.0 에서 PoS (Proof of Stake)방식으로 전환을 시도하고 있으나 2020년 11월 현재, 여전히 해결되지 못하고 있는 실정이다.



1.3. Solutions

AOK는 이러한 1세대, 2세대 블록체인의
단점을 보완한 제 3세대 메인넷(MinNet)으로
PoS 3.0 방식의 합의 알고리즘을 사용한다.

PoS 3.0은 Wallet을 오프라인 상태로 한 – node에 참여하지 않는 – 코인 보유자에게는 블록 보상을 주지 않고, node로 참여한 wallet 중 코인을 더 많이 스테이킹(Staking)한 보유자에게 블록 보상을 받을 수 있는 확률을 높여주는 합의 체제를 가지고 있다. 이는 기존의 PoS 방식이 코인을 더 오래 스테이킹한 wallet에 보상을 받을 확률을 높여주면서 발생하게 된 Coin-Age 문제를 해결한 방식이다.

AOK는 이러한 방식으로 기술적인 안정성, 효율성, 분산화는 물론, AOK 메인넷 코인을 기축통화로 하는 토큰(token) 발생도 가능하여 이를 통해 개별 프로젝트들이 eco-system을 구축하고, 개별 DApp들의 활성화에 따라 AOK 메인넷 코인도 value가 높아지는 선순환구조를 가지고 있다.

2. AOK MainNet

2.1. Overview of Development

AOK는 가장 전통적이며 체인의 안전성을 인정받은 비트코인의 블록체인 기술을 계승하여 보안성을 확보하고, PoS 3.0 합의 알고리즘을 통해 비트코인의 합의 알고리즘인 PoW 방식의 단점을 개선하고 비트코인의 최대 약점인 느린 처리 속도를 보완하여 목표 블록타임을 기존 20분에서 1분으로 줄여 거래의 속도를 높여 빠른 전송 속도를 보장하고, 가장 개선된 합의 알고리즘인 PoS 3.0을 통해 블록 검증을 위해 과도한 장비와 전기 에너지를 소모하는 비트코인, 이더리움에 비해 경제적이면서 안전한 블록검증이 가능한 합리적인 구조의 특징을 가지고 있다.

지분 증명에 대한 보안은 다년간의 시험을 통해 이미 입증되었으며, AOK의 PoS 3.0은 CoinAge와 블록보상 및 블록체인 사전계산 문제를 동시에 해결하였다. PoS 3.0 프로토콜은 강력하며 활성 노드를 권장하여 노드를 네트워크에 지속적으로 연결하게 한다. 이 문서에서는 기존 PoS 합의 알고리즘의 보안이슈와 해결책을 제시하고 AOK의 보안을 더욱 강화할 수 있는 아이디어를 기술한다.

2. AOK Main-Net

2.2. PoS 3.0

2.2.1. 기존의 합의 알고리즘

블록체인 시스템은 네트워크에 참여하는 모든 참여자들이 동일한 데이터를 각각 보유하며, 같은 데이터를 분산 저장하기 때문에 원본과 사본의 구별이 존재하지 않으며 통일된 의사결정을 내릴 수 있는 중앙이 존재하지 않게 된다. 이러한 상황에서 합리적이고 효율적인 의사결정을 내릴 수 있는 다양한 알고리즘이 개발되었다. 이러한 합의 알고리즘을 통해 분산원장이 데이터의 일관성을 이루게 되는데 이러한 합의체제(컨센서스)에는 작업증명 방식(PoW; Proof of Work)과 지분증명 방식(PoS; Proof of Stake), 위임지분증명 방식(DPoS; Delegated Proof of Stake) 등 이 있다.

대표적인 PoW 코인인 비트코인 네트워크에서 채굴자가 거래 검증 과정에 참여한다. 채굴자는 해시값을 계산하여 블록을 발견하여 네트워크에 보고하고 이에 따른 블록 보상을 통해 채굴이 진행된다. 이러한 PoW 합의 알고리즘은 일정한 블록생성을 위해 동적 난이도의 개념을 도입하였다. 이는 각 노드의 해시 파워(hash power)의 증감으로 블록 경쟁이 시작될 경우 실행되며, 해시 파워가 증가할 경우 연산 난이도가 증가하며 반대로 해시 파워가 감소할 경우에는 연산 난이도가 낮추어 진다.

즉, 채굴보상을 얻기 위한 채굴에 참여하는 컴퓨팅 파워가 적으면 난이도가 낮아지고, 많으면 난이도가 높아지는 것이다. 그러므로 암호화폐의 채굴 경쟁이 점점 더 치열해짐에 따라 채굴 난이도는 계속하여 상승하고 있다. 채굴 난이도가 상승한 다는 것은 투입되는 해시 파워의 양도 증가하는 것을 의미하며 늘 동일한 해시 파워로는 암호화폐를 채굴하기가 점점 더 어려워지는 것을 의미한다. 또한 채굴 난이도가 높아지면 이전과 동일한 블록을 생성하기 위해 더 많은 해시레이트(hashrate)를 필요로 하게 되고 과거와 동일한 수준으로 채굴하기 위해서는 채굴장비에 대한 지속적인 성능 업그레이드 비용 및 막대한 전기 비용 등 상당한 비용을 투자해야 하는 것이다. 이는 필연적으로 자원 낭비를 가져오게 되었다.

2.2.2. PoS 3.0 합의 알고리즘

비트코인은 '비잔틴 장군의 문제'를 해결함으로써 Peer-to-Peer 네트워크 구조가 위조와 변조를 방지할 수 있는 솔루션이라는 점을 보여주었고, 그 이후 많은 암호화폐가 Bitcoin가 공개한 오픈소스를 기반으로 만들어졌다. AOK 역시 Bitcoin의 안정된 오픈소스를 계승하여 필요한 차세대 기능을 추가하여 개발하였, 오픈소스 규칙에 따라 AOK 역시 자사의 Github 채널에 수정된 소스코드를 공개하는 투명한 Public Open-Source Public Blockchain이다.

AOK가 도입한 PoS 3.0 합의 알고리즘은 과도한 컴퓨팅 파워로 인한 전력과 장비 비용의 낭비를 지양하는 장점을 가지고 있다. AOK는 기본 합의 방식을 위해 최신의 비트코인 코어를 기반으로 PoS 3.0를 로직을 도입하여 합리적이고 경제적인 블록 생성을 실시한다. 일반적인 PoS 합의 로직은 Coin-Age 공격 및 여러가지 유형의 공격으로 인하여 다양한 보안 이슈를 가지고 있어 AOK는 개선된 PoS 3.0을 합의 로직으로 채택하고 있다.

2. AOK MainNet

PoS의 아이디어는 최초로 PeerCoin에서 구현되었고 이는 다시 BlackCoin에서 PoS 2.0의 개념으로 발전하여 이후 QTUM 등 일부 암호화폐 플랫폼이 PoS 3.0 알고리즘으로 발전시켰다. PoS의 지분 증거는 본질적으로 코인 보유자 간의 코인 보유량의 경쟁으로 치환되며 네트워크 연결성과 무작위 우연에 기반하여 확률적으로 코인을 보상받을 수 있다. 보상을 받을 확률은 얼마나 많은 코인을 스테이킹하는 가에 달려있는데, 보상을 받고나면 해당 지분은 일정기간 검증에 참여하지 않도록 하면서, 대량지분의 노드의 독식을 제어한다. 이는 비트코인의 에너지 낭비 문제를 해결하면서 네트워크 보안에 대한 새로운 도전 과제를 제시한다. AOK는 이 프로토콜 장점에 대한 기술적 구현을 실현하고 기존의 이론 창시자를 존중하고 잠재적인 개선점 및 단점에 대해서도 보완하고자 한다. AOK는 PoS 3.0이 현재 가장 안전하고 진보된 효율적인 블록 생성방식이라고 판단하여 PoS 3.0 합의 알고리즘을 구현하기로 결정하여 제작에 이르게 되었다.

2.3. Block Reward

기존의 PoS 시스템의 대부분의 증명에 대한 보상은 불행히도 Coin Age를 기반으로 했고, 이론적으로 이것은 노드가 잠정적인 지불을 받을 수 있게 함으로써 공정하게 관심을 분배하며 이는 공통된 이율을 유지하려는 시도이다. 또한 노드가 연결 상태를 유지할 수 있는 인센티브를 제공하지 않았다. 분산 시스템에서는 신뢰가 단일 엔티티에서 네트워크 자체로 이동하기 때문에 더 노드의 양이 많을 수록 보안을 강화된다.

AOK는 이런 문제를 해결하기 위해 PoS 3.0의 해법으로 블록 보상은 블록 당 4 AOK로 코인 생성 보상을 일정하게 유지하고, 노드로 일정 시간이상 참여했을 때만 블록보상의 대상으로 참여를 할 수 있게 설계되었다. 이런 방식은 노드로의 참여를 늘려 탈중앙화를 유도하고 안전한 네트워크와 인플레이션을 안정적으로 유지하는 효과가 있다.

2.4. Coin-Age Problem

2.4.1. 보안문제

지분 증명은 해당 코인을 많이 가지고 있는 (지분을 많이 보유한) 만큼 블록에 대한 유효성을 검증할 확률이 높아지는 구조인데, 코인 보유를 증명하고 코인의 보유 수량만큼 블록 보상을 가져갈 확률을 높인다. 이로써 더 많은 사람들이 더 많은 블록보상을 가져가기 위한 경쟁을 유발한다.

Coin Age는 코인을 오래 두면 블록발견 확률이 높아진다는 이론으로 원래의 의도는 코인을 보유하고 있는 사람들에게 동기를 부여하는 것이었으나 이는 보상이 증가할 때까지 기다리기만 해도 그 확률이 높아지기 때문에, 노드들이 실제로 네트워크에 계속 연결되어 있도록 하는 것을 권장하지는 않는다. 이런 문제로 오랜 기간 네트워크와 연결을 끊고 다시 접속하여 네트워크에 대한 51% 공격을 감행할 수 있는 가능성을 열어 두었다. 이처럼 연결된 노드가 적을 수록 합의를 이루는 블록의 대부분을 얻는 것이 쉬워지며 이러한 공격을 효과적으로 하기 위해 필요한 코인의 개수를 미리 계산할 수 있었다.

2. AOK Main-Net

2.4.2.스테이크 그라인드 공격(Stake grinding attack)에 대한 방어

시간의 증가에 따른 Coin Age 블록보상의 제거는 보안성의 개선을 가져왔다. 따라서, 고정하는 노드의 양이 감소는 끊어진 노드에 비례하여 증가한다. 예를 들어, 네트워크의 1/4 만이 스테이킹을 하고 있다면 보상은 보유량의 최대 5 배를 기대할 수 있게 된다. 많은 코인에는 노드가 충분하지 않기 때문에 소규모 보유자에게도 큰 이점이고 일반적으로 홀더의 20 % 미만인 것이 현실이다. AOK는 이러한 인센티브의 증가가 노드의 경쟁력을 확실히 유지할 것이라고 생각하며 “스테이크 그라인드 공격”을 방지하는 데 유용하다고 판단하고 있다.

이 공격의 확률에 대한 좋은 분석은 Neucoin에서 수행되었다. Neucoin의 주장은 비트코인 네트워크의 모든 해싱 파워를 사용하더라도 공격이 불가능하다는 것이다. 그러나 몇 분 Roll-back하면 새로운 사용자가 네트워크에 어떤 체인을 연결할 지 확신할 수 없게 되는데, Stake 시스템은 “Check pointing”을 사용하여 기본적으로 주 개발자가 이 작업을 시도하는 체인을 선택할 수 있도록 중앙에서 제어한다. 물론 이것은 이상적인 솔루션이 아니다. Coin Age 제거는 일반적으로 안전한 결정이었으며, 타임 서버를 검사하는 하이브리드 시스템을 수행하여 드리프트를 계산하고 노드가 일반적인 시간 합의와 밀접하게 동기화하도록 요구할 수 있었다. 블록 체인 자체에 기초한 다른 무작위 인자의 추가도 고려 사항 일 수 있다.

2.4.3. 문제 해결

Coin Age는 사용되지 않은 코인의 양과 보유 시간에 의해 계산되는데 최초의 PoS코인인 PeerCoin에서 도입한 개념으로 사용하지 않은 코인의 수와 보유한 기간을 곱한 만큼의 값으로 네트워크에서 가장 오래된 체인을 만들면 그 체인이 블록으로 등록되는 방식이다.

Coin Age는 첫 번째 블록보상을 받은 후 재설정되기 때문에 연속적인 이중 지출을 수행하기가 매우 어렵 기 때문에 Coin Age를 구하기 위한 공격이 이전에 불가능하다고 설명되었다.

그러나 입력이 수많은 출력으로 분할될 수 있기 때문에 이는 명확하지 않으며, 연속적인 이중지출 공격의 가능성을 줄 수 있었고 이는 공격자가 네트워크보다 큰 가중치를 유지하기 위해 상당한 금액의 자금을 필요로 하기 때문에 여전히 어려운 문제이다. 이론상으로는 매우 합리적이라 볼 수 있다.

AOK와 다른 인기있는 PoS 방식을 사용하는 시스템의 포크양을 보면 노드의 양이 상당히 적다는 사실을 알 수 있는데, 이는 소수의 소수 노드에 더 큰 비중을 둔다는 것을 의미한다, 많은 양의 코인을 소유한 사람은 코인의 가치가 심각하게 낮아질 수 있기 때문에 이 공격을 수행하기를 원하지 않을 수 있기 때문이다. Coin Age는 여전히 중요한 공격이 가능한 루트이며 매 순간 새로운 블록이 생성될 때 마다 코인이 발행되기 때문에 보안을 위해 가능한한 많은 노드를 연결하는 것이 필수적이기 때문에 PoS 2.0 부터 이 개념이 제거되었다. 따라서, AOK는 Coin Age를 통한 공격으로부터 자유롭다

2. AOK Main-Net

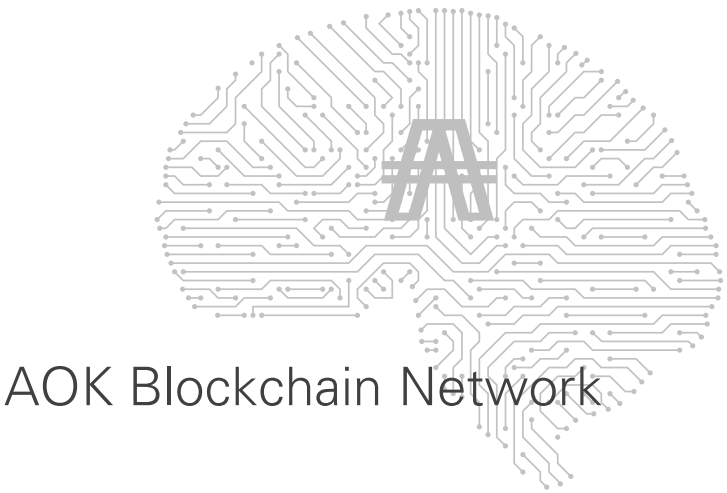
2.5. Multi signature Staking

프로토콜에 주목할 만한 추가 사항은 “다중 서명 스테이킹 (Multisignature Staking)”의 구현이다. 많은 PoS 알고리즘의 단점은 단일 키로 Stake를 지원한다는 것이다. 따라서 “2중 에스크로” 라고도 하는 단일 에스크로 시스템과 보다 안전한 이중 키 계정을 사용하는 한 계정을 네트워크 보안에 참여하도록 하는 것이 중요해졌다.

또한 P2SH를 이용하는 방법도 있다. P2SH(Pay To Script Hash)란 공개키가 아닌 스크립트 해시에 지불하는 개념으로, 하나의 공개키를 해싱하는 것이 아닌 공개키 해시 대신 스크립트 해시로 트랜잭션을 보낼 수 있다. 이러한 멀티시그 스테이킹이 중요한 이유는 단일 키 계정에서는 해커가 key logger를 사용하여 암호를 알아 내고 스테이킹을 위해 잠금이 해제 되어있는 동안 지갑을 손상시킬 수 있다는 것이다.

PoS 3.0 증명의 해법 : 사용자는 번지 주소로 알려진 출력에 블록 서명 키를 두어 표준 트랜잭션을 보내서 스테이크 할 수 있다.

이를 통해 모든 입력을 제출할 수 있고, 이로써 AOK는 소프트웨어, 투표 및 “Cold Staking”에 대한 큰 이점을 준다. 콜드 스테이킹 (Cold Staking) 기술에는 여러 대의 컴퓨터가 필요한데, 기본적으로 다중 서명 입력이 스테이킹에 적합 할 경우 서명은 여러 컴퓨터 간에 분할된다. 이로 인해 하나의 키가 손상된 경우에도 로컬 네트워크나 여러 서버에서 완전히 다른 위치에 있기 때문에 계정을 해킹하는 것은 사실상 불가능하며 이 기술은 BlackHalo의 최신 릴리스에서 이미 구현되고 있다.



2. AOK Main-Net

2.6. Payment System

2.6.1. UTXO

AOK는 비트코인의 결제 시스템인 UTXO를 사용한다. UTXO는 Unspent Trasaction Outputs의 약자로서, 미사용 트랜잭션 출력값을 의미한다. 비트코인은 이더리움의 '계좌 잔고모델'(Account Balance Model)과는 달리 계정이나 잔고가 없고, 블록체인에 기록된 '소비되지 않은 출력값'을 통해 거래의 유효성을 검사하여 코인의 존재 여부를 확인한다.

2.6.2. UTXO 동작 구조

AOK는 누군가로부터 받은 금액을 UTXO로 저장한다. 예를 들어, A와 B로부터 각각 2AOK와 3AOK를 받아 총 5비트코인을 갖게 되었으면, 지갑에는 5 AOK로 저장되지 않고, 각각 2 AOK, 3 AOK의 UTXO로 구분 저장된다. 그리고UTXO 안에 있는 금액을 송금할 경우에는 새로운 UTXO를 생성하여 기존의 UTXO는 파기된다. 즉 3 AOK가 있는 UTXO에서 2 AOK를 타인에게 송금하면 2AOK를 송금한 AOK와 남겨진 1 AOK에 대한 UTXO가 새로 생성된다.

2.7. Asset Function

2.7.1. 자산 발행과 거래

AOK의 토큰 이름은 중복될 수 없으며, 해당 이름으로 토큰을 발행하는 첫번째 발행자가 해당 프로젝트의 소유자가 된다. 발행자는 발행된 수량, 데시멀 (decimal, 소수점 자릿수), 향후 동일한 토큰을 더 많이 발행할 수 있는지 여부를 결정하고, 토큰을 QT 지갑에 통합하고 토큰 관리 기능을 제공하는 새로운 RPC 호출을 만들면 새로운 자산 토큰을 쉽게 발행하고 현재 잔액을 알려주며 다른 사용자에게 자산을 전송할 수도 있다.

2.7.2. 다양한 활용

AOK는 기업, 재단, 개별 프로젝트, 조합 또는 파트너쉽을 대표하는 프로젝트 토큰을 발행할 수 있다.

각 토큰에 대한 규칙은 해당 토큰 발행자에 따라 달라질 수 있으며 기록 보관은 작업이 분산된 AOK 블록체인 상에서 이루어지게 되므로 다양한 종류의 참여 구조를 적용하고 효율적으로 사용될 수 있다. AOK 메인넷 코인 기반의 토큰을 통해 유저들은 새로운 세계 경제에서 더 많은 자산 거래를 할 수 있게 되고 그에 대한 비용은 낮아질 수 있다. 또한 유저들은 AOK 토큰을 사용하여 고유 자산과 그 유효성을 보다 효율적이고 공공연하게 증명할 수 있게 된다.

2. AOK Main-Net

2.7.3. 자산발행의 조건

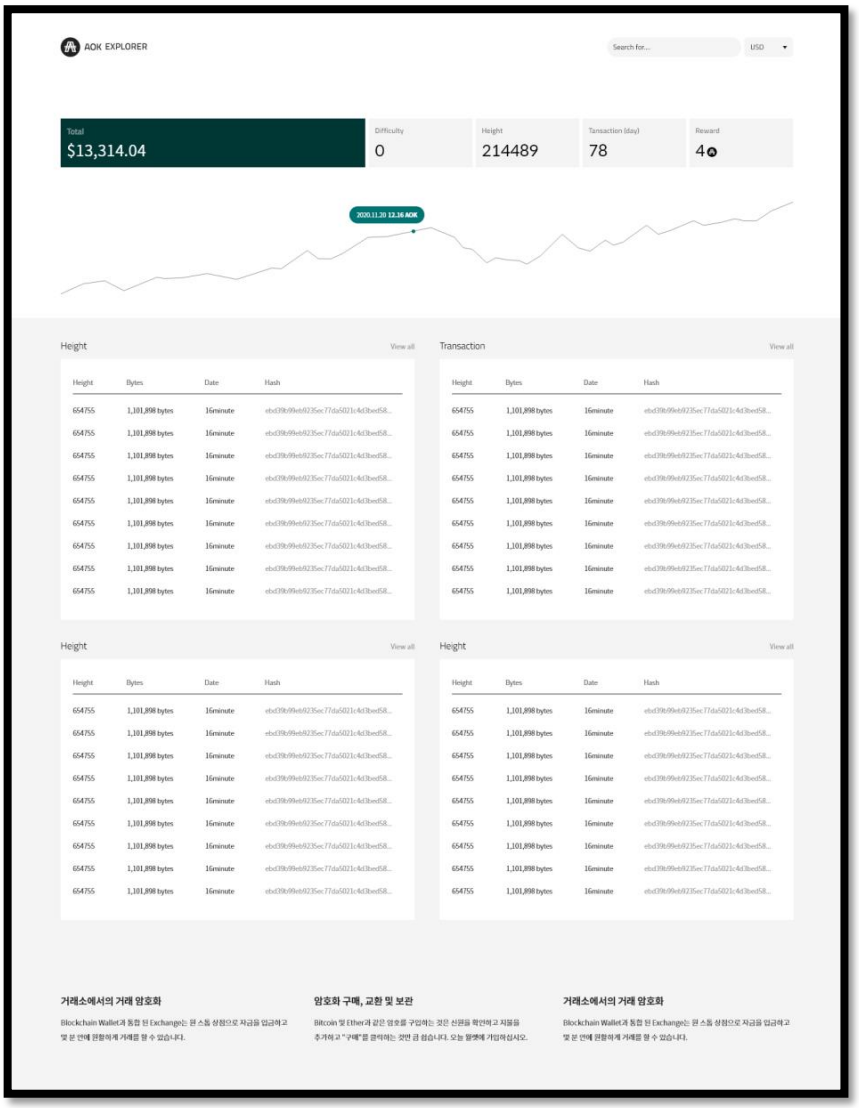
AOK는 무분별한 자산의 생성을 방지하기 위하여 새로운 자산을 토큰 형태로 생성하려는 경우 일정 수량의 AOK 메인넷 코인을 특정 주소로 전송하여야 하는 로직으로 개발되었다. 자산의 이름은 고유하며 자산의 단위나 총량은 자산 발행인이 결정하여 발행할 수 있다. 발행된 토큰은 이더리움의 ERC20 토큰과 유사한 방식으로 이용될 수 있으며, AOK 메인넷 네트워크에서는 기존 ERC20 이더리움 토큰의 복잡한 사용법이 아닌, 비트코인 방식의 명령어 체계에 따라 보다 직관적인 사용이 가능하도록 개선되었다.

그리고 특정 수량 이상의 토큰을 생성하기 위해서는 투표나 인증을 의무화하여 스팸과 같이 자산의 형태인 토큰이 무분별하게 난발되는 것을 방지할 수 있다. AOK의 메인넷이 더욱 안전한 고유자산을 허용함으로써 AOK의 메인넷 블록체인 생태계는 더욱 더 확장될 수 있으며 다양한 목적과 형태의 DApp 개발이 가능해지도록 개발되었다.

2.8. Transaction Fee

AOK 메인넷 네트워크에서 트랜잭션이 발생하는 경우 수수료는 최소 0.0001 AOK부터 발생하여 네트워크의 혼잡도에 따라 가변적으로 조절된다. 해당 블록에 사용된 모든 블록보상과 함께 블록을 발견한 스테이크 노드에 지급된다.

3. AOK Explorer



3.1. Explorer Overview

AOK는 빠르고 안정적인 블록 검색을 위해 독자적인 모델의 블록체인 탐색기를 서비스 하고 있고, Github를 통해 소스코드를 공개하고 있다. 이 AOK 블록체인 탐색기는AOK의 블록, AOK 주소, 거래내역 및 AOK 네트워크를 사용하는 서브토큰에 대한 기록을 자세하게 제공하고 있다.

3.2. Explorer Address

AOK 익스플로러의 접속 주소는 다음과 같다.

https://explorer.aok.network

4. AOK Wallet

4.1. Wallet Overview

AOK의 메인넷 코인 및 토큰을 저장, 전송, 관리할 수 있는 QT 지갑이 개발 완료되어 Github에 공개되어 있다.

4.2. Windows / MacOS / Linux

4.2.1. Windows OS

AokChain-Windows.zip
AokChain-Winows-Qt.zip

4.2.2. Apple Mac OS

AokChain-macOS.zip
AokChain-Qt.dmg

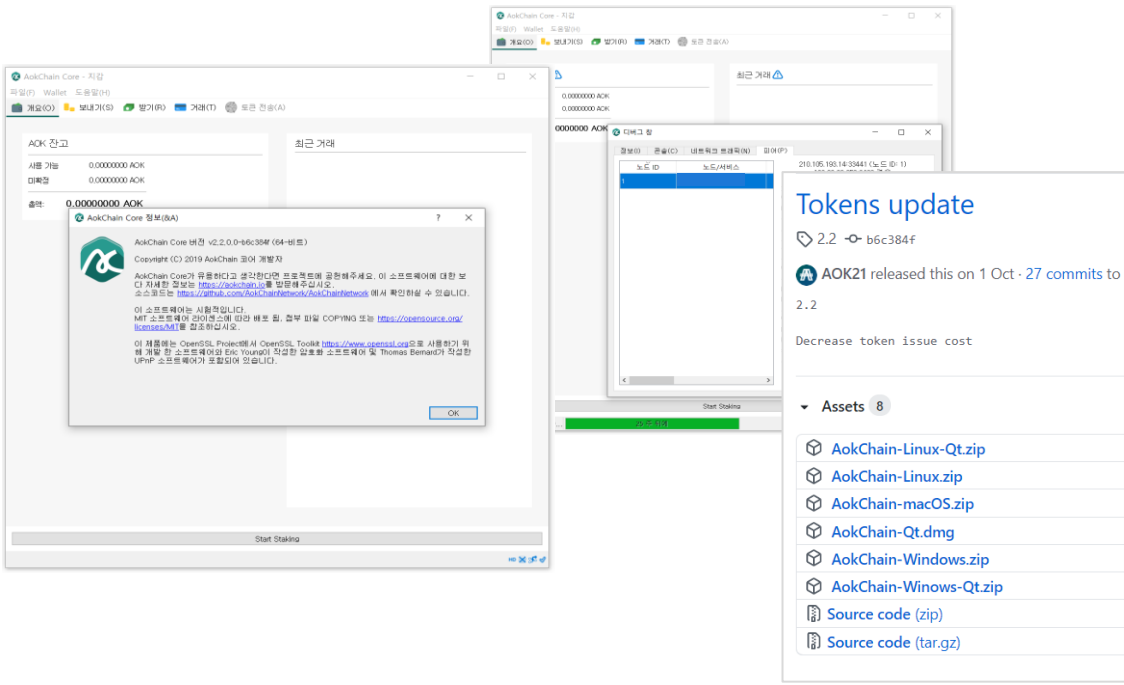
4.2.3. Linux

AokChain-Linux-Qt.zip
AokChain-Linux.zip

4.3. Wallet Address

AOK Wallet를 받을 수 있는 주소는 다음과 같다.

https://github.com/AokChain/AokChain/releases



4. AOK Wallet

4.4. QT Wallet Information

설치하고자 하는 OS에 맞는 Wallet 프로그램을 실행한다.

4.4.1. Wallet 실행

Wallet을 실행하면 프로그램은 자동으로 Block Sync를 시작한다. 프로그램의 하단에서 Sync 과정을 확인할 수 있다.

4.4.2. Wallet 표시화면 설명

Spendable: 현재 보낼 수 있는 코인의 수
Stake Weight: 스테이킹에 사용 중인 코인의 수
Immature Stake: 스테이킹 후 받은 블록 보상이 지갑에 반영될 코인의 수
Unconfirmed: 전송 후 confirm 대기 중인 코인의 수 (최소 1 confirm 이상 필요)

4.4.3. Wallet 암호 설정

Wallet 화면 상단에서 [설정〉〉지갑 암호화]를 선택하여 암호를 설정한다. 설정된 wallet 암호는 변경이 가능하나, 암호 자체를 잊어버린 경우에는 복구가 불가능하다.

4.4.4. 주소생성

Wallet을 실행하면 기본적으로 하나의 주소가 생성되며, 이 외에도 사용자가 원하는 만큼의 주소를 추가적으로 생성할 수 있다. 지갑 좌측 메뉴 중 Receive를 선택하면 생성된 주소가 나오며, 하단의 New Address 버튼을 통해 새로운 주소를 생성할 수도 있다.

4.4.5. 코인전송

Wallet 좌측 메뉴 중 Send 메뉴를 선택하면 코인을 전송할 수 있는 화면이 나타난다. 코인을 받을 상대의 wallet 주소와 코인 수량을 입력하고 하단의 보내기 버튼을 선택한다. 지갑에 암호를 설정한 경우에는 암호 입력창이 나타나며 암호 입력 후 코인 전송이 가능하다.

송금 수수료는 wallet 상단의 [설정〉〉옵션〉〉메인]에서 설정이 가능하다. 하단의 수령인 추가하기 버튼을 선택하면 주소 입력창이 추가되며, 이를 통하여 한번에 다량의 거래가 가능하다.

4.4.6. 거래내역확인

거래 메뉴는 wallet 내에서 이루어진 모든 거래 내역을 제공하며 옵션 설정을 통해 원하는 거래 내역을 간단하게 조회할 수 있다.

4. AOK Wallet

4.4.7. 주소록

Address Book 메뉴는 자주 사용하는 주소를 저장할 수 있으며 이 기능을 이용 하여 코인 전송 시 미리 저장한 주소를 불러와서 처리하는 것이 가능하다.

4.4.8. Staking (PoS Mining)

Wallet에 코인이 들어있는 경우 PoS Mining이 가능하다.

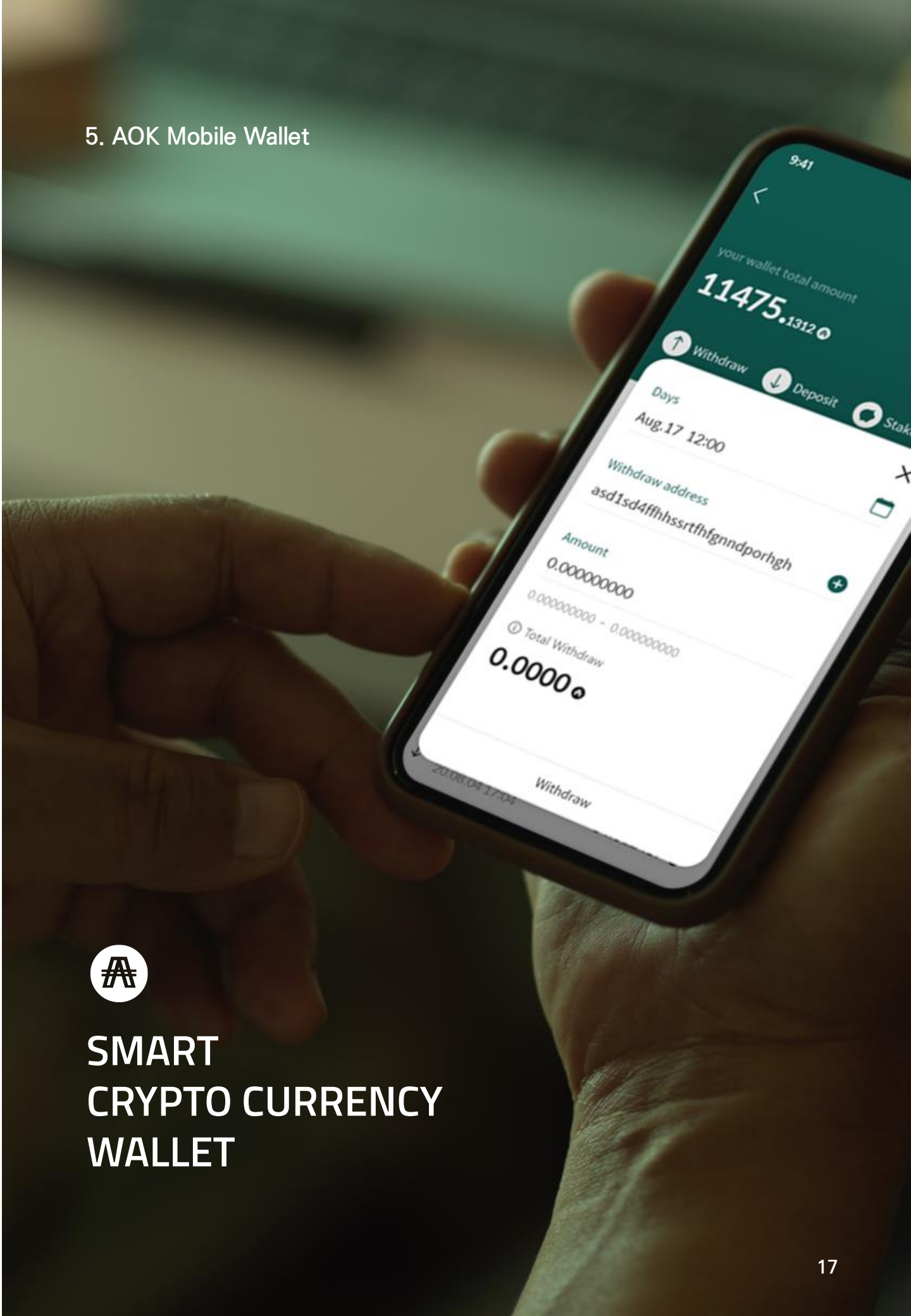
4.4.9. Backup

Backup 파일을 생성하여 유사시 wallet을 복구할 수 있다.

4.4.10. Restore

기존의 data를 손실한 상황에서 지갑을 열면 새로운 wallet이 생성된다. 이 경우 위에서 만든 backup file을 wallet이 설치된 경로로 이동하여 wallet을 복구할 수 있다

5. AOK Mobile Wallet



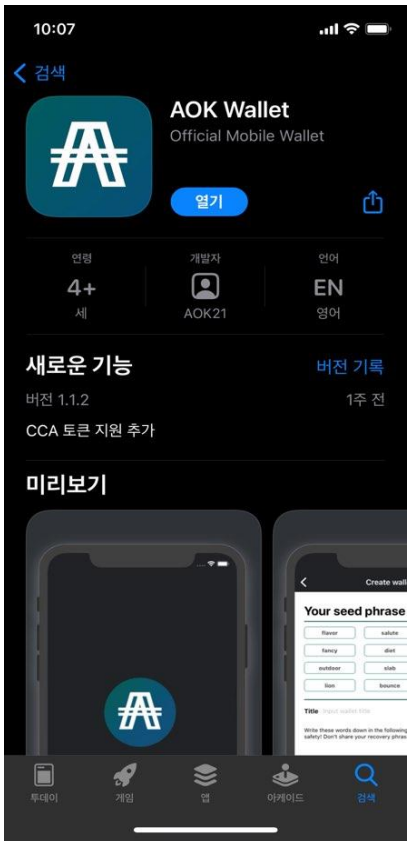
SMART CRYPTO CURRENCY WALLET

5.1. Mobile Wallet Overview

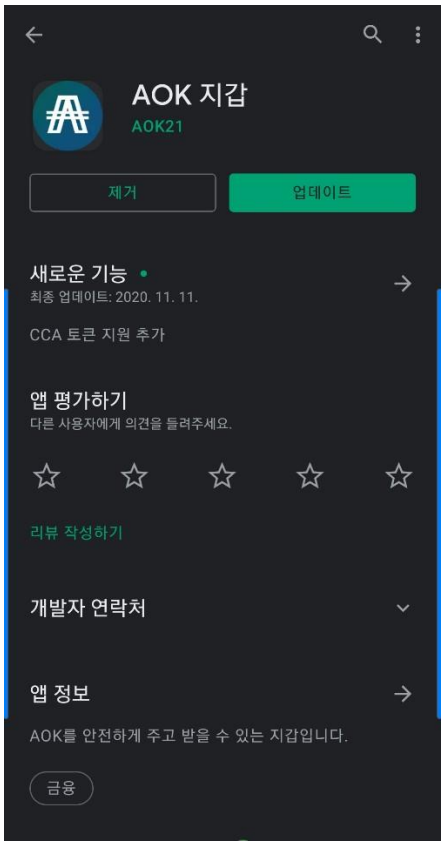
AOK는 탈중앙화된 모바일 지갑을 Android / iOS 플랫폼으로 공식 제공하고 있다. 이 앱을 이용하여 AOK 코인과 토큰의 전송, 보관, 관리를 편리하게 할 수 있다.

5.2. Android/iOS

AOK의 모바일 애플리케이션은 탈중앙화된 네이티브 어플리케이션으로 Android와 iOS 모두를 각각 지원하고 있다.



App Store by iOS



Play Store by Android

6. AOK API

6.1. API Overview

AOK API는 어플리케이션 소프트웨어를 구축하고 통합하기 위한 정의 및 프로토콜 세트로 AOK 네트워크를 사용하는 3rd party 소프트웨어를 제작할 때 유용하게 사용할 수 있는 어플리케이션 프로그래밍 인터페이스를 의미한다.

AOK의 API를 사용하면, 소프트웨어 노드를 직접 운영하지 않고도 전송내역을 검증하거나 잔액을 확인하거나 하는 일련의 과정을 편리하게 수행할 수 있다. AOK의 API는 URL 방식으로 편리하게 이용가능하며, 모든 결과는 항목이 포함된 JSON 형식으로 제공되어 활용도가 높다.

현재 사용가능한 API의 종류

- /Info
- /height/int:height
- /block/string:hash
- /header/string:hash
- /range/int:height
- /balance/string:address
- /mempool/string:address
- /unspent/string:address
- /history/string:address
- /transaction/string:hash
- /mempool
- /fee
- /decode/string:raw
- /broadcast

6.2. API Address

AOK의 API는 다음과 같은 주소에서 확인할 수 있다.

https://api.aok.network/

7. Disclaimer 면책사항

7.1.

This white paper is intended to help you understand the AOK business. Investors are encouraged to purchase through exchanges or open sales channels at their own discretion.

본 백서는 AOK 사업의 이해를 돕기 위한 설명으로 투자자는 각자의 판단으로 거래소 또는 공개된 판매 루트를 통해 구입하기 바랍니다.

7.2.

AOK, we do not guarantee return on investment to the buyer.

AOK는 구매자에게 투자수익을 보장하지 않습니다.

7.3.

AOK, we do not guarantee the price after listing.

AOK는 상장 후 가격을 보장하지 않습니다.

7.4.

AOK, we do not promise repurchase at the specified price

AOK는 지정된 가격으로 재구매를 약속하지 않습니다.

7.5.

AOK, we do not operate branch AOKs or sales agents.

AOK는 지점 또는 영업 에이전트를 운영하지 않습니다.

7.6.

AOK investors should make their own judgment that they are not in violation of the blockchain policy of each country.

AOK 투자자는 각 국가의 블록 체인 정책을 위반하지 않는다는 자체 판단을 해야 합니다.

7.7.

Despite technical efforts, AOK may incur investment losses depending on market conditions.

기술적인 노력에도 불구하고 AOK는 시장 상황에 따라 투자 손실이 발생할 수 있습니다.

7.8.

Despite our efforts, market instability or risk of market collapse is possible.

우리의 노력에도 불구하고 시장 불안정 또는 시장 붕괴 위험이 있습니다.

7.9.

AOK main notice is to prioritize the presentation of the homepage.

AOK 주요 공지는 홈페이지 프리젠테이션을 우선합니다.

7.10.

AOK Other policies are announced on the official website.

AOK 다른 정책은 공식 웹 사이트에 발표됩니다.

7. Disclaimer 면책사항

7.11.

AOK is not a stock or any way of value guarantee.

AOK는 주식 또는 가치 보장 방법이 아닙니다.

7.12.

AOK business model may change slightly depending on the agreement with the partner company.

AOK 사업모델은 파트너 사와 협약하는 내용에 따라 일부 변경될 수 있습니다.

7.13.

Purchase of AOK coin must be done by the buyer himself according to local law, AOK does not make any legal guarantee for purchase.

AOK coin의 구입은 구매자가 현지 법률에 따라 스스로 진행해야 하며, AOK 는 구매에 대한 어떠한 법률적 보증을 하지 않습니다

7.14.

Among the contents mentioned in this white paper, the business model may change its brand or target in the process.

본 백서에 언급되는 내용 중 사업모델은 진행 과정에서 브랜드 또는 대상 등이 변경될 수 있습니다.

8. References

[1] Stuart Haber & W. Scott Stornetta. (1991). How to time-stamp a digital document. Journal of Cryptology volume 3, pages99–111.

[2] Karamitsos, I. , Papadaki, M. & Barghuthi, N. (2018). Design of the Blockchain Smart Contract: A Use Case for Real Estate. Journal of Information Security, 9, 177-190.

[3] Bo Liu, Fan Qiu, Yanchuan Cao, Bin Chang, Yi Cui & Yuan Xue. (2011). Maximizing Resilient Throughput in Peer-to-Peer Network. Communications and Network, Vol. 3 No. 3, pp. 168-183.

[4] Ioanna Roussou, Emmanouil Stiakakis & Chaido Dritsaki. (2019). The Bitcoin's Network Effects Paradox—A Time Series Analysis. Theoretical Economics Letters, 9, 1981-2001.

[5] Satoshi Nakamoto. (2008). Bitcoin: A peer-to-peer electronic cash system. bitcoin.org.

[6] Gao, X. (2015). Design and Implementation of Peer-to-Peer Service Routing Algorithm. Journal of Software Engineering and Applications, 8, 575-580.

[7] Lim, I.K., Kim, Y.H., Lee, J.G., Lee, J.P., Nam-Gung, H. & Lee, J.K. (2014). The Analysis and Countermeasures on Security Breach of Bitcoin. In: International Conference on Computational Science and Its Applications, Springer International Publishing, Berlin, 720-732.

[8] Sunny King & Scott Nadal. (2012). PeerCoin: http://peercoin.net/assets/paper/peercoinpaper.pdf.

[9] Pavel Vasin. (2013). Proof of Stake 3.0: http://bravenewcoin.com/assets/Whitepapers/blackcoin-pos-protocol-v2-whitepaper.pdf.

[10] Kourosh Davarpanah, Dan Kaufman & Ophelie Pubellier. (2015). NeuCoin: the First Secure, Cost-efficient and Decentralized Cryptocurrency: http://www.neucoin.org/en/whitepaper/download.

[11] https://www.blackhalo.info

[12] https://www.ethereum.org

백서 최초 발행일

2020.11.24

AOK Group