옐로우 페이퍼: Nebulas Rank

Nebulas 기술연구팀

2018년 6월

v1.0.1

목차

1 서론

보다 많은 이들이 블록체인이 제시하는 탈 중앙화의 이념 아래 블록체인의 기술 개발에 참여하고 있으며 그 기술은 점점 더 많은 곳에서 적용되며 사용 사례가 증가하고 있다. 블록체인 기술의 근원으로 알려진 비트코인은 이미 탈 중앙화된 디지털 자산에 대한 가치와 중요성을 제시했으며, 더 나아가 이더리움은 탈 중앙화 기술 기반의 분산 어플리케이션(DApp)에 대한 중요성을 증명했다.

블록체인 기술의 근간은 개방성(Openness)과 익명성이라고 볼 수 있다. 다만, 블록체인의 이러한 특성으로 인해 블록체인 데이터의 가치를 측정하는데 다소 어려움 있으며, 이것은 크게 두 가지로 분류할 수 있다. 첫째, 블록체인의 익명적 특성으로 인해 다른 계정에 속하는 다수의 계정과 자산이 동일한 사용자 계정에 속하는지에 대한 여부를 추론하기 어렵다. 이는 블록체인 시스템에 TTP Cookie와 유사한 메커니즘을 구성할 수 없을 뿐더러 기존의 데이터 분석 기술을 통해 다양한 관점에서 사용자 경험과 특성을 분석하기가 어렵다. 둘째, 블록체인 시스템의 개방성으로 인해 전체 시스템 자체가 강한 부정행위 공격에 노출될 수 있으며 각종 타깃성 부정행위 공격에 취약하다. 즉, 블록체인 데이터의 가치측정 시스템은 기존의 폐쇄적이고 독립적인 가치측정 시스템과는 크게 다르다.

효율적인 가치측정 시스템의 구축은 블록체인 기술과 생태계의 무궁무진한 발전을 위한 발판이 되어 줄 것이며, 비효율적인 가치측정 시스템은 모든 블록체인 산업의 발전과 사용 사례를 제한시킬 것이다.

우선, 효율적인 가치측정 시스템 구축을 위해 블록체인 데이터, 어플리케이션 및 계정의 가치를 계량화하는 방법이 필요하다. 근본적인 원인으로는 각기 다른 블록체인 협력과 효율성에 대한 수요가 지속적으로 증가하고 있다는 것이다. 가치측정 시스템이 없다면, 이러한 협력을 위한 작업은 부정적인 영향을 받을 수 밖에 없다.

둘째, 블록체인 기술은 여전히 개발 초기 단계에 있으며 블록체인에 있는 내재되어 있는 데이터 및 자산의 진정한 가치는 십분 활용되지 못하고 있다. 효율적인 가치측정 시스템을 통해 가치를 발견하여 보다 많은 어플리케이션에 활용하고 대출, 신용, 데이터 검색 및 크로스체인 상호작용과 같은 블록체인 사용 사례를 창출해 낼 수 있다.

마지막으로, 가치측정을 기반으로 하는 인센티브는 양질의 블록체인 생태계를 구축하는데 필수적이다. 효율적인 가치측정 시스템 없는 인센티브 메커니즘은 무분별한 인센티브로 인해 블록체인 생태계를 부패 및 붕괴시킬 수 있다.

블록체인을 위한 효율적인 가치측정 시스템을 구축하기 위해서는 아래 세 가지 요건을 충족시켜야 한다:

- **진정성.** 양질의 가치측정 시스템은 해당 영역에서 신뢰성을 보장할 수 있도록 블록체인 경제 시스템의 특징을 정확히 반영해야 한다.
- **공정성.** 가치측정 시스템은 인센티브 메커니즘의 기준을 제공하는데, 이 기준은 공평성이 유지되어야 조작 또는 부정행위가 야기시키는 “부정적 인센티브가 긍정적 인센티브를 쫓아내는 현상”을 방지할 수 있다.
- **다양성.** 블록체인 어플리케이션의 가치측정에 대한 수요와 요구사항은 각기 다를 수 있고 이에 따른 인센티브 방식 또한 달라질 수 있기 때문에 가치측정 시스템은 다양한 시나리오를 수용할 수 있어야 하며 앞서 언급된 신뢰성과 공정성을 충족시켜야 한다.

Nebulas Rank는 이러한 세 가지 요건을 모두 충족하는 블록체인의 가치측정 척도이다. 진정성을 반영하기 위해 여러 지표를 참고한 끝에, Nebulas Rank는 계정주소가 블록체인의 경제 시스템에 기여하는 정도를 측정한다.

블록체인은 하나의 경제체로서 기존의 화폐 이론을 위반하지 않는다. 블록체인 상에서의 암호화폐는 일반 화폐의 기능(교환의 수단, 가치의 저장수단, 회계의 수단)과 성질 뿐만 아니라 유동성으로 인해 가치의 변화가 이루어질만큼 일반 화폐와 유사하다. 화폐의 유동성에 따라 그의 가치가 상승하듯이, 암호화폐 또한 사용자 간의 각 거래를 통해 유동성이 증가할수록 가치가 상승한다. 따라서, 블록체인 상에서 사용자의 거래 행위는 결국 블록체인 시스템의 가치를 반영하기 때문에 효율적인 가치측정 시스템을 구축하기 위한 가장 중요한 데이터라고 볼 수 있다.

Nebulas Rank의 성능을 평가하기 위해 이더리움 체인 상의 데이터 중 Nebulas Rank의 모든 계정의 합을 산출하여, Coinmarketcap.com에서 같은 시기의 이더리움 시가총액과 대조하여 비교했다. 이는 Nebulas Rank 계정의 합과 이더리움의 시가총액 사이에서 밀전한 상관관계를 보여 주었으며(약 0.84), Nebulas Rank는 매크로 수준에서 블록체인 시스템의 가치를 측정할 수 있는 동시에 미시적 수준에서 계정의 기여도를 측정하는데 효과적이라는 의미이다.

Nebulas 기술연구팀은 공정성을 보장하기 위해 효과적으로 부정행위에 대응할 수 있는 특별한 산출 함수를 도입하였고, Nebulas Rank의 반(反)부정행위의 기능 분석을 통해 성능을 입증할 것이다.

Nebulas Rank 이론에 근거하고 다양한 어플리케이션과 시나리오에 대한 수요를 충족시키 위해 Nebulas Rank를 Core Nebulas Rank와 Extended Nebulas Rank로 나누어 개발할 것이다. Core Nebulas Rank는 전체 블록체인 시스템에 대해 일정 시간 동안의 기여도를 계산하기 위한 알고리즘이다. 본 알고리즘은 일정 기간 동안의 계정의 평균 지분값과 출납률을 산출한다. Extented Nebulas Rank는 Core Nebulas Rank를 기반으로 하며, 다양한 어플리케이션과 시나리오에 적합하도록 제공된다. 예를 들어, Core Nebulas Rank를 통해 스마트 컨트랙트의 순위를 결정 짓는 방법과 Extented Nebulas Rank를 통해 여러 차원으로 확장하고 다른 가중치를 부여하는 방법에 활용할 수 있다. Nebulas Rank의 이론과 방법을 제외하고도, Nebulas Rank의 구현 계획, 랭킹 지수를 온체인으로서의 포함 여부, Nebulas Rank의 업데이트 방법과 Nebulas Rank의 추후 개발 계획을 제공할 수 있다.

> 특별 참고: 기본 알고리즘을 지속적으로 검토했고 그 성능을 실험하여 확인해 본 결과를 토대로 하기 때문에, 본 Nebulas Rank에 대한 옐로우 페이퍼의 내용은 Nebulas 화이트 페이퍼(기술백서)(2018년 4월에 발표된 v1.0.2)[3]와는 다소 차이가 있을 수 있다. 본 옐로우 페이퍼에서는 특별 참고를 추가하여 화이트 페이퍼(기술백서)에서 업데이트된 사항들을 제시한다.

2 배경 및 관련 기술

이 장에서는 주로 블록체인 및 관련 기술의 발전 배경을 소개하려 한다. 현 블록체인 영역에서 가치측정 시스템의 필요성과 기존 전통기술의 랭킹 알고리즘이 블록체인 영역에서의 적용 사례 및 취약점에 대해 논하려 한다.

2.1 블록체인의 개발 현황

2008년 10월 Satoshi Nakamoto가 비트코인 백서를 발표하였으며, 비트코인은 블록체인의 초기 어플리케이션으로서 “개인간 디지털 화폐 시스템”이라는 초념을 이행하였다. 비트코인의 탄생은 어떠한 특정 조직을 위함이 아닌 오직 특정 알고리즘을 수행해 내기 위해 대량 컴퓨팅 연산 능력으로 비트코인의 네트워크 분산식 원장 회계 시스템을 일관적으로 보장했다. 특정한 스크립팅 언어를 통해, 비트코인을 사용하여 이중지불을 방지하고 중재자 없이 제 3자 거래와 효율적인 소액 결제를 할 수 있게 되었다. 그 이후 비트코인을 기반으로 한 많은 시제품들이 생겨났고, 화폐의 기본적인 속성을 제공하는 것 이외에도 다양하고 많은 실험이 시행되고 있었다. 예를 들어, 초기의 네임코인(Namecoin)[5]은 분산식 도메인 네임 시스템(DNS)을, Open Assets은 “컬러드 코인(Colored coins)”을 제공 하였으며, 이 둘은 모두 비트코인을 모방하고 특징을 반영한 스마트 디지털 자산의 대표적인 예이다.

안타깝게도 비트코인 스크립팅 언어의 설계에는 지침과 튜링 완정성(Turing-Complete)의 부재, 그리고 제한된 응용성 등 개선점이 존재했다. 블록체인 기술이 발전함에 따라 보다 많은 이들이 블록체인 기술을 연구하여 많은 어플리케이션과 관련 기능을 확장하고 추가하였다. 그 중 단연 돋보이는 성과를 이뤄낸 프로젝트는 이더리움(Ethereum)이다[7]. 이더리움은 획기적으로 튜링 완정성을 기반으로 하는 스마트 컨트랙트(Smart Contracts)을 제공하였고, 이에 어플리케이션 개발 영역은 새로운 국면을 맞이하게 되었다.

스마트 컨트랙트는 블록체인 시스템에서 기술적 수단을 통해 특정 조건 성립 시 자동으로 계약이 시행되는 일종의 스마트 계약이다. 이더리움 스마트 컨트랙트는 이더리움의 가상 머신(Ethereum Virtual Machine, EVM)에서 실행되며 EVM은 어떠한 주체의 억압을 받지 않고 합의 알고리즘으로 계약 자체 및 산출물의 완전성을 검증한다. 이더리움의 스마트 컨트랙트를 기반으로, 많은 이들이 복잡한 기능의 분산 어플리케이션(DApp) 개발을 구현할 수 있게 되었다.

이러한 DApp는 기본적인 기능 외에도 투표, 크라우드 펀딩, 대출, 지적재산권 등과 같은 광범위한 분야에서 각종 솔루션으로서 기능할 수 있다. 이더리움은 블록체인의 가능성을 확장시키는데 성공하였지만, 이 모든 블록체인 데이터에 대한 가치측정 시스템의 부재로 인해 현재 이더리움 블록체인 플랫폼 상에는 킬러 앱(Killer Dapps)가 여전히 개발되지 않은 상황이다.

스마트 컨트랙트를 지원하는 블록체인 시스템의 경우, 일반적으로 외부 소유 계정(Externally owned account, EOA)과 스마트 컨트랙트 계정 두 가지 계정 유형으로 분류된다. 하지만, 현재 이 두 가지 계정 유형에 대한 합리적인 가치측정 지표가 극히 부족한 상태이다. 이 뿐만 아니라 많은 거래 및 스마트 컨트랙트의 이용 과정에서 귀중한 데이터들이 숨겨져 있다. 이러한 데이터는 기존 기술의 거래 데이터보다 더욱 고차원적인 데이터를 지니고 있기 때문에 기존 기술을 기반으로 하는 가치측정 척도로 데이터를 분석하거나 평가할 수 없다.

2015년 초 Chris Skinner는 “가치 웹(Value Web)”의 개념을 제시하였는데, 그 중 가치 생태계(Value Ecosystem)안에는 가치의 교환(Value Exchanges)과 가치의 저장(Value Stores) 및 가치

의 관리 시스템(Value Management Systems), 위 세 가지를 반드시 포함해야 한다고 언급한 바 있다. 더 나아가 Chris는 비트코인과 같은 암호화폐의 경우 데이터 가치의 측정이 기존의 사회적 데이터 가치의 측정과는 크게 다르고 난이도가 높다는 점을 지적했다.

2.2 그래프에서 노드의 랭킹 알고리즘

스마트 컨트랙트의 도입으로, 현재 이더리움을 대표적으로 하는 새로운 세대의 블록체인 프로젝트는 전자 화폐 거래 플랫폼 보다 복잡하고 거대한 경제체제이다. 다만, 아직까지 사용자 계정과 같은 체인 상의 주체의 가치를 평가할 합리적인 방법은 없다. 예를 들어, 현재 어떤 주체가 블록체인 생태계에 얼마나 기여하는지, 또한 이러한 기여도를 어떻게 측정할 수 있을지 제시된 솔루션은 전혀 없다.

여기서 보편적으로 알려진 기존 인터넷 영역의 가치측정 표준인 PageRank 알고리즘[9]을 언급하고자 한다. Google의 초기 핵심 알고리즘인 PageRank는 원래 웹 링크 분석에서 랭킹 문제를 해결하도록 설계되었다. 글로벌적인 규모의 연구와 함께, PageRank 알고리즘은 널리 학술 논문의 순위, 웹 크롤러, 키워드 문장 추출뿐만 아니라 PageRank를 기반으로 한 소셜 사용자의 영향력 순위 조사 등 다방면으로 널리 사용되고 있다. 학술계는 이미 PageRank 알고리즘을 Fleder, Kester, Pilai 등 블록체인의 연구에 사용하고 있으며[10], PageRank를 통해 비트코인 주소와 활동 내역을 검색 및 분석할 수 있게 하려 시도하고 있다. 그러나 그들이 주로 사용하는 방식은 PageRank를 수동적으로 이용한 수동적 분석 방식이며 PageRank는 단순히 보조 역할을 할 뿐이다.

Web 2.0 시대에 활용하기 위해 개발된 랭킹 알고리즘으로써 PageRank 알고리즘은 온라인 소셜 네트워크에서의 영향력 평가에 적용하여 활용하기엔 한계가 있다. 그 이후로, PageRank 알고리즘을 중점적으로 연구가 진행되었는데, 그 중 PageRank에서 보다 확장된 형태로 널리 알려진 것이 LeaderRank 알고리즘이다. PageRank에서 동일한 전환 확률을 사용하는 대신, LeaderRank는 노드와 가중치가 있는 양방향 링크를 도입하여 전환 확률을 획일적으로 향상시켜 노드가 안밖으로 다른 전환 확률을 가질 수 있도록 개선하였다. 그러나 LeaderRank는 노드 간의 관계를 고려하여 평판 및 영향력 순위를 반복적으로 계산하지만 사용자(혹은 주소)의 활동은 영향력 평가는 하지 못한다.

여기서 중요한 점은 PageRank의 랭킹 알고리즘은 시빌 공격(Sybil Attack)의 대응할 수 없다는 것이다. LeaderRank는 노드 사이의 관계(즉, 네트워크 구조)만을 고려하고, 반복 과정을 통해 최종적으로 영향력의 랭킹을 도출 하는데, 이 랭킹 순위는 사용자 활동성을 측정하기에 어렵다. 이로 인해, 시빌 공격을 통해 공격자는 대량의 가명의 로고를 생성하고 네트워크 측정 시스템을 파괴하여 인위적으로 높은 랭킹 지수를 얻을 수 있다.

Nebulas Rank와 가장 관련이있는 프로젝트는 NEM으로, [17] 비트코인의 작업증명(Proof of Work)와 이더리움의 지분증명(Proof of Stake) 합의 알고리즘과는 달리 NEM은 중요도증명(Proof of Importance) 합의 알고리즘을 설계했으며, 랭킹 알고리즘 NCDawareRank[14]을 사용한다. NCDawareRank는 네트워크 토폴로지의 클러스터링(집단화) 효과를 SCAN[15] [16] [17] 알고리즘에 기반한 클러스터링 알고리즘과 함께 활용한다. 커뮤니티 구조는 트랜잭션 그래프에 존재하고 스팸 노드를 처리하는 데 도움이 되지만, 동일한 주체가 제어하는 블록체인의 모든 노드가 하나의 클러스터로 매핑된다는 보장이 없으므로 부정행위를 통해 충분히 조작될 가능성이 있다.

2.3 반(反)부정 능력

Nebulas Rank의 가장 중요하고 도전적인 목표는 신뢰성 향상, 즉 부정행위에 대한 저항성이다. Hopcroft 외 다수의 의견에 의하면[18], 악의적으로 PageRank를 조작하는 경우 온라인 네트워크에

서 사용자의 영향력을 효율적으로 측정할 수 없다는 사실을 발견했다고 한다. Zhang 외 다수의 의견에 의하면 소셜 네트워크에서 노드의 영향력 측정 지표가 설정되었다 하더라도, 공격자는 다른 비(非) 시빌 사용자의 영향을 약화 시킬 수 있다고 지적한다[19]. 이는 주로 PageRank 알고리즘이 네트워크 토폴로지를 기반으로 사용자 랭킹을 측정하기 때문에 대칭 네트워크(Symmetric Network)에서 공격자는 이미지 네트워크를 생성하여 동일하거나 보다 더 높은 영향력 지수를 쉽게 얻을 수 있다[20][12]. 블록체인 시스템에서 보편적으로 사용되는 부정행위의 방법은 다음과 같다:

1. 루프 전송. 공격자는 루프 토폴로지를 따라 돈을 전송하므로 동일한 금액의 자산이 같은 가장자리에서 반복적으로 순환 및 누적되오 루프 가장자리의 가치가 지속적으로 증가한다.
2. 시빌 노드의 출력 차수(out-degree)가 증가하도록 임의의 주소로 전송, 그 결과로 자금의 번식량도 증가한다.

3. 공격자가 제어하는 주소를 사용하여 독립적인 네트워크 구성 요소를 구성하고, 공격자 스스로가 중앙 노드인 것처럼 가장 또는 위조 할 수 있다.

4. 신뢰할 수 있는 계정 주소와의 빈번한 거래와 상호 작용을 통해,해당 주소로 반복적으로 동일한 금액 송금하여 공격자가 네트워크에서 보다 나은 구조적 지위를 얻을 수 있다.

따라서 Nebulas는 Core Nebulas Rank를 설계할 때, 상기 내용을 고려하여 공정성을 보장하려 한다.

3 블록체인 경제 모델

암호화폐는 일종의 거래 매체 또는 스마트 자산으로서 경제적 중요성을 부여 받는다. 따라서 합리적인 경제 모델은 Core Nebulas Rank의 궁극적 목표인 블록체인 데이터에 대한 가치측정 시스템을 수립하는데 도움이 될 수 있다. 이 장에서는 우선 암호화폐의 수학적 표현을 소개하고 간단하면서도 보편적으로 알려진 통화(화폐) 모델을 사용하여 암호화폐를 분석하며 Core Nebulas Rank에 대해 설명하고자 한다.

3.1 암호화폐에 대한 설명

암호화된 디지털 화폐와 기존 경제 시스템 및 법정화폐의 가장 큰 차이점은 모든 암호화폐는 거래내역을 추적 할 수 있다는 것이다. 이는 더 큰 경제적 시스템에 대해 각 거래의 영향을 분석 할 수있는 중요한 데이터 소스를 제공한다. 일반적으로 암호화폐 시스템은$(\mathscr{L}, \mathscr{U})$ 한 쌍으로 정의 할 수 있습니다. 여기서 $\mathscr{L}$은 원장 시스템을 나타내며 $\mathscr{U}$는 암호화폐 사용자 집합을 나타난대. 또한 원장 시스템은 다음과 같이 세 쌍으로 설명 될 수 있다:

$$\mathscr{L} = (\mathscr{A}, \mathscr{D}, \mathscr{T}) \tag{1}$$

여기서 $\mathscr{A}$는 계정 집합을, $\mathscr{D}$는 각 계정의 초기 잔액 집합을, $\mathscr{T}$는 트랜잭션(거래) 집합을 나타낸다. 각 거래는 아래와 같이 테트라드(tetrad)로 나타낼 수 있다:

$$\mathscr{D} = \{a \to d, a \in \mathscr{A}, d \in R^*\} \tag{2}$$

$$\mathscr{T} = \{(s, t, w, \tau)\} \tag{3}$$

여기서 $a \to d$는 계좌 a(d는 양의 실수입니다. 즉, 잔액이 0인 계정을 고려하지 않음)에 해당하는 잔액 d를 나타낸다. s, t, w 및 τ는 거래의 소스 계정, 대상 계정, 금액 및 시간을 각각 나타낸다. 계정은 그 계정으로 거래를 제안 할 수있는 관련 사용자가 관리하며 다음과 같이 표시 할 수 있다:

$$u \text{ dom } a \,.\, u \in \mathscr{U}, a \in \mathscr{A} \tag{4}$$

한편으로 사용자는 다음과 같이 표현된 여러 계정을 제어 할 수 있다:

$$A(u) = \{ \forall a \in \mathscr{A} : u \ dom \ a \} \tag{5}$$

반면 계정은 다음과 같이 단일 사용자만 제어 할 수 있다:

$$\forall u_1, u_2 \in \mathscr{U} : A(u_1) \cap A(u_2) = \phi \tag{6}$$

위에 설명된 모델은 모든 암호화폐 시스템을 합리적으로 간소화 한 것이다. 이 모델에서는 오프체인 데이터와 온 체인 데이터를 따로 구별하지 않으며 거래 가격이나 스마트 컨트랙트의 도입 등을 채택하지 않는다. 또한 거래의 계정은 유형별로 분류된다. 일반적으로 거래는 체인에 기록되는 일반 거래와 중앙 데이터베이스에 기록되지 않는 내부 교환 트랜잭션 두 가지 범주로 나눌 수 있다. 이는 체인에서 데이터만 가져 오는 경우 거래를 잃게되는 결과를 초래한다. 그러나 협조를 얻어 내부 교환 거래를 얻을 수있는 경우 교환 계정을 여러 계정으로 매핑하여 위에서 설명한 모델처럼 활용할 수 있다.

3.2 암호화폐의 모델

비록 암호화폐는 기존 법정화폐와는 크게 다르지는 않지만, 기존 화폐 이론은 오늘 날에도 여전히 실제적으로 선도적인 의미를 지니고 있다. 암호화폐는 새로운 경제적 주체[21]에서 나온 현대적인 형태의 화폐로 기존 화폐의 성질으로 교환의 수단, 가치의 저장수단 및 회계의 수단이라는 세 가지 필수 기능을 지니고 있다.

이로써 Nebulas Rank의 물리적 중요성과 의미를 이해하는데 도움을 주는 기존의 화폐모델 구축한다.

우선, 암호화폐 생태계 내에서 “유동성”을 측정하기 위한 지표를 제공하려 한다. 경제 체제에서 속도 요소(Velocity Factor)와 구별되는데 필요한 또 다른 필수 개념은 유동성이다. 유동성은 교환의 수단을 위해 자산을 교환할 때의 난이도를 나타낸다. 자산 자체가 경제학의 중요한 매개체이기 때문에 최고의 유동성을 가진 요소는 바로 자산이라고 할 수 있다.

> 특별 참고: Nebulas 화이트 페이퍼(기술백서)[3]에서는 유동성이라는 단어를 자주 언급했다. 그러나 유동성에 대한 엄격한 정의는 없으며 경제학에서도 그 의미가 매우 넓다. 예를 들어, “새로운 폴그레이브: 경제 사전”에서 유동성을 설명하는 항목에는 완전히 다른 세 가지 양상이 포함된다. R.S Kroszner는 지난 6개월 동안 유동성에 대해 언급한 2,795개의 독립적인 논문을 보유하고 있으며, 각각의 논문은 일반적으로 다른 성명서를 냈다고 언급한다[22]. 본 옐로우 페이퍼에서 언급되는 유동성은 일정 기간동안 화폐 단위의 회전율을 의미하며, 이는 자산의 유동 속도를 의미한다.

암호화폐의 유동 속도를 사용하여 암호화폐의 회전율을 나타내는데[23], 즉 화폐 단위를 일정한 기간내의 회전율을 V로 표시한다. 기존 화폐이론에 따르면 이와 관련된 방정식은 다음과 같이 나타낸다:

$$M \times V = P \times Y \tag{7}$$

여기서 M, V, P 및 Y는 경제 시스템의 총 화폐 수량, 화폐의 속도, 가격 수준(단위 경제 산출의 화폐로 측정하며, 화폐 가격은 $\frac{1}{p}$ 이다.) 그리고 실제 경제 생산량(GDP) 각각 나타낸다. 위 방정식(7)은 화폐의 수량과 화폐의 속도의 곱은 화폐의 가격과 경제 생산량의 곱과 동일하다는 것을 보여준다.

총 화폐 수량 M의 경우 Nebulas는 이더리움과 비슷하지만 비트코인과 다른 점은 화폐 수량이 꾸준히 증가하고 있다는 점이며(Nebulas 화폐 NAS의 추가 발행 비율은 현재 4 %로 설정됨), 후자의 금액은 총 2100만 개의 코인이 채굴되면 안정될 것이다. 화폐의 속도 V는 회전되는 화폐 금액 및 화폐 공급의 비율로 나타낼 수 있다. 결과적으로, 방정식(7)은 더 나아가 다음과 같이 표현 될 수 있다:

$$(M + \Delta m) \times \frac{\sum_{(s,t,w,\tau)\in\mathcal{T}} w}{M} = P \times Y \tag{8}$$

여기서 Δm은 추가적으로 발행할 화폐량을 의미한다. 가격 수준 P의 관점에서 볼 때, 가격의 가치는 기존 화폐이론과 새로운 케인스 모델(New Keynesian Models)를 기반으로 화폐 수요와 공급 간의 관계에 의해 결정된다. 장기적으로 전체 가격 수준은 화폐 공급과 수요가 균형점에 유지되도록 조정할 예정이다.

그러나 단기적으로 보았을 때, 전체 가격 수준 자체가 화폐의 공급과 수요의 균형점에 항상 머무리지는 않을 것이다. 건강한 경제 시스템에서 가격의 성장률은 종종 화폐의 성장도 보다 느리다. 화폐 공금을 적절히 증가시킴으로써(즉, 이자율을 낮춤으로써), 가격 P의 증가와 동시에 상품 및 서비스 수요량 Y가 증가할 것이다. 반면에 과도한 성장 기대로 인해 사용자가 암호화폐 자산 보유상태를 유지하지 못하도록 제어해야하므로 오히려 화폐의 회전율 속도가 저하될 수 있다.

실질적인 경제 생산량 Y의 경우, 경제학자들은 대개 실질 GDP, 즉 일정 기간동안 생산된 모든 재화와 서비스의 시장 가치에 대한 경제적인 척도로 나타낸다. 기존 화폐이론에서 크게 다를 바 없이 암호화폐의 가치는 회전율에 기반한다고 생각하며, 각 거래는 전체 경제적 집합에 다소 기여한다고 믿는다. 즉, 거래가 발생하면 암호화폐의 유동성은 어느정도 증가하게 될 뿐만 아니라 암호화폐에 대한 참여자의 인식과 신뢰도 또한 다소 향상된다. 결과적으로 방정식(8)의 Y는 각 거래에서 파생된 구성을 보인다. 경제 시스템의 주체가 계정이라는 것을 감안할 때 Y는 각 계정에서 발행한 거래로 설명할 수 있다:

$$Y = \sum_{a\in\mathcal{A}} \mathcal{C}(a) \tag{9}$$

여기서 $C(a)$는 계정 a가 총 경제 생산량, 즉 Core Nebulas Rank에 참여한 기여도 지수를 나타낸다. Nebulas 팀은 암호화폐의 발전은 지속적인 커뮤니티 구축과 개발에 달려 있다고 믿는다. 따라서, 각 계정별로 기여도를 정량화하는 것이 합당한 인센티브 메커니즘을 설계하는 초석이라고 생각한다. 이를 토대로 경제 시스템은 명시적인 인센티브(예: Nebulas 기술백서의 Proof of Devotion 합의 알고리즘)

또는 암시적 인센티브(검색엔진에서 제공하는 검색결과)를 만들 수 있다. 암호화폐에서의 지침과 인센티브는 기존의 화폐이론과 차별화되며 화폐의 추가 발행을 의미한다.

4 Nebulas Rank

Core Nebulas Rank는 일정 기간 동안 전체 경제체를 기준으로 한 사용자 기여도를 측정하는 데 사용된다. 정확한 계산은 비교적 복잡하므로 계산을 위한 근사 알고리즘을 제안한다. 이 근사 알고리즘에서 두 가지 중요한 요인인 계정이 보유한 화폐와 거래 네트워크의 계정 위치 정보를 고려한다. 아래의 평가는 근사 알고리즘의 정확성에 대한 유효성을 제공한다:

일정 기간 동안 메인 네트워크의 거래 내역을 Core Nebulas Rank의 데이터 소스로 사용한다. 기간 $[t_0 - T, t_0]$의 모든 거래는 집합으로 지정할 수 있다:

$$\Theta(t_0) = \{(s, t, w, \tau) \mid t_0 - T \leq \tau \leq t_0 \ \wedge \ w > 0 \wedge s \neq t\} \tag{10}$$

$\Theta(t_o)$에 기반하여 가중치 적용 그래프를 정의 할 수 있고, 노드는 계정의 주소를 참조하고, 노드 s에서 노드 d까지의 엣지는 하나의 거래를 나타내며, 엣지의 가중치는 c이며, 엣지의 시간 τ으로 나타낸다.

계정 $a \in A$의 경우 Core Nebulas Rank $C(a)$의 계산은 $\Theta(t_o)$를 기반으로 하며 다음과 같이 나타낼 수 있다:

$$\mathscr{C}(a) = \Omega(\beta(a)) \times \Psi(\gamma(a)) \tag{11}$$

$\beta(a)$는 일정 기간동안 계정 a의 중간 지분값이다. $\gamma(a)$는 일정 기간동안의 입출력 계좌의 정도를 나타낸다.

> 특별 참고: Nebulas 화이트 페이퍼(기술백서)[3]에서 Core Nebulas Rank를 계산하는 방법과 달리 다음과 같이 몇 가지 업데이트 사항을 제시한다:
>
> 1. 거래 그래프를 작성할 때 가중치로 K 상위 거래량을 더 이상 사용하지 않는다.
> 2. 더 이상 노드의 중요성을 달성하기 위해 LeaderRank의 노두 가중치에 의존하지 않는다. 첫째, 입출력 정도를 계산하기 이전에 거래 루프를 제거하므로써 루프 공격에 견딜 수 있다. 동시에 여전히 엣지의 가중치를 고려한다. 동일 토폴로지 그래프, PageRank 및 일부 다른 대칭함수(예: LeaderRank)는 시빌 공격에 저항할 수 없다는 것이 입증되었다[20]. 본 옐로우 페이퍼에서는 더 이상 토폴로지와 같은 랭킹 전략을 사용하지 않는다. § 4.3에서 낮은 지분 노드를 위조하여 보상을 줄이는데 도움이 되는 비대칭 연산 기능 21을 제안한다.

4.1 중간값 계정 지분 $\beta(a)$

$[t_0 - T, t_o]$의 기간에는 블록체인 시스템에 n개의 블록이 있으며, 아래와 같이 표기된다:

$$B_o, B_1, \ \ldots, B_n$$

B_i는 B_{i+1}의 부모 블록을 나타냅니다. 계정 $a \in A$의 경우 각 블록의 끝에있는 계정의 잔액은 아래와 같이 표기된다:

$$d_o^a, d_1^a, \ldots, d_n^a$$

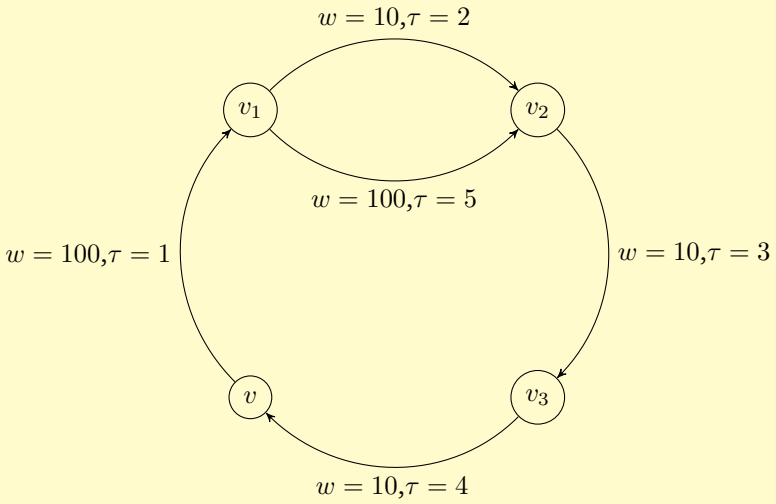
항목을 오름차순으로 정렬하여 새 목록을 가져올 수 있다:

$$d_{(0)}^a, d_{(1)}^a, \ldots, d_{(n)}^a$$

여기서 $d_{(i)}^a < d_{(i+1)}^a, 0 \leq i \leq n-1$이며, 따라서 $\beta(a)$는 아래처럼 나타낼 수 있다:

$$\beta(a) = \begin{cases} d_{(k)}^a & \text{for} \quad n = 2 \times k, k = 1, 2, 3, \ldots \\ (d_{(k)}^a + d_{(k+1)}^a)/2 & \text{for} \quad n = 2 \times k + 1, k = 1, 2, 3, \ldots \end{cases} \tag{12}$$

중앙값 계정 지분은 특정 방식으로 코인을 나타낸다. 즉, 계정이 기간의 절반 이상 동안 지분을 보유해야 함을 의미한다.



$$H(v) = \{(v, v1, 100, 1), (v1, v2, 10, 2), (v2, v3, 10, 3), (v3, v, 10, 4)\}$$

그림.1: 거래에서 루프 전달

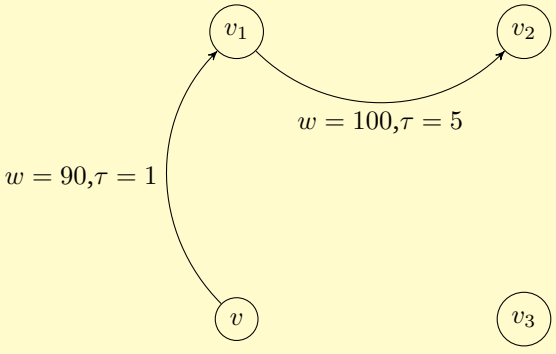


그림.2: 그림.1에서 전달 루프를 제거한 거래 그래프

4.2 입출력 정도(In-and-Out Degree)

공격자가 루프 공격을 사용하여 출입률을 높일 수 있다고 가정해보자. 이러한 상황을 저지하려면 거래 그래프의 입출력(in-and-out) 정도를 계산하기 전에 전달 루프를 제거해야 한다. 전달 루프는 순차적인거래 루프이다. 거래 그래프의 엣지 집합인 동일한 노드 v에서 시작하고 끝난다. 전달 루프는 $H(v)$로 표기 할 수 있다:

$$H(v) - \{(v, v_1, w_1, \tau_1), (v_1, v_2, w_2, \tau_2), \ldots, (v_i, v_{i+1}, w_i, \tau_i), \ldots, (v_n, v, w_{n+1}, \tau_{n+1})\}$$

그 중, $\forall 1 \leq i \leq n : \tau_1 \leq \tau_{i+1}$은 그림.1에 제공된 바와 같이, 전달 루프가 존재하며, 전달 루프 내에 거래 $(v_1, v_2, 100, 5)$는 포함되지 않는다는 것을 주목해야 한다. 전달 루프를 찾은 후에 루프를 제거한 다음 사용해야 한다.시스템에 n개의 전달 루프가 있다고 가정하면 전달 루프는 다음과 같은 순서로 나열된다:

$$H^1(v_1), H^2(v_2), \ldots, H^n(v_n)$$

$H^i(v_i)$내에 최소 거래량은 $(s_m^i, t_m^i, w_m^i, \tau_m^i)$이며, 그리고

$$\forall (s^i, t^i, w^i, \tau^i) \ \in \mathcal{T} : w^i \geq w_m^i$$

$H^i(v_i)$내에 최소 거래량은 w_m^i이며, $H^i(v_i)$의 각 거래에 대해 최소 거래량을 적절히 뺀 다음 최신 거래 금액이 0인 경우 이 거래를 제거해야 한다:

$$\mathcal{E}((s,t,w,\tau), w_m) = \begin{cases} (s,t,w-w_m,\tau) & \text{if} \quad w \neq w_m \\ \phi & \text{if} \quad w = w_m \end{cases}$$

$$\Theta'(t_0) = \Theta(t_0) - H^i(v) \cup \{\mathscr{E}(t), t \in H^i(v_i)\} \quad i = 1,2,\ldots,n \tag{13}$$

그림.2는 그림.1의 전달 루프를 제거한 후의 비(非) 루프 거래 그래프이다.

노드 v의 입력 정도를 $p(v)$로 설정한다:

$$p(v) = \sum_{(s_i, v, w_i, \tau_i) \in \Theta'(t_0)} w_i \tag{14}$$

위와 비슷하게 노드 v의 출력 정도는 아래 방정식과 같다:

$$q(v) = \sum_{(v, t_i, w_i, \tau_i) \in \Theta'(t_0)} w_i \tag{15}$$

이 경우, 노드 v의 입출력 정도 $\gamma(v)$는 다음과 같다:

$$\mathcal{G}(v) = (p(v) + q(v)) \cdot e^{-2\sin^2(\frac{\pi}{4} - \arctan\frac{q(v)}{p(v)})} \tag{16}$$

위의 함수 도형은 그림.3과 같으며 기능 14의 곡선을 나타낸다.

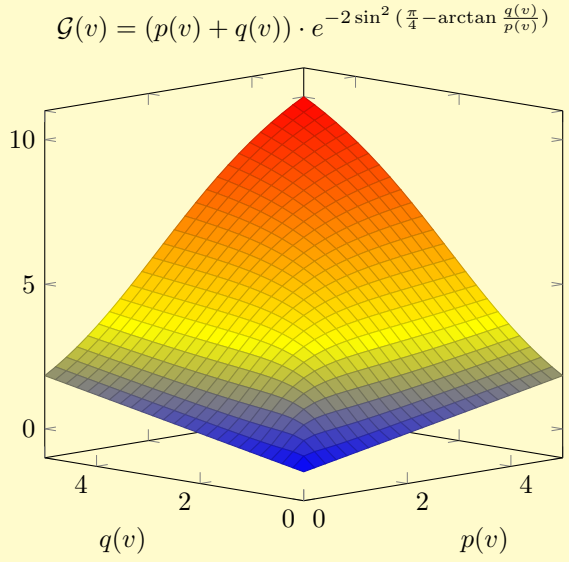


그림.3: 입출력 정도 기능의 곡선

$$\gamma(v) = (\frac{\theta \cdot \mathcal{G}(v)}{\mathcal{G}(v) + \mu})^{\lambda} \tag{17}$$

여기서 θ, μ, λ는 결정할 매개 변수이다.

4.3 Wilbur 함수

각기 다른 사용 사례와 관련 특징들을 전부 고려하게 되면 Core Nebulas Rank를 계산하는 것은 매우 복잡해진다. 그러나 Nebulas Rank에 대해 보다 일반적인 기능을 제공 할 수 있다. Core Nebulas Rank의 계산 함수를 $f(x)$, 즉 Wilbur 함수[1]라고 정의한다. 여기서 x는 Core Nebulas Rank의 요소이며, 계정 지분, 코인 또는 입출력 정도라고 볼 수 있다. $f(x)$는 두 가지 속성을 충족시킨다:

속성 1. 0보다 큰 두 변수 x_1과 x_2에 대해 두 함수의 합은 두 변수의 합계 함수보다 작다.

$$f(x_1 + x_2) > f(x_1) + f(x_2) \quad x_1 > 0, x_2 > 0 \tag{18}$$

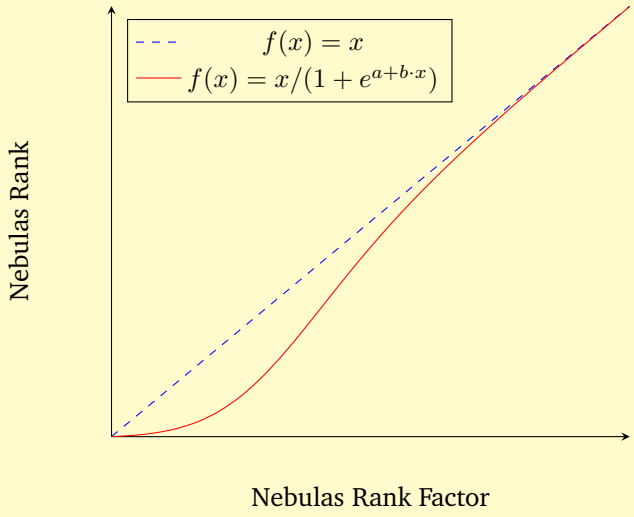


그림.4: Nebulas 기능을 나타내는 곡선

속성 2. 두 변수 x_1과 x_2가 무한대라면 두 함수의 합은 두 변수의 합계 함수와 거의 동일하다.

$$\lim_{x_1 \to \infty, x_2 \to \infty} f(x_1 + x_2) = f(x_1) + f(x_2) \quad x_1 > 0, x_2 > 0 \tag{19}$$

[1] 시빌 공격(Sybil Attack)이라는 이름은 1970년 TV 미니 시리즈 시빌(Sybi)l에서 유래됐다. 시빌 시리즈에서는 젊은 여성이 정신 질환자로 진단 받고 Dr. Cornelia Wilbur라는 정신과 의사로부터 치료를 받았다. Wilbur 함수의 유래 또한 살펴볼 수 있다.

위에 설명된 이러한 특징은 특정 거래 행위에 따라 지분을 작은 계정으로 분할하는 이점이 단일 계정 내에 유지하는 것보다 비교적 작음을 보장한다. 동시에, 지분이 충분히 크면 지분을 작은 계정으로 나누는 비용을 무시할 수 있다. 위의 두 가지 특성을 만족하는 함수가 두 가지 이상 존재한다. 여기서는 간결한 함수를 제공하고 함수의 곡선을 그림.4로 제공한다.

$$f(x) = x/(1 + e^{a+b\cdot x}) \quad a > 1, b < 0 \tag{20}$$

함수에 대한 자세한 내용은 부록 A에 수록되어 있다.

요컨대, 방정식 (11)은 다음과 같이 더 나타낼 수 있다:

$$\mathscr{C}(v) = \frac{\beta(v)}{1 + e^{a+b\cdot\beta(v)}} \cdot \frac{\gamma(v)}{1 + e^{c+d\cdot\gamma(v)}} \tag{21}$$

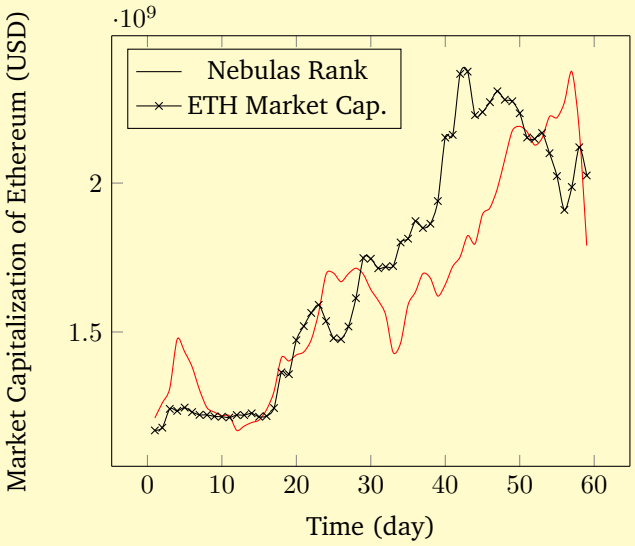


그림.5: 시가총액과 이더리움의 Core Nebulas Rank

여기서 a, b, c, d는 결정될 매개 변수다.

함수의 유효성을 증명하기 위해 일정 기간동안 이더리움 블록체인의 모든 계정에 대한 Core Nebulas Rank를 계산한다. Nebulas 팀은 2017년 5월 1일부터 2017년 6월 30일까지(블록 높이 : 3629091에서 3955158까지) 모든 거래 기록을 수집했으며 또한 일일 평균 ETH 토큰 가격(달러 기준)과 거래량에 대한 데이터를 수집했다[24].

그림.5는 ETH 시가 총액과 이더리움의 Core Nebulas Rank 사이의 추세를 보여주며 검은색 실선은 ETH 시가 총액(달러 기준)을 나타내고 빨간색 실선은 방정식(21)를 기반으로 산출된 모든 계좌의 Core Nebulas Rank 합계를 나타낸다.

Core Nebulas Rank가 이더리움의 시가총액 변동을 정확하게 반영하고 있음을 알 수 있다. 상관 계수는 0.84427, p(p 값)은 $4.48 \times 10^{-17} < 0.001$이다. 즉 방정식(11)은 Core Nebulas Rank의 타당성과 정확성을 모두 보여주는 체인상의 경제 시스템에 대한 사용자 기여도를 성공적으로 보여준다.

5 Core Nebulas Rank의 반(反)부정 행위

본 장에서는 Core Nebulas Rank가 Nebulas Rank의 공정성과 같이 부정행위에 어떻게 저항하는지 분석하고자 한다.

공격자가 시도할 수 있는 부정행위에는 임의적인 자산 이체 및 타인의 자산 또는 계정을 제어하여 공격자 스스로의 개인 이익을 위해 부정한 행동을 하는 것이 포함된다. 자산 이체 중 자산의 양은 공격자가 소유한 자산을 초과하지 않는다. 이체 소스는 공격자와 협력자가 소유한 계정이거나 교환의 역할을 하는 일부기관의 계정이다. 일반적으로 얻을 수있는 이익은 개인 키가 공격자가 알고있는 계정에 의해 결정된다. 간단한 경우는 공격자의 이익이 모든 계정의 랭킹 지수를 합한 것이다. 물론 이전에 언급한 기관 계정의 개인 키가 공격자에 의해 제어되지 않는다는 것을 알 수 있다.

본 장에서의 분석은 수행된 작업과 위에 정의된 공격자의 이점을 기반으로 한다. 먼저 단일 계정의 랭킹 지수 향상에 대한 상한선을 논의하고자 한다. 그리고 여러 계정에 대한 상한을 분석한다. 마지막으로, 공모의 상황을 가정해, 한 명 이상의 공격자의 상황을 논의하고자 한다.

5.1 단일 계정의 랭킹 지수 상향

방정식(21)에 따르면 하나의 계정에 대한 랭킹 지수를 높이기 위해 계정의 랭킹 지수는 자산 금액과 입출력 정도의 상관 관계가 존재한다. 계정에 있는 자산의 양 β는 상한이 정해져 있다. 즉, 0으로 표시된 공격자가 소유한 자산의 절대합계 β_o를 넘지 않는다. 그리고 입출력 정도 γ는 이체의 양을 나타낸다. 즉, 공격자가 통제하는 계정의 이체 금액을 가능한 많이 늘려놔야 함을 의미한다.

이체량의 증가는 입력 정도의 증가 및 출력 정도의 증가, 두 가지 부분을 포함한다. 입출력 정도를 높이려면 두 개의 참여 계정이 필요하며, 그 중 하나는 랭킹 지수를 올리는 것이 목표인 계정이고, 다른 계정은 제어한 계정이거나 제어되지 않은 계정일 수 있다. 제어되지 않은 계정이라면, 입출력 정도가 증가한다는 것은 타인과 거래하는 것을 의미하며, 이 상황은 §5.3에서 구체적으로 논의하고자 한다. 또 다른 경우로는 공격자가 대상에게 무조건적으로 자산을 보낸다. 그러나 이 방법 실행하기 위한 값이 비싸기 때문에 본 장에서는 논의하지 않는다. 따라서 일반적으로 공격자의 행동은 주로 자신이 관리하는 계정 간의 이체를 늘리는 데 중점을 둔다. 공격자가 관리하는 자산은 제한적이며 랭킹을 지정하는 기간도 제한되어 있으므로 계정의 랭킹은 공격자가 보유한 자산의 양에 따라 결정되는 상한선을 유지해야 한다.

위에서 분석한 바와 같이 동일한 소유자의 계정으로 거래하는 시나리오를 고려하고자 한다. §4.3에서 정의된 연산 방법 중 방정식(21)에 기반하여 자산 전송을 여러 개로 분할하면 공격자의 이익이 감소한다. 따라서 공격자는 거래 금액을 가능한 한 높게하려고 시도할 것이다. 즉, 소유하고 있는 모든 자산을 계정으로 전송한 다음 모든 자산을 재전송하려고 시도할 것이다. 주기 제거 알고리즘(Cycle-removal Algorithm)으로 인해 해당 기간동안 공격자는 자신의 자산을 다시 이전할 수 없다. 그리고 입출력 정도는 $\gamma = 2\beta_o$이다. 랭킹 지수는 $\mathscr{C} = \frac{2\beta_0^2}{(1+e^{a+b\cdot\beta_0})(1+e^{c+2d\cdot\beta_0})}$ 이다.

만약 공격자가 오프체인 거래를 사용해 자산을 다른 계정으로 옮기고 또 다시 목표 계정으로 옮긴다고 가정한다면 이 때의 최대 입출력 정도의 합은 자산의 이체량에 자산의 수만큼 곱한 수이다. 랭킹을 지정하는 기간이 제한되어있기 때문에 이체량은 상수이다. 그리하여 γ의 상한선은 $2T\cdot\beta_o$으로, 이 중 T는 시간을 길이를 측정하는 상수이다. 최대 랭킹 지수는 $C = \frac{2T\cdot\beta_0^2}{(1+e^{a+b\cdot\beta_o})(1+e^{e^c+c\cdot c\cdot d\cdot\beta_o})}$이다.

5.2 다수 계정의 랭킹 지수 상향(시빌 공격)

Sybil Attack은 P2P 네트워크의 평판 시스템을 악의적으로 조작하기 위해 많은 수의 허위의 계정을 생성하여 인위적인 지수를 얻는 것을 말한다[25]. P2P 네트워크상의 주체는 로컬 리소스에 대한 액세스 권한이 부여된 소프트웨어이다. 주체는 신원을 제시하여 P2P 네트워크에 자신을 알린다. 하나 이상의 ID가 하나의 주체에 해당한다고 볼 수 있다. 즉, 개체에 대한 ID 매핑은 배수일 수 있다는 것이다. P2P 네트워크의 주체는 가회성 회로(Redundancy), 리소스 공유, 안정성 및 무결성을 위해 여러 ID를 사용한다. P2P 네트워크에서 ID는 추출의 방법으로서 사용되므로 원격 주체는 로컬 주체에 대한 ID의 통신을 반드시 알지 못해도 ID를 인식할 수 있다. 기본적으로 각 별개의 ID는 일반적으로 별개의 로컬 주체에 해당한다고 가정해보자. 실제로 많은 ID는 동일한 로컬 주체에 해당 할 수 있다. 공격자는 다수의 개별 노드로 나타나고 기능하기 위해 P2P 네트워크에 여러 개의 신원을 제시할 수 있다. 따라서 공격자는 투표 결과에 영향을 줌으로써 네트워크에 대한 통제력을 획득 할 수 있게 된다[26].

여기서 공격자의 보수는 공격자가 관리하는 모든 계정의 합계라고 가정한다. 마지막 하위 섹션에서 분석 한 하나의 계정에 대한 랭킹 지수를 높이는 전략을 고려하면 공격자는 동일한 계정을 여러 계정에 적용할 수 있다. 하나의 계정에서 시작하여 공격자가 자산의 일부를 다음 계정으로 이전하여 최종적으로 연결된 자산 흐름 형성한다. 이 경우 Core Nebulas Rank는 계정의 유효 금액 이상이 해당 기간의 절반 이상 동안 계정에 남아 있지 않아야하므로 공격자가 둘 이상의 계정을 소유한 총 자산 금액으로 만들 수가 없다. 따라서 공격자는 자산이 모든 계정에 균등하게 분배되는 또 다른 전략을 채택해야 한다. 링크 길이가 N, 즉 N개의 제어된 계정이 있고 모든 계정에 대해 $\beta = \frac{\beta_o}{N}$ 이라고 가정한다. 입력 및 출력 정도 분석은 §5.1과 동일하며, 상한은 γ는 $K \cdot \beta$이며, 여기서 $K = 2 \cdot N$은 상수이다. 따라서 공격자가 소유한 모든 계정의 합계의 상한선은 다음과 같다:

$$\mathscr{C} = N \cdot \frac{K\frac{\beta_0^2}{N}}{(1+e^{a+b\cdot\frac{\beta_0}{N}})(1+e^{c+K\cdot d\cdot\beta_0})} = \frac{K\beta_0^2}{(1+e^{a+b\cdot\frac{\beta_0}{N}})(1+e^{c+K\cdot d\cdot\beta_0})} \tag{22}$$

5.3 합동 조작

합동 조작의 결과는 한 명의 공격자가 두 명의 공격자의 총 자산을 소유한 경우와 다를 바 없다. 이 경우에서 단일 공격자의 자산 증가의 결과를 분석함으로써 합동 조작의 사례를 분석하고 사전에 대응할 수 있게 된다.

6 Core Nebulas Rank의 시행

본문의 논의 범위 안에는 Core Nebulas Rank의 완전한 시행에 대해 포함하고 있지 않기 때문에 본 장에서는 Core Nebulas Rank의 시행을 위한 핵심 포인트에 대해서만 논의하고자 한다.

6.1 온체인 혹은 오프체인?

Core Nebulas Rank는 경제 총량에 대한 각 계정의 기여도를 제시한다. 일반적으로 각 노드는 과거 블록 정보를 기반으로 총 경제 규모에 대한 지정된 계정의 기여도를 계산할 수 있다. 그러나 우리는 주기적으로 Nebulas Rank를 꼭 온체인의 형태로 구축해야할 필요성에 대한 의문이 들었다.

다음 두 가지 이유로 인해 Nebulas Rank를 온체인의 형태로 구축하지 않아도 된다고 결정했다:

- 체인은 막대한 양의 데이터를 저장하기에 부적합하며, IPFS, Genaro[27][28]와 같이 데이터 저장을 목표로 하는 퍼블릭 체인일지라도, 주기적으로 모든 계정에 대한 데이터를 저장하는 Core Nebulas Rank 에 적합하지 않다고 판단되었다.
- Core Nebulas Rank에 대한 연산은 블록 생성 속도에 영향을 미치는데, Core Nebulas Rank의 연산 방식은 비교적 복잡하다. 만약 연산 결과가 온체인과 블록 생성 속도 및 검증 속도에 영향을 끼치면, 시스템 전체 TPS의 감소를 초래할 수 있다.

각 노드가 Core Nebulas Rank를 자체적으로 연산이 가능하다고 판단 되어진다. 그러나 노드가 자체적으로 Core Nebulas Rank를 연산하는 경우 Core Nebulas Rank 연산의 신뢰성을 보장하는 방법이 중요한 문제가 될 수 있다. 예를 들어, 노드는 Core Nebulas Rank의 연산 결과를 임의로 변경하여 연산 오류가 있는 Core Nebulas Rank를 기반으로 지정된 인센티브를 잘못 부여할 수 있다. 중요한 어플리케이션의 경우, Core Nebulas Rank와 관련된 연산을 각 노드에서 검사하여 결과의 공정성을 보장해야 한다. 반대로, 중요도가 다소 떨어지는 어플리케이션의 경우, Core Nebulas Rank의 사용은 어플리케이션 자체에 의해 상이하며, Core Nebulas Rank에 대한 확인 여부는 어플리케이션에 따라 달라진다.

노드가 Core Nebulas Rank를 자체적으로 연산할 시, 노드가 에너지 소비 문제를 고려하여 Core Nebulas Rank의 연산을 거부하는 것 또한 주요한 문제이다. 이와 관련하여 신뢰할 수 있는 Core Nebulas Rank 서비스를 도입하여 각 노드에서의 중복 연산을 방지할 수 있을거라 본다. 이 서비스는 무료 또는 횟수로 연산하여 사용할 수 있다. 구체적인 시행 및 서비스 세부 사항은 본문의 범위를 벗어나기 때문에 추후에 관련 사항을 업데이트할 예정이다.

6.2 Core Nebulas Rank의 업데이트

Core Nebulas Rank는 암호화폐의 생태계와 밀접한 관련이 있으며, 생태계가 변화함에 따라 Core Nebulas Rank의 연산 또한 지속적으로 업데이트 되어야 하며, 특히 그 중 다양한 매개 변수가 필요하다. Core Nebulas Rank의 연산을 빠르게 업데이트하는 방법이 매우 중요하다. 이와 관련하여, Nebulas Force 알고리즘을 통해 Core Nebulas Rank 연산의 빠른 업데이트를 보장할 것 이다.

자세히 설명하자면, 블록 구조를 새롭게 갱신 할 시 새로운 블록 구조에는 Core Nebulas Rank의 알고리즘과 매개 변수를 포함될 것이다(LLVM IR의 형태). Nebulas의 가상 머신(NVM)는 알고리즘의 실행 엔진으로써, 블록에서 Core Nebulas Rank의 알고리즘 및 매개변수를 생성하고 알고리즘을 실행하여 각 노드 내에서 계정의 Core Nebulas Rank를 얻는다.

알고리즘 또는 매개 변수를 업데이트 해야 하는 경우, 커뮤니티와 함께 최신 알고리즘 및 매개 변수를 새 블록에 포함시켜 전체 업데이트 프로세스의 적시성 및 원활성을 보장하고 발생 가능한 분기를 방지한다.

7 Extended Nebulas Rank

Core Nebulas Rank는 전체 암호화폐의 경제총량에 대한 계정 주소의 기여도를 측정한 것이다. Core Nebulas는 PoD(기여도증명 합의 알고리즘) 및 DIP(개발자 인센티브 프로토콜)의 사용 사례에 굉장히 중요한 영향을 끼치며, 실제로 Core Nebulas Rank의 사용 사례와도 일치한다. 그러나 예의주시 했듯이, 다른 평가가 필요할 수 있는 다른 사용 사례가 항상 존재할 것이며, 이를 위해 Extended Nebulas Rank를 설계했다. Extended Nebulas Rank는 Core Nebulas Rank를 기반으로 다양한 사용 사례 하에서도 Nebulas 생태계의 지속적인 발전을 장려할 것을 보장한다.

7.1 스마트 컨트랙트 중심의 Extended Nebulas Rank

스마트 컨트랙트의 랭킹은 Nebulas 생태계와 경제 내에서 중요한 역할을 한다. 한편으로는 사용자가 양질의 DApp을 찾는데 보다 많은 도움을 준다. 그리고 다른 한편으로는 개발자들이 양질의 DApp을 개발하도록 장려하여 생태계가 지속적으로 발전될 수 있다.

스마트 컨트랙트의 랭킹은 스마트 컨트랙트에 대한 계정 주소의 호출과 스마트 컨트랙트 간의 호출이라는 두 가지 요인에 의해 결정된다. 먼저 스마트 컨트랙트에 대한 계정 주소의 호출을 계정 주소로 간주하여 계정 주소는 경제 총량에 대한 기여를 스마트 컨트랙트에 분배하여 각 스마트 컨트랙트가 초기 배점을 갖도록 한다. 스마트 컨트랙트 간의 호출을 방향 비순환 그래프(Acyclic Graph)로 간주하고, Page Rank를 사용하여 각 스마트 컨트랙트의 최종 Nebulas Rank를 도출한다.

7.2 다차원적인 Extended Nebulas Rank

일부 어플리케이션에서는 블록체인의 데이터 관련성을 계산하기 위해 다차원의 데이터가 필요하다는 것을 알게 되었다. 예를 들어, 블록체인 기반 광고 시스템은 다차원적으로 제공되어야 하는 광고 및 사용자에 대한 상관 관계 연산이 필요하다. 이러한 경우에서 Extendede Nebulas Rank는 다차원적으로 쓰일 수 있으며, 벡터로도 표현되는데, Core Nebulas Rank도 그 중 하나에 포함된다.

Extended Nebulas Rank는 다차원적이며, Core Nebulas Rank 이외에도 특정 어플리케이션 현황에 따라 다른 차원에서 활용할 수 있다. 해당 차원의 실질적 사용 가능 여부는 각 어플리케이션 현황에 달려있다. 그럼에도 불구하고, Extented Nebulas Rank의 연산 방식은 언제나 Core Nebulas Rank의 연산 방식을 참조할 수 있다.

스마트 컨트랙트의 Extended Nebulas Rank와 같은 실제 어플리케이션 현황을 통해 Extended Nebulas Rank의 시행 방법을 서술하고, 해당 가치 측정 값을 제공한다. 또한 보다 다양한 사용 사례에서 가치 측정의 가능성을 열어주는 다차원적인 Extended Nebulas Rank를 제공한다.

8 향후 개발사항

Nebulas Rank의 궁극적 목표는 계정 주소와 같은 주체가 경제적 총량에 기여하는 관점에서 블록체인의 데이터를 측정하는 것이 아니라 이에 필요한 가치측정의 척도를 제공하는 것이다. 따라서 향후에는 지속적으로 많은 개발사항들이 진행될 예정이다. 다음은 Nebulas 팀에서 특별히 주의를 기울여 진행하고자 하는 개발사항들을 간략하게 설명하고자 한다:

- 크로스 체인의 Nebulas Rank. 향후 반드시 크로스 체인의 데이터 전송에 대한 높은 수요가 있을 것이라고 예측한다. 대표적인 예로, 크로스 체인 데이터 상호 작용 혹은 디지털 자산 전송 등은 서로 다른 체인 위에서의 서로 다른 가치를 일률적으로 측정해야 한다. 구체적으로, 개발자들은 DApp를 하나의 체인에서 다른 체인으로 이동시켜야만 하는 상황이 있을 것이다. 이때 각기 다른 체인 위에서 Dapps의 가치를 측정할 수 있는 가치측정 척도가 필수적일 것이다.
- 경제적 총량에 대한 기여도를 측정하는 척도. Nebulas 랭킹은 경제적 총량에 대한 기여도를 기반으로 한다. 그러나 블록체인은 지속적으로 성장할수록 그에 상응하는 커뮤니티를 필요로 한다. 그러므로 경제적 집합체적인 측면에서 커뮤니티의 공헌과 기여를 절대 무시할 수 없다. 커뮤니티에서 개인이나 조직의 기여도를 측정 및 평가하는 방법과 Nebulas 랭킹에 어떻게 반영되는지에 대한 중요도는 굉장히 클 것이다.

참조 문헌

[1] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, “A fistful of bitcoins: characterizing payments among men with no names,” in *Proceedings of the 2013 conference on Internet measurement con- ference*, pp. 127–140, ACM, 2013.

[2] “Http cookie.” https://en.wikipedia.org/wiki/HTTP_cookie.

[3] “Nabulas Technical White Paper.” https://nebulas.io/docs/ NebulasTechnicalWhitepaper.pdf. Accessed: 2018-04-01.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[5] “Namecoin.”https://namecoin.org.

[6] “Openassets protocol.” http://github.com/OpenAssets/ open-assets-protocol.

[7] V. Buterin *et al.*, “Ethereum white paper,” 2013.

[8] “Forget fintech – welcome to the valueweb.” http://thefinanser.com/2015/ 02/forget-fintech-welcome-to-the-valueweb.html/.

[9] L. Page, S. Brin, R. Motwani, and T. Winograd, “The pagerank citation ranking: Bringing order to the web.,” tech. rep., Stanford InfoLab, 1999.

[10] M. Fleder, M. S. Kester, and S. Pillai, “Bitcoin transaction graph analysis,” *arXiv preprint arXiv:1502.01657*, 2015.

[11] Q. Li, T. Zhou, L. Lu¨, and D. Chen, “Identifying influential spreaders by weighted LeaderRank,” *Physica A: Statistical Mechanics and its Applications*, vol. 404, pp. 47–55, 2014.

[12] A. Cheng and E. Friedman, “Manipulability of pagerank under sybil strategies,” 2006.

[13] “NEM Technical Reference.” http://nem.io/NEM_techRef.pdf. Accessed: 2017-08-01.

[14] A. N. Nikolakopoulos and J. D. Garofalakis, “NCDawareRank,” *Proceedings of the sixth ACM international conference on Web search and data mining - WSDM ’13*, no. February 2013, p. 143, 2013.

[15] X. Xu, N. Yuruk, Z. Feng, and T. A. Schweiger, “Scan: a structural clustering algorithm for networks,” in *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 824–833, ACM, 2007.

[16] H. Shiokawa, Y. Fujiwara, and M. Onizuka, “Scan++: efficient algorithm for finding clusters, hubs and outliers on large-scale graphs,” *Proceedings of the VLDB Endowment*,

vol. 8, no. 11, pp. 1178–1189, 2015.

[17] L. Chang, W. Li, L. Qin, W. Zhang, and S. Yang, “pscan: Fast and exact structural graph clustering,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 2, pp. 387–401, 2017.

[18] J. Hopcroft and D. Sheldon, “Manipulation-resistant reputations using hitting time,” in *International Workshop on Algorithms and Models for the Web-Graph*, pp. 68–81, Springer, 2007.

[19] J. Zhang, R. Zhang, J. Sun, Y. Zhang, and C. Zhang, “Truetop: A sybil-resilient system for user influence measurement on twitter,” *IEEE/ACM Transactions on Networking*, vol. 24, no. 5, pp. 2834–2846, 2016.

[20] A. Cheng and E. Friedman, “Sybilproof reputation mechanisms,” in *Proceed- ings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, pp. 128–132, ACM, 2005.

[21] M. Swan, *Blockchain: Blueprint for a new economy*. O’Reilly Media, Inc., 2015.

[22] R. S. Kroszner, “Liquidity and monetary policy,” 2007.

[23] R. Selden, “Monetary velocity in the united states,” 1956.

[24] “CoinMarketCap.”https://coinmarketcap.com/.

[25] D. Quercia and S. Hailes, “Sybil attacks against mobile users: friends and foes to the rescue,” in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–5, IEEE, 2010.

[26] Wikipedia contributors, “Sybil attack — Wikipedia, the free encyclopedia,” 2018. [Online; accessed 25-June-2018].

[27] “Ipfs.”https://ipfs.io/.

[28] “Genaro.”https://genaro.network/en/.

부록 A. 증명

A.1 Proof of Property 1

proof. For any $x_1 > 0, x_2 > 0$, we have

$$\begin{aligned} f(x_1 + x_2) &= \frac{x_1 + x_2}{1 + e^{a+b\cdot(x_1+x_2)}} \\ &= \frac{x_1}{1 + e^{a+b\cdot(x_1+x_2)}} + \frac{x_2}{1 + e^{a+b\cdot(x_1+x_2)}} \\ &= \frac{x_1}{1 + e^{b\cdot x_2} \cdot e^{a+b\cdot x_1}} + \frac{x_2}{1 + e^{b\cdot x_1} \cdot e^{a+b\cdot x_2}} \end{aligned}$$

In formula 21, we have $b < 0$, so $0 < e^{(a+b)\cdot x_1} < 1, 0 < e^{b\cdot x_2 < 1}$, moreover,

$$\frac{x_1}{1 + e^{b\cdot x_2} \cdot e^{a+b\cdot x_1}} > \frac{x_1}{1 + e^{a+b\cdot x_1}} = f(x_1)$$

$$\frac{x_2}{1 + e^{b\cdot x_1} \cdot e^{a+b\cdot x_2}} > \frac{x_2}{1 + e^{a+b\cdot x_2}} = f(x_2)$$

is actually:

$$f(x_1 + x_2) > f(x_1) + f(x_2)$$

A.2 Proof of Property 2

proof. For any $x_1 > 0, x_2 > 0$, we have

$$\begin{aligned} f(x_1 + x_2) - f(x_1) - f(x_2) &= \frac{x_1 + x_2}{1 + e^{a+b\cdot(x_1+x_2)}} - \frac{x_1}{1 + e^{a+b\cdot x_1}} - \frac{x_2}{1 + e^{a+b\cdot x_2}} \\ &= \left(\frac{x_1}{1 + e^{b\cdot x_2} \cdot e^{a+b\cdot x_1}} - \frac{x_1}{1 + e^{a+b\cdot x_1}}\right) \\ &\quad + \left(\frac{x_2}{1 + e^{b\cdot x_1} \cdot e^{a+b\cdot x_2}} - \frac{x_2}{1 + e^{a+b\cdot x_2}}\right) \end{aligned} \tag{23}$$

Here we use function $g(x_1, x_2)$ represents the left part, $h(x_1, x_2)$ represents the right part:

$$g(x_1, x_2) = \frac{x_1}{1 + e^{b\cdot x_2} \cdot e^{a+b\cdot x_1}} - \frac{x_1}{1 + e^{a+b\cdot x_1}} \tag{24}$$

$$h(x_1, x_2) = \frac{x_2}{1 + e^{b \cdot x_1} \cdot e^{a+b \cdot x_2}} - \frac{x_2}{1 + e^{a+b \cdot x_2}} \tag{25}$$

So (23) for x_1 and x_2, their limits can be represented as:

$$\lim_{x_1 \to \infty, x_2 \to \infty} [f(x_1 + x_2) - f(x_1) - f(x_2)] = \lim_{x_1 \to \infty, x_2 \to \infty} g(x_1, x_2) + \lim_{x_1 \to \infty, x_2 \to \infty} h(x_1, x_2)$$

we have

$$\begin{aligned} g(x_1, x_2) &= \frac{x_1}{1 + e^{b \cdot x_2} \cdot e^{a+b \cdot x_1}} - \frac{x_1}{1 + e^{a+b \cdot x_1}} \\ &= \frac{x_1 \cdot e^{a+b \cdot x_1} \cdot (1 - e^{b \cdot x_2})}{(1 + e^{b \cdot x_2} \cdot e^{a+b \cdot x_1}) \cdot (1 + e^{a+b \cdot x_1})} \\ &< \frac{x_1 \cdot e^{a+b \cdot x_1} \cdot (1 + e^{a+b \cdot x_1})}{(1 + e^{b \cdot x_2} \cdot e^{a+b \cdot x_1}) \cdot (1 + e^{a+b \cdot x_1})} = \frac{x_1 \cdot e^{a+b \cdot x_1}}{1 + e^{b \cdot x_2} \cdot e^{a+b \cdot x_1}} \\ &< \frac{x_1 \cdot e^{a+b \cdot x_1}}{1 + e^{a+b \cdot x_1}} = \frac{x_1}{1 + \frac{1}{e^{a+b \cdot x_1}}} \end{aligned}$$

Calculate limit for $\frac{x}{1 + \frac{1}{e^{a+b \cdot x}}}$, according to L'Hospital's rule,

$$\begin{aligned} \lim_{x \to \infty} \frac{x}{1 + \frac{1}{e^{a+b \cdot x}}} &= \lim_{x \to \infty} \frac{1}{(e^{-a-b \cdot x})'} \\ &= \lim_{x \to \infty} \frac{1}{-b \cdot e^{-a-b \cdot x}} \end{aligned}$$

In formula 21, we have $b < 0$, so $\lim_{x \to \infty} -b \cdot e^{-a-b \cdot x} = \infty$, moreover,

$$\lim_{x \to \infty} \frac{x}{1 + \frac{1}{e^{a+b \cdot x}}} = 0$$

According to A.1, we have $g(x_1, x_2) > 0$, so according to sandwich theorem:

$$\lim_{x_1 \to \infty, x_2 \to \infty} g(x_1, x_2) = 0$$

Similarly, we can get:

$$\lim_{x_1 \to \infty, x_2 \to \infty} h(x_1, x_2) = 0$$

So,

$$\lim_{x_1 \to \infty, x_2 \to \infty} [f(x_1 + x_2) - f(x_1) - f(x_2)] = 0$$

부록 B. 변경 기록

- v1.0 발표
- v1.0.1 §4.3 내용안에 포함되는 속성 1과 속성 2의 수학적 서술을 수정
- v1.0.2 문법과 오타 수정