

# AKT: 아카시 네트워크 토큰 & 채굴 경제학

그렉 오슈리, 아담 보자니츠\*

아카시 네트워크, 아카시 네트워크

(날짜: 2020년 1월 31일)

아카시는 낭비를 줄이고 소비자의 비용을 절감하고 공급자의 수익을 증대하도록 설계된 클라우드 컴퓨팅 리소스 시장입니다. 이 백서에서는 아카시 네트워크의 경제성을 다루고 AKT(아카시 토큰)를 소개합니다. 당사는 채택을 촉진하고 아카시 생태계의 경제적 보안을 보장하기 위해 설계된 경제적 인센티브 구조를 설명합니다. 우리는 경제적 목표를 달성하기 위한 인플레이션 메커니즘을 제안합니다. 우리는 채굴 보상과 인플레이션율에 대한 계산을 제공합니다. 우리는 또한 다수의 수수료 토큰을 허용하는 메커니즘을 제시합니다.

## 감사의 말씀

우리는 서니 애그가왈(텐더민트의 리서치 사이언티스트), 고티에 마린(텐더-민트), 모건 토마스(Kassir 의 공동 창업자), 브랜드 골드만(Blockfolio의 수석 건축가)에게 원고를 크게 개선한 가치 있는 코멘트를 제공해주심에 대하여 감사를 표합니다.

## I. 소개

클라우드 인프라는 324억 달러 규모의 시도[1]이며 2022년에는 2,100억 달러에 이를 것으로 예상됩니다[2].

2021년까지 전체 인터넷 애플리케이션 및 컴퓨팅 인스턴스의 94%가 클라우드 서비스 공급자(CSP)에 의해 처리될 것으로 예상되며, 기존 데이터 사용자[3]에 의해 처리되는 비율은 6%에 불과합니다. 이러한 성장의 주요 요인은 [4]년 동안 최대 컴퓨팅 아웃풋의 6% 이하가 평균적으로 제공되고 최대 30%의 서버가 공동 사용(전기를 사용하지만 유용한 정보 서비스를 제공하지 않음)되기 때문에 기존 데이터 센터에서 IT 리소스의 활용률이 저조하다는 것입니다.

전 세계적으로 840만 개의 데이터 센터가 있으며 서버 용량의 96%가 부족하고, 클라우드 서비스 공급업체인 아마존 웹 서비스(AWS), 구글 클라우드 및 마이크로

아주라가 71%의 시장 점유율[1]을 차지하며 클라우드 컴퓨팅 시장을 주도할 것으로 예상됩니다. 이 수치는 급증할 것으로 예상됩니다. 이러한 공급업체는 복잡하고 융통성이 없으며 제한적이며 공급업체에 종속된 계약[6]에 따라 비용이 많이 듭니다. 클라우드 사용량 증가로 인해 클라우드 비용 최적화가 3년 연속 클라우드 서비스 사용자의 최우선 과제가 되었습니다[7].

대규모 기존 제공업체 이외에는 클라우드 컴퓨팅에 대한 옵션이 많지 않습니다. 아카시는 현재 시장에서 낭비되는 컴퓨팅 리소스를 용도 변경하여 클라우드 호스팅 시장의 효율성을 높이는 것을 목표로 합니다.

블록체인을 활용함으로써, 아카시는 분산과 투명성을 현재 독점자가 지배하고 있는 산업으로 유도합니다. 그 결과 클라우드 컴퓨팅은 경쟁적 자유 시장으로 인해 상용화되며, 현재 비용의 극히 일부에 전 세계 어디서나 사용 가능하고 액세스할 수 있습니다.

아카시는 세계 최초이자 유일한 서버 없는 컴퓨팅용 슈퍼클라우드로, 컴퓨터를 가진 사람이라면 누구나 안전하고 마찰이 없는 시장에서 사용하지 않는 컴퓨팅 싸이클을 제공함으로써 클라우드 공급자가 될 수 있도록 지원합니다

본 논문에서는 아카시 네트워크의 고유 통화인 AKT를 사용하여 분산 컴퓨팅 환경에서 경제적 주권을 달성하는 경제 시스템을 소개합니다. 또한 초기 시장경제에 직면하고 있는 임대 내 채택 문제를 완화하기 위한 인플레이션 설계를 제안합니다. 즉, 공급 부족으로 인한 수요에 부정적인 영향을 미치는 테넌트(컴퓨팅 소비자)의 충분한 수요 부족입니다.

\*greg@akash.network, adam@akash.network

또한 분권형 생태계 채택의 주요 과제인 토큰 변동성을 해소하여 안정적인 교환매체를 위한 메커니즘을 제시합니다.

**참고:** 이 백서는 진행 중인 지속적인 작업을 나타냅니다. 우리는 이 문서를 최신의 개발 진행과 함께 최신 상태로 유지하도록 노력할 것입니다. 아카시 개발 프로세스의 지속적이고 반복적인 성질의 결과, 결과적인 코드와 구현은 본 문서가 나타내는 것과 다를 수 있습니다.

시간이 지남에 따라 시스템의 다양한 구성 요소를 지속적으로 공개하므로 관심있는 독자가 Akash GitHub 환매 조건부 채권매매를 <https://github.com/ovrclk>에서 숙독하도록 초대합니다.

## A. 정의

**AKT (아카시 토큰):** AKT는 아카시 네트워크의 기본 토큰입니다. AKT의 핵심 유틸리티는 네트워크를 보호하고 시장 경매의 컴퓨팅 가격을 정상화하기 위한 고정 메커니즘의 역할을 합니다. 검증자를 향해 배치된 AKT의 양은 검증자가 새 블록을 제안할 수 있는 빈도와 블록을 커밋하기 위한 표의 가중치를 정의합니다. 검증자에게 본딩(스테이킹)하는 대가로 AKT 보유자는 블록 보상(AKT에서 지급)을 받을 수 있을 뿐만 아니라 트랜잭션 수수료 및 서비스 수수료(화이트리스트 토큰 중 하나에서 지급)의 일부도 받을 수 있습니다.

**검증자:** 검증자는 트랜잭션을 검증 및 릴레이하고, 블록을 제안, 확인 및 완료하여 아카시 네트워크를 보호합니다. 초기에는 64명인 한정된 검증자 집합이 자동 서명 인프라의 높은 표준을 유지하는 데 필요합니다. 검증자는 AKT에서 위임자에게 수수료를 부과합니다.

**위임자:** 위임자는 AKT의 소유자이며 아카시 체인을 보호하기 위해 토큰의 일부 또는 전부를 사용합니다. 대신, 위임자는 거래 수수료의 일부뿐만 아니라 차단 보상도 받게 됩니다.

**공급자:** 공급자는 아카시 네트워크에서 컴퓨팅 주기(일반적으로 사용되지 않음)를 제공하고 기여금으로 수수료를 받습니다. 제공업체는 AKT에 대한 지분을 담보로 유지해야 하며, 이는 획득한 시간당 소득에 비례하므로, 모든 제공업체는 위임자 및/또는 검증자입니다.

**임차인:** 임차인 역경매 프로세스를 사용하여 시장 주도 가격을 책정하기 위해 공급업체가 계산 주기를 임대합니다(아래 섹션 참조).

## II. 네트워크 개요

아카시 네트워크는 컴퓨팅 리소스(클라이언트)가 필요한 사용자(클라이언트)와 임대(공급자) 컴퓨팅 용량을 가진 사용자를 연결하는 안전하고 투명한 분산형 클라우드 컴퓨팅 시장입니다. 아카시는 시장에 나와 있는 모든 공급업체보다 높은 통합 계층을 제공하는 슈퍼 클라우드 플랫폼 역할을 하므로 고객에게 어떤 특정 공급업체를 사용하든 상관없이 단일 클라우드 플랫폼을 제공합니다.

임차인은 비용 이점, 사용성, 클라우드 공급자 간 이동성, 그리고 글로벌 구현의 성능 이점 때문에 아카시를 사용합니다. 공급자는 전용 또는 일시적으로 사용되지 않는 용량에서 이익을 얻을 수 있기 때문에 아카시를 사용합니다.

컴퓨팅 단위(CPU, 메모리, 디스크)는 아카시에서 컨테이너로 임대됩니다. 컨테이너 [8]는 코드와 모든 종속성을 패키징하는 소프트웨어의 표준 단위이므로, 애플리케이션은 한 컴퓨팅 환경에서 다른 컴퓨팅 환경으로 빠르고 안정적으로 실행됩니다. 컨테이너 이미지는 코드, 런타임, 시스템 도구, 시스템 라이브러리 및 설정 등 응용 프로그램을 실행하는 데 필요한 모든 것을 포함하는 경량 독립 실행형 소프트웨어 패키지입니다.

물리적 시스템(즉, 컴퓨터, 서버)을 사용하는 모든 사용자는 가상화라는 프로세스를 사용하여 컴퓨터의 리소스를 컨테이너에 저장할 수 있습니다. 도커는 널리 채택된 컨테이너 가상화 기술을 제공하는 회사이며, 컨테이너를 "도커 이미지"라고 부르는 것이 일반적입니다. 실제 컴퓨터와 컨테이너 사이의 관계는 그림 1에 나와 있습니다.

모든 시장 거래는 아카시 블록체인에 있습니다. 컨테이너를 임대하기 위해 임차인(개발자)은 단위 유형과 각 단위 유형의 수량을 지정하여 배포를 요청합니다. 장치 유형을 지정하기 위해 임차인은 지역(예: 미국) 또는 개인 정보 기능(예: Intel SGX)과 같이 일치시킬 속성을 지정합니다. 또한 테넌트는 각 장치 유형에 대해 지불할 최대 가격을 지정합니다.

주문서는 주문 보관함에 작성됩니다(검증자가 승인한 경우).

주문의 모든 요구 사항과 일치하는 공급자는 가격에 따라 경쟁하여 입찰합니다. 주문에서 가장 낮은 금액을 입찰하는 공급자는 테넌트와 주문에 대한 제공자 간에 리스가 생성되는 조건과 일치합니다. 성공적인 임대에 대해, sec.IV A에서 보여지는대로 임대 금액의 일부(수취 수수료)가 스테이커에게 지급됩니다.



그림 1: 물리적 서버와 관련된 컨테이너형 애플리케이션의 간단한 예시

#### A. 지분 기반 합의 증명

아카시는 검증 결과 일치 모델에 의해 확보된 블록체인을 합의 프로토콜 참여를 결정하기 위한 Sybil 저항 메커니즘으로 채택하고 있으며, 비잔틴 내결함성 합의를 위한 텐더민트 [9] 알고리즘을 구현하고 있습니다. 텐더민트는 다음과 같은 속성으로 작업 증명서를 통해 속도, 확장성 및 환경 문제를 해결하도록 설계되었습니다.

- a) 검증자는 가중 라운드 로빈 방식으로 블록을 차례로 생성합니다. 즉, 알고리즘은 블록 단위로 리더를 덜 변경할 수 있습니다.
- b) 비잔틴의 결함에 대한 엄격한 책임으로 잘못된 유효성 검사를 처벌하고 네트워크를 위한 경제적 보안을 제공할 수 있습니다.

아카시 토큰을 소유하는 모든 사용자는

자신의 코인을 결합(또는 위임)할 수 있으며 검증자가 될 수 있으므로 검증자 세트가 개방되고 허가되지 않습니다. 아카시 토큰의 제한된 리소스는 Sybil 예방 메커니즘의 역할을 합니다.

투표 권한은 검증자의 결합 지분(명성이나 실생활의 정체성이 아님)에 의해 결정됩니다. 투표권이 보세지분에 비례하므로 투표권을 높이기 위해 단일 행위자는 여러 개의 노드를 작성할 수 없습니다. 검증자는 "슬래싱"이라고 알려진 프로세스에서 프로토콜에 의해 압류 및 연소될 수 있는 "보안 보증금"을 게시 해야 합니다.

이 보증금은 결합 계좌에 잠겨 있으며, 스테이커가 결합 해제를 원하는 경우에 한해 "결합 해제 기간" 후에만 해제됩니다. 슬래싱은 시스템을 잘 작동시키는 비잔틴의 결합을 야기시킬만 한 어떤 나쁜 행동들을 처벌할 수 있게 합니다.

슬래싱 조건과 비잔틴의 각각의 결합 및 처벌은 본 문서의 범위를 벗어납니다. (이들에 대한 자세한 정보는 아카시 넷 - 워크 기술 백서를 검토하십시오.)

### 1. 검증자 수에 대한 제한

아카시의 블록체인은 텐더민트 합의의 기반으로 합니다. 텐더민트 합의는 통신 복잡성 증가로 인해 검증자가 많아지면서 속도가 느려집니다. 다행히도 우리는 거래 확인 시간이 매우 빠른 강력하고 전 세계에 분산된 블록체인을 위해 충분한 검증자를 지원할 수 있으며, 대역폭, 스토리지 및 병렬 컴퓨팅 용량이 증가함에 따라 향후 더 많은 검증자를 지원할 수 있을 것입니다.

초창기에  $V_i(0) = V_{i,0} = 64$ 로 설정되어 있으며,  $t$  year의 검증자 수는 다음과 같습니다:

$$V_n(t) = \lfloor \log_2(2t) \cdot V_{i,0} \rfloor \quad (1)$$

따라서 10년 후에는 그림 2 에서와 같이  $V_n(10) = 277$ 개의 검증자가 나올 것입니다.

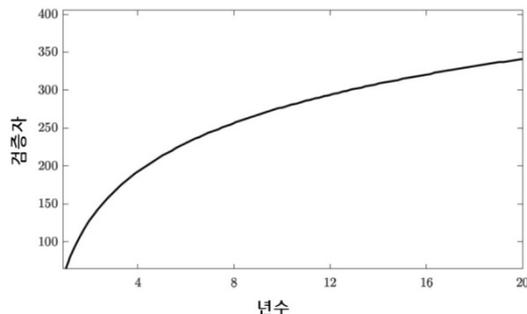


그림 2: 연도별 검증자 수

## III. AKT: 아카시 네트워크 토큰

AKT의 주요 기능은 고정(네트워크에 보안을 제공하는) 기능, 임대 계약 및 시장이 지원하는 모든 통화의 가격 책정 단위의 역할을 하는 것입니다. 시장에서 거래를 해결하는 데 AKT를 사용할 수 있지만, 리스는 본 문서의 뒷부분에서 설명한 것처럼 다수의 토큰을 사용하여 결제할 수 있습니다. 단, 거래 수수료와 블록 보상은 AKT로 표기되어 있습니다. 스테이커들이 버는 수입은 고정된 토큰과 고정된 약속의 길이에 비례합니다. 즉, AKT는 세 가지 주요 기능을 수행합니다. 해결, 보상 및 예약입니다.

### A. 해결

아카시는 일련의 검증자들이 제안을 투표하는 블록체인에 의존합니다. 각 제안은 제안자의 투표 권한에 의해 가중되는데, 이는 제안자가 보관한 총 토큰과 그들에게 결합된 토큰입니다. (제안자는 유효자에게 투표 권한을 위임할 수 있습니다.)

## B. 보상

AKT 사용자는 운영 및 자본 지출을 보조하기 위해 토큰을 보유합니다. 스테이커는 시스템에 고정된 토큰 수, 잠금 시간 기간 및 모든 토큰에 비례하여 보상을 받습니다. 로크업 시간은 1개월에서 1년까지 다양합니다. 로크업의 유연성은 약세 시장의 낮은 가격압력에 최적화되도록 설계된 자체 조정 인플레이션 시스템에서 더 짧은 기간 동안 (약세 시장) 지분을 가진 스테이커를 격려합니다.

## C. 예약

아카시의 수수료는 AKT와 함께 다수의 통화를 사용하여 결제할 수 있습니다. 시장 주문서는 AKT(아카시 토큰)를 생태계의 준비 통화로 사용합니다. AKT는 AKT와 결제 통화 사이의 환율을 고정할 수 있는 새로운 결제 옵션을 제공합니다. 이러한 방식으로 제공업체와 임차인은 낮은 유동성으로 인해 발생할 것으로 예상되는 AKT의 가격 변동성으로부터 보호됩니다. 이 섹션에서는 sec. IV D에서 설명한 것처럼 오라클 없이 환율을 설정하기 위한 "합치 가중 중위수를 사용한 트랜잭션 순서" 메커니즘도 제시합니다.

## IV. 정산 및 수수료

이 절에서는 아카시 네트워크 사용자가 부담하는 다양한 요금에 대해 설명합니다.

## A. 수수료 받기

성공적인 임대 때마다 임대 금액의 일부(수취 수수료)가 Take Income Pool로 이동합니다. Take Income Pool은 나중에 스테이커의 이해관계 무게(스테이킹된 양 및 잠금 해제 남은 시간)에 따라 스테이커에 배포됩니다(다음 절에 자세히 설명되어 있음). 수취 요율은 결제 시 사용되는 통화에 따라 다릅니다. Genesis에서 제안된 TokenTakeRate(토큰 테이크레이트) 사용 시 10%, 다른 통화(TakeRate) 사용 시 20%입니다. TokenTakeRate 및 TakeRate 매개 변수는 거버넌스에 의해 관리되는 커뮤니티의 합의에 따라 결정됩니다.

## B. 환율 로킹으로 결제

임대료는 AKT로 표시되지만 화이트리스트에 있는 모든 수신인을 사용하여 결제할 수 있습니다. AKT와 결제 통화 간에 환율을 고정할 수 있는 옵션이 있습니다. 이는 낮은 유동성으로 인해 발생할 것으로 예상되는 AKT의 가격 변동성으로부터 공급자와 임차인을 보호합니다.

예를 들어 리스가 다음으로 설정되어 있다고 가정합니다. 10 AKT를 사용하고 1 AKT = 0.2 BTC의 환율을 잠급니다. AKT의 가격이 2배, 즉 1 AKT = 0.4 BTC인 경우, 임차인은 5 AKT를 지불해야 합니다. 반대로, BTC의 가격이 2배, 즉 1 AKT = 0.1 BTC인 경우, 임차인은 20 AKT를 지불해야 합니다.

## C. 다수의 토큰을 사용하는 수수료

네트워크 남용 문제(예: DOS 공격)를 방지하기 위해 아카시의 모든 거래 및 임대에는 수수료가 부과됩니다. 모든 트랜잭션에는 BlockGasLimit를 초과하지 않는 한 트랜잭션을 처리하기 위한 특정 관련 수수료인 GasLimit가 있습니다.

가스리미트는 송금인의 계좌 잔액에서 차감하여 거래하는 가스량입니다.

이더리움[10], 비트코인[11], 네오[12] 등 플랫폼의 토종 암호화폐에서 수수료를 내야 하는 대부분의 다른 블록체인 플랫폼과 달리 아카시는 수수료에 대한 토큰을 대거 받아들입니다. 아카시의 각 검증자 및 제공자는 통화 또는 통화 조합을 수수료로 받아들이도록 선택할 수 있습니다.

결과 거래 수수료(예비 풀에 들어가는 순근로세 제외)는 검증자와 위임자의 지분(금액 및 길이)에 따라 구분됩니다.

#### D. 합의 가중 중위수를 사용한 트랜잭션 순서

여러 토큰을 사용할 때 트랜잭션의 우선 순위를 지정하려면 검증자가 트랜잭션 수수료의 상대적 가치를 결정하는 메커니즘이 필요합니다. 예를 들어, BTC의 상대적 가치는 200 AKT이고 ETH의 상대적 가치는 0.4 AKT임을 알려주는 신탁이 있었다고 가정해 보겠습니다. 동일한 가스 비용의 두 가지 거래가 있고, 그 거래 수수료는 각각 10 BTC와 6000 ETH라고 가정합니다. 첫 번째 거래의 수수료는  $2000(10 \times 200)$  AKT와 같고, 두 번째 거래의 수수료는  $2400(6000 \times 0.4)$  AKT와 같습니다. 두 번째 트랜잭션의 우선 순위가 더 높습니다. 오라클을 사용하지 않고 이러한 상대적 값을 얻기 위해 지역화된 검증자 구성 [13] 메커니즘을 사용하여 컨센서스 가중 중위수를 사용할 수 있습니다.

이 방법에서 각 검증자는 정기적으로 업데이트되는 구성 파일에서 토큰의 상대적 값에 대한 로컬 보기를 유지하며 가중 평균을 사용하여 상대적 값을 얻습니다. 즉, 트랜잭션으로 각 토큰 값에 대한 "복수"를 제출합니다.

예를 들어, 파워가 있는 검증자 {A, B, C, D, E}이(가) 5개 있습니다.

각각 {0.3, 0.3, 0.1, 0.1, 0.2}입니다. 각 토큰에 대한 개인 견해에 대해 다음과 같은 표를 제출합니다.

A : AKT = 1, BTC = 0.2

B : AKT = 2, BTC = 0.4

C : AKT = 12, BTC = 2

D : AKT = 4, BTC = 1

E : AKT = 1.5, BTC = 0.5

이러한 값은 투표를 실시한 검증자와 함께 순서가 지정된 목록에 저장됩니다.

AKT : [1<sub>A</sub>, 1.5<sub>E</sub>, 2<sub>B</sub>, 4<sub>D</sub>, 12<sub>C</sub>]

BTC : [0.2<sub>A</sub>, 0.4<sub>B</sub>, 0.5<sub>E</sub>, 1<sub>D</sub>, 2<sub>C</sub>]

제안자는 각 화이트리스트 토큰의 일치된 상대적 가치를 결정하기 위해 각 화이트리스트 토큰에 대한 표의 가중 평균(의견별)을 취합니다. 여기서  $w'(x_n) = W \cdot \text{edM} \cdot \text{ean}(x_n)$ :

AKT :  $\bar{w}([1, 0.3], [1.5, 0.2], [2, 0.3], [4, 0.1], [12, 0.1])$

BTC :  $\bar{w}([0.2, 0.3], [0.4, 0.2], [0.5, 0.2], [1, 0.1], [2, 0.2])$

각 대상(AKT = 2.8, BTC = 0.58)에 대한 상대적 값을 제공합니다.

#### V. 토큰 경제 및 인센티브

공급자는 컴퓨팅 서비스를 유료로 임대하는 임차인에게 컴퓨팅 주기를 판매하여 수익을 얻습니다. 다만, 네트워크 초기에는 입주자(컴퓨팅 소비자)의 충분한 수요 부족으로 제공자가 의미 있는 수입을 얻지 못할 가능성이 높아 공급 부족에 따른 수요에 타격을 입힙니다. 이 문제를 해결하기 위해, 우리는 건강한 임계값을 달성할 수 있을 때까지 블록 보상으로 제공자들에게 인플레이션을 통한 인센티브를 제공할 것입니다.

이 섹션에서는 광산의 경제성과 아카시 네트워크의 인플레이션 모델에 대해 설명합니다. 이상적인 팽창 모형은 다음과 같은 특성을 가져야 합니다.

- 초기 제공업체는 네트워크 외부의 시장보다 기하급수적으로 낮은 비용으로 서비스를 제공하여 채택을 가속화할 수 있습니다.
- 제공자가 얻을 수 있는 수입은 자신이 보유한 토큰 수에 비례합니다.
- 스테이커에 대한 블록 보상은 고정된 양, 잠금 해제 시간 및 전체 잠금 토큰에 비례합니다.
- 스테이커는 더 오랜 기간 동안 말뚝에 대한 인센티브를 받습니다.
- 단기 스테이커(예: 일부 약세 시장 참여자)도 참여하지만, 적은 보상을 받습니다.
- 보상을 극대화하기 위해, 스테이커는 수입을 재평가하도록 인센티브를 받습니다.

#### A. 동기 부여

아카시 네트워크는 임차인을 위한 가치 제안으로 기하급수적인 비용 절감 효과를 제공하고 테넌트와 제공자를 위한 부가 가치 제안으로 서버 없는 인프라의 효율성을 제공하여 조기 채택을 보장하는 것을 목표로 합니다. 이러한 가치 제안은 특히 머신러닝(machine learning)과 같은 데이터 및 컴퓨팅 집약적인 애플리케이션에 매우 매력적입니다.

#### B. 스테이크와 바인드: 마이닝 프로토콜

제공자는 최소한 T 시간 동안 서비스를 제공하기로 약속하고  $T_{comp} = 1$ 일 보상 기간마다 서비스 수익을 얻으려고 합니다. 공급자는 Akash 토큰을 지정하고 잠금 해제 시간  $t_1$ 을 지정합니다. 여기서 최소 잠금 시간  $t_1 - t$ 는  $T_{min} = 30$ 일 이상이어야 합니다. 또한 BindValidator 트랜잭션을 통해 자신의 지분을 결합하여 검증자 v에 위임(투표력)합니다.

스테이커는 위임자 및/또는 위임자가 위임하는 유효성 검사자입니다. 모든 제공자는 스테이커이지만 모든 스테이커가 공급자인 것은 아닙니다.. 다른 서비스를 제공하지 않는 순수 위임자인 스테이커가 있을 수 있고, 다른 서비스를 제공하지 않는 순수 검증자가 있을 수 있습니다.

어느 시점에서든 스테이커는 다음을 할 수 있습니다: a) 그들의 말뚝(또는 그들의 말뚝의 일부분)을 두 조각으로 쪼개세요. b) AKT를 더해서 말뚝 l을 늘립니다. c) 잠금시간 T, 여기서  $T > T_{min}$ .

스테이커는 나중에 다룰 잠금 시간 L에 따라 보상이 달라지기 때문에 지분을 분할합니다.

### C. 일반 인플레이션 속성

#### 1. 초기 인플레이션

아카시가 NuCyber [14] 및 DASH [15]:  $\lambda = 60\%$ 와 동일한 수의 토큰이 잠길 것이라고 가정하면 AKT 공급의 1 - 40%가 유통됩니다. 인플레이션에 대한 조정된 인플레이션율은 다음과 같습니다.

$$I^* = \frac{I}{1 - \lambda}, \quad (2)$$

ZCash[16]가  $I^* = 350\%$ (전체 불 마-케트 중 회전 지점)를 가졌다는 점을 고려하면, 초기 인플레이션을  $I_0 = 100\%$  APR(하루 1/365라는 의미)으로 설정하는 것은 충분히 안전합니다.

#### 2. 인플레이션 붕괴

모든 광부들이 최고 보상률을 가지고 있다고 가정해 보세요. 이 경우 인플레이션 붕괴 인자(인플레이션을 절반으로 줄이는 시간)를  $T_{1/2} = 2$ 년으로 정의합니다. Genesis t에서 경과한 시간에 따른 인플레이션은 다음과 같습니다.

## 3. 스테이킹 시간과 토큰 만들기

$$I(t) = I_0 \cdot 2^{-\frac{t}{T_{1/2}}} = I_0 \exp\left[-\ln 2 \frac{t}{T_{1/2}}\right], \quad (3)$$

이 경우 시간  $t$ 에 대한 토큰 공급의 의존도는 다음과 같습니다.

$$M(t) = M_0 + \int_0^t I(t) dt = M_0 + \frac{I_0 T_{1/2}}{\ln 2} \left[1 - 2^{-\frac{t}{T_{1/2}}}\right] \quad (4)$$

$I_0$ 을 상대 인플레이션율로 지정하면  $I_0 = IOM_0$ 입니다. 100% APR의 경우  $i_0 = 1$  및  $I_0 = M_0$ 이 생성될 토큰의 최대 개수를 제공합니다(그림 3 참조):

$$M_{\max} = M(\infty) = M_0 \left(1 + \frac{i_0 T_{1/2}}{\ln 2}\right) \approx 3.89 M_0 \quad (5)$$

여기서  $M_0$ 은 초기 토큰 개수입니다.

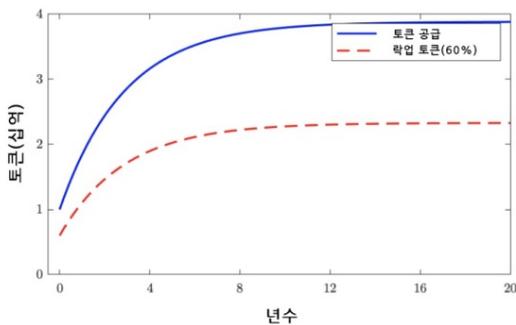


그림 3: 토큰 공급과 토큰은 100% APR의 초기 인플레이션으로 수년간 락업되고, 인플레이션 비율은 2년마다 절반씩 감소

최소  $T_1 = 1$ 년(365일)의 지분을 가진 스테이커에게 전액 보상해 드립니다.  $T_{\min} = 1$ 개월의 지분을 가진 사람들은 보상의 절반에 가까울 것입니다( $\gamma = 0.54$ ). 대체적으로,

$$\gamma = \left(0.5 + 0.5 \frac{\min(T_i, T_1)}{T_1}\right), \quad (6)$$

$$T_{i, \text{initial}} > T_{\min}, \quad (7)$$

여기서 잠금 해제 시간  $T_i$ 는 토큰을 잠금 해제하는 데 남은 시간을 의미합니다.  $T_i = t_1 - t$ .  $t_1$ 은 토큰이 잠금 해제되는 시간이며  $t$ 는 현재 시간입니다. 초기  $T_i$ 는  $T_{\min} = 1$ 개월보다 작게 설정할 수 없지만, 시간이 경과하고  $t$ 가  $t_1$ 에 가까워질수록 결국  $T_i$ 보다 작아집니다.

(보상이 낮은 경우) 이해 기간이 짧을수록 일일 토큰 배출량이 줄어듭니다. 약세장 중에는 광부들이 단기적으로 지분을 보유할 가능성이 높다는 점을 감안하면 약세장 중에는 토큰 배출량이 줄어들 것으로 예상할 수 있어 가격 상승에 도움이 될 것으로 보입니다. 따라서 우리는 이 메커니즘이 가격 안정을 지원할 것으로 기대합니다.

배출 반감기 시간  $T_{1/2}^* = T_{1/2}/\gamma^*$ , 여기서  $\gamma^*$ 은 평균 착석 파라미터이며, 모든 스테이커가  $\gamma = 0.5$ 인 경우  $\gamma^* < 0.5$ .  $T_{1/2}$ 는 2가 아니라 4년일 때 또한 길어집니다.

시간 경과에 따른 총 공급량(eq. 4) := 1은 다음과 같습니다.

$$M(t) = M_0 \left[1 + \frac{i_0 \gamma^* T_{1/2}^*}{\ln 2} \left(1 - 2^{-\frac{t}{T_{1/2}^*}}\right)\right]. \quad (8)$$

#### D. 풀 배포를 위임

지수화는 인플레이션이 아직 채굴되지 않은 토큰의 양에 비례하는 미분 방정식의 솔루션입니다.

$$I(t) = \frac{\ln 2}{T_{1/2}} (M_{\max} - M(t)) \quad (9)$$

$$dM = I(t) dt. \quad (10)$$

여기서  $M(t)$ 은  $M(0) = M_0$ 을 사용하는 현재 토큰 공급 장치이며,  $dt$ 는 채굴 기간(1일)과 같을 수 있습니다. 각 검증자는 마지막 기간의 토큰 공급 장치  $M$ 을 사용하여 몇 가지 작업을 사용하여  $dM$ 을 사소한 방법으로 계산할 수 있습니다.  $t$  시간의 검증자 풀  $p$ 에 대해 채굴된 토큰의 양은 다음 공식에 따라 계산할 수 있습니다.

$$\delta m_{v,t} = \frac{s_v \ln 2}{S T_{1/2}} \delta M(t), \quad (11)$$

$$\delta M_t = \sum_v \delta m_{v,t}, \quad (12)$$

여기서  $s_v$ 는 검증자의 대리자 풀에 바인딩된 토큰의 수  $v$ 이고  $S$ 는 잠긴 총 토큰의 수입니다.  $v$ 에 대한 모든 합계를 계산하는 대신 각 검증자는 해당 부분  $\Delta m_{v,t}$ 를 추가할 수 있습니다.  $v$  풀에 바인딩된 대리인의 분포 계수는 다음과 같습니다.

$$\kappa = \frac{1}{2} \left( \frac{\gamma}{\gamma_v} + \frac{s}{S_v} \right), \quad (13)$$

$\gamma_v$ 는 풀에 대한 총 이해 관계 보상 요소이며  $S_v$ 는 풀에 바인딩된 모든 토큰의 합계입니다.

#### E. 채굴 전략과 예상되는 보상

이 섹션에서는 고정시간을 연장하면서 모든 보상을 청산하는 스테커(액정광업 보상), 현재의 지분에 모든 보상을 추가하는 스테커, 그리고 시간  $T$ 가 끝난 후 그들의 지분이 풀리기를 기다리는 광부. 이러한 각각의 가능성은 서로 다른 분배의 분포를 가질 수 있습니다.

$\gamma = 1$ 과  $\gamma = 0.5$ 를  $\gamma$ 의 두 극단값으로 간주합니다. DASH에서와 같이 잠긴 토큰의 양을  $= 60\%$ 로 계산하겠습니다.

##### 1. 채굴 보상금을 청산

이 시나리오에서는 풀에 있는 모든 스테이커들이  $T_{\text{comp}}$  기간마다 모든 수익을 청산하고 있습니다. 네트워크에 배치된 토큰의 총량은  $S = \lambda M$ 으로 표시할 수 있습니다. 모든 위임자가 풀에 바인딩된 동일한 양의 지분을 가지고 있다고 가정합니다. 이 경우 말뚝의 양은  $m_i = s$ 와 동일하게 일정하게 유지되며  $mv = sv$  및  $\gamma = \gamma_v$ 를 만듭니다. 여기서  $\gamma_v$ 는 풀의 평균 고정 파라미터입니다. 그러면 풀 마이닝 속도(즉, 누적 풀 보상)는 다음과 같습니다.

$$\frac{dr_v}{dt} = \bar{\gamma}_v \frac{S_v \ln 2}{\lambda M(t) T_{1/2}} (M_{\max} - M(t)). \quad (14)$$

eq. 8에서  $M(t)$ 을 교체하고 시간이 지남에 따라 통합하면 다음과 같은 총 풀 보상을 얻을 수 있습니다.

$$r_v(t) = S_v \frac{\bar{\gamma}}{\gamma^* \lambda} \ln \frac{M(t)}{M_0}, \quad (15)$$

$\Delta r_v(t) = r_v(t) - C(C)$ 가 검증자 커미션인 경우, 개별 스테이커의 보상은 다음과 같습니다.

$$r(t) = \kappa \cdot \Delta r_v(t) = \frac{1}{2} \left( \frac{\gamma}{\gamma_v} + \frac{s}{S_v} \right) \cdot \Delta r_v(t) \quad (16)$$

$\gamma = 1$ (1년 동안 보관) 및  $\kappa = 60\%$ (모든 AKT의 60%가 고정됨)인 경우입니다.  $C = 0.1 \cdot r(t)$ 일 경우 AKT의 스테이커 보상은 하루 0.45%에서 시작되며, 스테이커 보상은 스테이킹 첫 해의 101.6%에서 시작됩니다.

우리는 만약 다른 채굴자들이 1년 미만의 지분을 가지고 있다면, 인플레이션율은 더 느리게 감소하고, 일정 기간 동안의 보상은 더 높아질 것이라는 것을 주목해야 합니다.

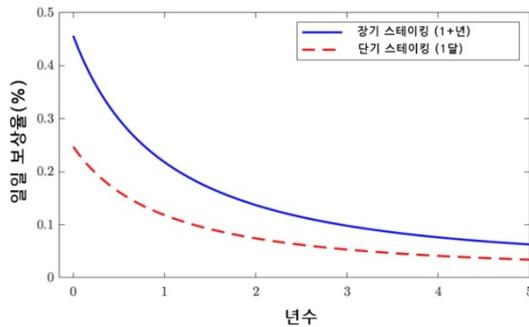


그림 4: 60%의 토큰이 1년과 1개월의 기간동안 락업된다는 가정하에 따른 기간별 일일 보상

## 2. 채굴 보상 다시 스테이크 하기

마이닝 보상을 청산하는 대신, 위임자의 지분을 늘리기 위해 이 보상은 풀에 다시 고정될 수 있습니다. 이 경우 실제 이해관계는 시간이 지남에 따라 지속적으로 증가하고 있습니다.

$$\frac{ds}{dt} = \gamma \frac{s}{\lambda M(t)} \frac{\ln 2}{T_{1/2}} (M_{\max} - M(t)). \quad (17)$$

eq. 8에서  $S(t)$ 를 대체하고  $s$ 에 대해 이 미분 방정식을 해결하면 다음과 같은 결과를 얻을 수 있습니다.

$$s(t) = s(0) \left[ \frac{M(t)}{M_0} \right]^{\frac{\gamma}{\lambda}}. \quad (18)$$

검증자 커미션이 1%라고 가정할 때,  $\kappa = 1$ (1년+ 기간 동안 유지) 및  $\kappa = 60\%$ (네트워크 내 모든 노드의 60%가 고정 중)일 경우, AKT의 대리 보상은 하루 0.45%에서 시작되며,  $s(1) - s(0) = 176.5\%$ 에서 시작됩니다.

## 3. 채굴 보상 및 스펀다운을 수행

노드가 아래로 회전할 때 스테이커는 고정  $t_1$ 의 종료 시간을 연장하지 않으며, 잠금 해제 시간이 점점 줄어들면서 보상이 지속적으로 감소하여 효과적으로  $\gamma$ 를 0.5로 점차 감소시킵니다. 이것이 기본 동작입니다. 이를 방지하려면 스테이커는  $t_1$ 을 충분히 크게 설정하거나 주기적으로  $t_1$ 을 늘려야 합니다.

## 4. FAQ

**얼마나 많은 토큰이 존재하게 될까요?** 우리는 1억 개의 토큰으로 시작할 것이며, 지금까지 만들어진 토큰의 최대 양은 3억 8천 9백만 개입니다. 그림 3에서 볼 수 있듯이 말이죠.

**인플레이션율이 어떻게 되나요?** 인플레이션율은 얼마나 많은 단기 채굴자와 장기 채굴자들이 이 시스템에서 일하고 있는지에 따라 달라질 것입니다. 이에 따라 초기 인플레이션은 50% APR(모든 채굴자가 매우 짧은 기간일 경우)과 100% APR(모든 채굴자가 장기간 약속할 경우) 사이입니다. 인플레이션은 매일 기하급수적으로 붕괴될 것이며, 2년(모든 채굴자들이 장기적이라면)에서 4년(모든 채굴자들이 단기적이라면) 사이에 어느 정도 시간이 절반으로 줄어들 것입니다. 그림 5.

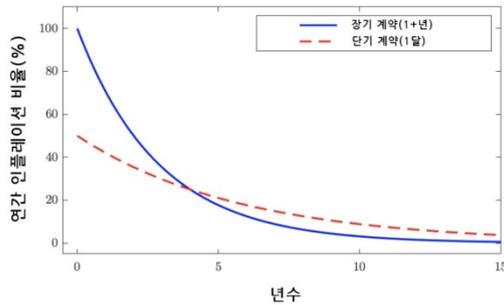


그림 5: 토큰이 장기 및 단기 계약으로 락업 되는 기간 동안의 연간 인플레이션

## VI. 관련 작업

지분 네트워크의 대다수가 해당됩니다. [19] 모두 단일 토큰 모델을 사용합니다. 하지만 좀 더 새로운 모델을 실험하는 네트워크가 있는 것 같습니다. 이 섹션에서는 이러한 시스템 중 일부를 검토하고 아카시의 토큰 모델과의 차이점을 살펴보겠습니다.

### A. Cosmos Hub

아카시 및 Cosmos Hub는 텐더민트 [9] 컨센서스 알고리즘 [9] 을 사용하며 상호운용성 및 사용자 경험과 핵심 가치 세트를 공유합니다. 코스모스의 아톰 [13]과 유사하게, AKT의 주요 효용은 네트워크에 경제적 보안을 제공하는 것입니다. 아카시의 모델은 코스모스의 모델을 다양하게 개선해 줍니다. 첫째, AKT는 시장 경매를 위해 컴퓨팅 가격을 정상화할 수 있는 메커니즘을 제공합니다. 둘째, 아카시는 더 오랜 기간 동안 컴퓨팅을 ash's token model. 임대할 때 AKT의 시장 드라이브 변동성 위험을 완화하기 위해 환율을 선택적 통화에 고정하는

메커니즘을 도입했습니다. 마지막으로 아카시의 블록 보상 분포는 일정한 시간 동안 균일하게 분포하는 코스모스의 모델과 달리, 지분의 시간과 양에 비례합니다. 코스모스는 21일(폐쇄로 간주)의 "결합 해제" 기간을 부과하며, 더 긴 기간 동안 약속할 동기가 없습니다. 반면, 아카시의 스테이커는 1개월에서 1년 동안 커밋을 선택할 수 있습니다. 이 커밋은 각각 54%와 100% 보상을 받게 됩니다.

### B. NEO

NEO의 백서 [12]에 따르면 다음과 같습니다.[12]:

네오 네트워크에는 두 개의 토큰이 있습니다. 네오 블록체인의 관리권을 나타내는 NEO와 네오 블록체인의 사용권을 나타내는 GAS입니다.

표면적으로는 NEO의 1차 유틸리티가 스테이킹 토큰이고, GAS는 수수료 토큰입니다. 네오의 모델은 아카시의 모델과 매우 다릅니다.

첫째, 토큰을 보유할 필요 없이 각 네오 계정이 얼마나 많은 표를 획득하는지 결정하는 메커니즘으로 네오를 사용합니다. 각 계정은 원하는 만큼 많은 검증자를 투표할 수 있으며, 각 검증자는 투표자의 계정에서 네오의 양에 해당하는 표를 받습니다.

수수료와 관련하여 네오의 체인은 아카시의 멀티토큰 모델과 달리 하나의 수수료 토큰만 지원합니다. 또한 아카시와 달리 네오는 GAS 토큰에 대한 변동성을 제공하지 않습니다.

### C. EOS

EOS가 위임한 지분 일치 증명[20]은 아카시의 모델과 유사하지만, 완전히 다릅니다. EOS에서는 각 토큰 보유자가 블록 생산자에게 투표하기 위해 자신의 토큰을 보유할 수 있으며, 그 대가로 CPU, RAM, NET 등의 리소스 단위로 보상하여 순작업의 트랜잭션에 사용할 수 있습니다.

단, NEO에서와 마찬가지로, 스테이킹 토큰 EOS는 블록 생산자에 의해 고정되지 않으며, 잘못된 행동의 경우에도 삭제가 불가능합니다. EOS에서 스테이킹이란 말은 스테이커가 토큰을 자물쇠에 넣고 있다는 뜻입니다. 기간이며, 반드시 순 작업의 기능에 기여하지는 않습니다. 스테이커는 다음에서 보상을 받습니다.

네트워크의 계산 리소스를 구입하는 데 사용되는 CPU, RAM 및 NET입니다.

이러한 리소스는 전송할 수 없습니다. CPU와 NET은 수신기만 사용할 수 있는 반면, 수신기는 사용할 수 있습니다.

RAM은 Bancor 스타일의 시장에서 다른 사용자와 거래될 수 있습니다 [21].

EOS는 이러한 리소스를 블록 생산자에게 제공하는 대신 지출할 때 사용합니다. 검증자 보상 모델이 불명확하여 거래 수수료를 회피하는 것이 주요 메커니즘이 아닙니다. EOS는 뉘앙스와 추가 단계가 있음에도 불구하고 걸보기에는 단일 토큰 네트워크입니다.

## VII. 결론

본 백서에서는 아카시 네트워크와 채굴 경제성에 대해 설명하고 다양한 토큰의 다양한 인센티브와 유틸리티를 스테이킹 및 수수료 메커니즘에 제시합니다. AKT(아카시 토큰)는 정산을 위해 다수의 토큰을 사용하는 동안 네트워크의 토큰 및 예약 통화로 작동합니다.

[1] “Worldwide Market Share Analysis: IaaS and IUS” [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018>

[2] “Cloud Infrastructure Market - Global Forecast to 2022” [Online]. Available: <https://www.marketsandmarkets.com/PressReleases/cloud-infrastructure.asp>

<https://www.marketsandmarkets.com/PressReleases/cloud-infrastructure.asp>

[3] “Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper” [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html>

[4] J. Kaplan, N. Kindler, and F. William, “Revolutionizing Data Center Efficiency McKinsey and Company.” [Online]. Available: [https://www.sallan.org/pdf\\_docs/McKinsey\\_Data\\_Center\\_Efficiency.pdf](https://www.sallan.org/pdf_docs/McKinsey_Data_Center_Efficiency.pdf)

[5] “Uptime Institute Comatose Server Savings Calculator.” [Online]. Available: <https://uptimeinstitute.com/resources/asset/comatose-server-savings-calculator>

[6] “Prime Leverage: How Amazon Wields Power in the Technology World” [Online]. Available: <https://www.nytimes.com/2019/12/15/technology/amazon-aws-cloud-competition.html>

[7] “RightScale 2019 State of the Cloud Report.” [Online]. Available: <https://www.flexera.com/about-us/press-center/rightscale-2019-state-of-the-cloud-report-from-flexera-identifies-cloud-adoption-trends.html>

[8] “What is a Container?” [Online]. Available: <https://www.docker.com/resources/what-container>

[9] E. Buchman, J. Kwon, and Z. Milosevic, “The latest gossip on BFT consensus” [Online]. Available: <https://arxiv.org/abs/1807.04938>

[10] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger.” [Online]. Available: <https://gavwood.com/paper.pdf>

[11] N. Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Online]. Available: <https://bitcoin.org/bitcoin.pdf>

[12] “NEO Whitepaper.” [Online]. Available: <http://docs.neo.org/docs/en-us/basic/whitepaper.html>

- [13] S. Aggarwal, “Cosmos Multi-Token Proof of Stake Token Model” [Online]. Available: [https://github.com/cosmos/cosmos/blob/master/Cosmos\\_Token\\_Model.pdf](https://github.com/cosmos/cosmos/blob/master/Cosmos_Token_Model.pdf)
- [14] M. Egorov, M. Wilkinson, and, “NuCypher: Mining & Staking Economics” [Online]. Available: <https://www.nucypher.com/static/whitepapers/mining-paper.pdf>
- [15] E. Duffield and D. Diaz, “Dash: A Payments-Focussed Cryptocurrency.” [Online]. Available: <https://github.com/dashpay/dash/wiki/Whitepaper>
- [16] “ZCash Emmission Rate.” [Online]. Available: <https://z.cash/technology/>
- [17] “Ethereum 2.0 White Paper.” [Online]. Available: <https://github.com/ethereum/wiki/wiki/White-Paper>
- [18] L. M. Goodman, “Tezos: a self-amending crypto-ledger.” [Online]. Available: [https://tezos.com/static/white\\_paper-2dc8c02267a8fb86bd67a108199441bf.pdf](https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf)
- [19] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A Provably Secure Proof of Stake Blockchain Protocol.” [Online]. Available: <https://iohk.io/research/papers/#ouroboros-a-provably-secure-proof-of-stake-blockchain-protocol>
- [20] D. Larimer, “EOS: Technical Whitepaper.” [Online]. Available: <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md>
- [21] “EOS RAM 101: Non-Technical Guidebook for Beginners.” [Online]. Available: <https://medium.com/coinmonks/eos-ram-101-non-technical-guidebook-for-beginners-6f971322042e>