sui × SEIREN SQUAD

Sui 스마트 컨트랙트 플랫폼: 이코노믹스 & 인센티브

The Sui Smart Contracts Platform: Economics and Incentives

한국어 번역판

2022.12.27

sui × SEIREN SQUAD

백서 한글판 번역은 Seiren Squad 팀에서 진행하였으며, 그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.

Seiren Squad는 2018년 설립된 블록체인 연구기업 Numbers 프로젝트팀의 다른 이름입니다. Seiren Squad는 Sui가 그리는 생태계에 공감하고, 저희의 경험과 개발력이 그곳에 기여할 수 있기를 소망하며 개발에 매진하고 있습니다. 대한민국의 훌륭한 개발력을 가진 많은 프로젝트 팀과 함께 공감하기를 소망합니다. 번역 및 표현에 대한 의견이나 저희 팀에 대한 궁금하신 부분은 contact@serien.xyz으로 부탁드립니다.

Sui 스마트 계약 플랫폼: 경제와 인센티브

The Mysten Labs Team

econ@mystenlabs.com

1. 서론

Sui 스마트 계약 플랫폼은 환경 친화적이고, 가격대비 효율이 높으며, 대량신속처리(high-throughput)가 가능하고 저지연의 허가가 필요치 않은 블록체인이며, Sui의 역량은 기존의 블록체인 체계들의 최전방에 있는 선례들보다 월등히 앞서 있다고 말할 수 있다. 최근 테스트에 따르면 아직 최적화가 덜 된 8코어 맥북 프로 M1에서 실행되는 단일 작업자(single-worker) Sui의 밸리데이터(validator)는 초당 120,000개의 토큰 전송 트랜잭션 (TPS)[1]를 실행할 수 있으며, 이 성과는 광범위한 web3 어플리케이션에서 수십억 명의 사용자에게 서비스를 제공하는데 있어서 꼭 필요한 막대한 요구 사항을 충족시킬 수 있는 플랫폼의 탄생을 예고한다.

Sui의 최첨단 성능은 분산 시스템, 암호화 그리고 프로그램 언어 분야에서의 주요 기술 발전으로 가능 해졌으며, 비슷한 맥락으로 Sui economy 또한 블록체인 경제와 인센티브 연구의 최전방에서 설계되었다. 이 설계의 큰 틀에서의 목표는 Sui 생태계 내에 참가하는 다양한 객체들에게 인센티브를 부여하는 경제적 시스템을 구현하는 것이며, 작은 틀

[1] Sui의 테스트넷이 출시되면 전체 성능 보고서도 게시될 예정

에서의 목표로는 Sui의 통화 유통 방식(financial plumbing)이 Sui의 공학 설계와 같은 수준이 되도록 하여 Sui가 수십억의 참가자들에게 성장하는 경제를 선사할 수 있도록 하는 것이다. 본 토큰경제 연구지는 Sui economy의 핵심적인 요소들을 다룬다. 본 연구지를 읽기에 앞서, 독자들은 Sui의 기술적 디자인을 논하고 있는 <Sui Smart Contracts Platform> 백서 (https://sui.io/whitepaper)를 함께 열어 읽기를 권장한다.

Sui economy는 총 세 세트의 객체 (entities)들로 구성된다.

- 디지털 자산을 생산, 변형, 또는 이전하기 위해, 혹은 스마트 계약, 상호 운용성 및 구성 가능성으로 인해 더 발전된 어플리케이션을 활용하기 위해서 Sui 플랫폼에 트랜잭션을 제출하는 사용자들
- Sui의 고유 자산 (SUI라 칭하며 한정된 수량을 가짐)을 소유하는 소유자들. 이 소유자들은 보유 자산을 밸리데이터들에게 위임하고, proof-of-stake 메커니즘에 참여할 수 있는 권리를 가진다. 또한, SUI 소유자는 Sui의 거버넌스에 참여할 수 있는 권리를 가진다.
- Sui platform의 트랜잭션 진행과 실행을 관리하는 밸리데이터들

Sui economy는 네 가지 핵심 요소를 가진다.

- SUI 토큰은 Sui 플랫폼의 고유 자산이며, Sui economy에 온-체인 유동성을 제공한다.
- 모든 네트워크 운영에 가스 비용(gas fees)가 부과되며, 이는 proof-of-stake 메커니즘 참여자에 대한 보상에나 스팸 및 서비스 거부 공격을 방지하는데 사용된다.
- Proof-of-stake 메커니즘은 Sui 플랫폼의 운영진들 (밸리데이터 혹은 SUI 위임자)의 정직한 행동이란 무엇인지 선택하고, 정직하게 행동하도록 인센티브와 보상을 제공하는데 사용된다.
- 온-체인 거버넌스는 시간이 지남에 따라 Sui 프로토콜의 기능을 수정하고 개선하는데 사용된다.

Sui economy가 가지는 주요한 새로운 점은 Sui의 오브젝트(objects) 중심 설계의 직접적인

결과인 proof-of-stake 메커니즘의 구현이다. Sui 오브젝트는 FT/NFT를 포함하는 모든 유형의 자산을 인코딩하고 Sui의 글로벌 상태[2]를 결정할 수 있다. Sui에서 발생하는 트랜잭션은 오브젝트를 입력(input)으로 사용하고, 새 오브젝트를 출력(output)으로 선사한다.

오브젝트 중심 설계에 따라, Sui는 인과 관계 접근 방식을 사용하여 트랜잭션을 처리하고 실행한다. 간단히 요약하면, 두 트랜잭션의 오브젝트가 완전히 독립적일 경우 어떤 트랜잭션이 먼저 진행되는지가 중요하지 않다는 이야기가 된다. 실제로 동시에 트랜잭션이 입력되었을 때, 몇몇 밸리데이터들은 A라는 트랜잭션을 선행하고, 다른 밸리데이터들은 B라는 트랜잭션을 선행할 것이다[3]. 이러한 설계는 Sui가 비공유 오브젝트 (단일 주소가 소유한 오브젝트)의 트랜잭션 처리를 병렬화할 수 있기 때문에 효과적이다. 따라서, 각 밸리데이터는 자체적으로 스스로를 확장할 수 있으며, 더 많은 계산 성능을 추가하여 트랜잭션 처리량을 늘릴 수 있다. 이는 독립적인 데이터에 대한 네트워크 활동에 따라 처리량과 비용이 선형적으로 확장된다는 점에서 매우 효율적인 단위 경제 (unit economics)를 제공한다. Sui의 "멀티-레인" 디자인은 전체 주문에 의존하는 전통적인 블록체인 디자인과는 현저하게 대조되며, 여기서 전체 주문에 의존한다는 것은 모든 단일 트랜잭션들이 서로 관계성을 가지며 주문되는 것을 뜻하는데, 이에는 완전히 독자적인 트랜잭션 또한 포함된다.

Sui의 proof-of-stake 메커니즘은 인과적 순서 접근 방식 (causal-ordering approach)을 활용하여 각 트랜잭션을 처리하고 실행하려면 지분별로 밸리데이터의 2/3에 달하는 쿼럼을 필요로 한다. 밸리데이터는 들어오는 트랜잭션을 수신하고, 진위를 확인하며 서명을 사용자에게 전송함으로써 수동적으로 참여하게 된다. 따라서 Sui는 서로 다른 트랜잭션을 병렬로 처리하고 밸리데이터가 제출 직후에 바로 트랜잭션을 처리할 수 있도록 한다. Sui는 리더가 없고 모든 밸리데이터는 검사 및 실행에서 동등한 역할을 지니기 때문에, 모든 충실한 밸리데이터는 위임 지분에 따라 이익을 얻고 지분 보상을 받는다. 결과적으로, Sui

---

[2] Sui 오브젝트는 디지털 자산에만 국한되지 않고 다른 오브젝트를 만들고 관리하는데 사용되는 스마트 계약 및 Move 패키지를 인코딩할 수도 있다. 이 백서의 목적을 위해, 오브젝트는 디지털 자산과 동의어인 것처럼 취급된다. Sui 오브젝트에 대한 자세한 내용은 Sui 백서를 참조.

[3] 그러나 인과적 순서는 어느 정도의 순서가 필요하긴 하다. 예를 들어, 트랜잭션 B가 트랜잭션 A의 출력 오브젝트를 입력으로 사용하는 경우, 트랜잭션 B는 반드시 트랜잭션 A를 따라야 한다. 오브젝트가 여러 주소에서 소유되는 공유 오브젝트의 경우에도 순서 지정이 중요하다.

는 계산에 있어 낭비가 없으며, 더 높은 지분의 밸리데이터가 프로토콜 보상을 얻을 확률이 더 높은 다른 proof-of-stake 구현에 존재하는 “부자가 더 부자가 되는” (“rich-get-richer”) 현상을 피한다.

Sui의 가스비 책정 (gas pricing) 메커니즘은 사용자에게 낮고 예측 가능한 트랜잭션 수수료를 제공하고 밸리데이터에게 트랜잭션 처리 작업을 최적화하도록 장려하며 서비스 거부 공격을 방지하는 세 가지 결과를 담당한다. 여기서 중요한 것은 Sui의 가스비 책정 메커니즘만의 특징 중 하나는 Sui 사용자가 실행 및 저장에 대해 별도의 비용을 지불해야 한다는 것이다. 실행 또는 계산에 대한 가스비는 Sui epoch들에 걸쳐 반복적으로 작동하는 3단계 프로세스를 통해 결정된다 (시간은 각각 약 24시간 정도 지속되는 연속적인 기간들로 나뉜다).

1. 가스비 관련 설문이 밸리데이터에게 epoch 시작 시 예약 가격, 즉 거래를 처리할 의향이 있는 최소 가스 가격을 제출하도록 한다. 프로토콜은 지분의 2/3 백분위수를 epoch 기준 가스 가격으로 설정한다.
2. 사용자가 트랜잭션을 제출하고 밸리데이터가 이를 처리하는 epoch이 진행됨에 따라, 밸리데이터는 다른 밸리데이터의 작업에 대한 신호를 얻게 된다.
3. Epoch 종료 시 각 밸리데이터는 다른 모든 밸리데이터의 행동에 대한 주관적인 평가를 제출하고, 이 평가는 지분 보상 분배 규칙에 대한 입력으로 사용된다. 가스비 조사 중 낮은 가격 견적, 즉, 기준 가격보다 낮은 가격을 제출하거나 자체 선언된 예약 가격보다 높은 모든 트랜잭션을 처리한 밸리데이터는 즉시 보상을 받게 된다. 반대로, 가스비 조사 중 높은 가격 견적을 제출하거나 자체 선언한 예약 가격을 지키지 않는 밸리데이터는 보다 낮은 보상을 받는 불이익을 지게 된다.

Sui의 가스비 책정 메커니즘은 최종 사용자들에게는 훌륭한 유저 경험을 선사하며, 밸리데이터들에게는 더 지속 가능한 비즈니스 모델을 운용할 수 있게끔 인센티브를 제공한다. 사용자 측면에서 보면, Sui는 가스비가 참고용 가스 가격보다 높거나 낮아야 함을 사용자들에게 요구하지는 않는다. 실제로 사용자는 가스비를 자유롭게 제출할 수 있다. 그러나, 가스비 책정 메커니즘은 밸리데이터가 실제 예약 가스비를 도출하고 그러한 가격을 존중할 수 있게끔 인센티브를 제공하도록 설계되어 있다. 결과적으로 Sui 사용자는 기준 가격에 가깝거나, 기준 가스비에 맞게 제출된 트랜잭션이 즉시 처리될 것으로 기대할 수 있다. 따라서 Sui 사용자는 현재 가스비를 예측해야 하고 예측 실패에 따른 초과 비용을

부담해야하는 비효율적인 상황을 피할 수 있게 된다. 밸리데이터 측면에서는, 밸리데이터는 항상 건전한 총 마진으로 운영할 수 있어야 하는데, 이는 밸리데이터의 쿼럼은 기준 가스비를 집합적으로 결정하기 때문이다. 또한, 가장 효율적인 밸리데이터는 더 높은 보상을 받기 때문에, Sui의 가스 메커니즘은 가격 설정시 카르텔 같은 행동을 피하기 위한 인센티브 또한 포함된다. 요컨대, Sui의 가스비 메커니즘은 공정한 가격에 대한 건전한 경쟁을 지향시킨다. 밸리데이터들은 가스 가격을 낮출 수는 있으나, 너무 낮게는 책정할 수 없다. 해당 가격에 트랜잭션을 진행하지 못할 시에는 불이익을 받기 때문이다.

Sui의 가스비 메커니즘은 Sui 사용자들에게 중요한 모니터링 역할을 부여한다. 사용자는 한편으로 트랜잭션이 최대한 빠르고 효율적으로 처리되기를 원한다. 지갑 (wallet)같은 사용자 클라이언트는 가장 반응이 빠른 밸리데이터와의 소통을 우선시하여 이를 권장한다. 이런 효율적인 작업은 반응이 빠른 밸리데이터에게 상대적으로 느린 밸리데이터에 비해 향상된 보상을 줌으로써 보상한다. 반면에, SUI 토큰 위임자들은 위임 밸리데이터와 동일한 향상 혹은 페널티 보상을 받게 되는데, 이에 따라 반응이 느린 밸리데이터는 가스비 책정 메커니즘에 의해 이중으로 손해를 보게 된다. 반응이 느린 밸리데이터는 더 적은 보상을 통해 직접적인 손해를 보고, 스테이커가 다소 더 빠른 반응의 밸리데이터에게 토큰을 이전함에 따라 추후 epoch에서 위임될 지분이 줄어들어 간접적으로도 손해를 보게 된다.

Sui는 데이터 스토리지 가격 책정을 위한 효율적이고 지속 가능한 경제 메커니즘 또한 포함한다. Sui의 높은 처리량과 낮은 대기시간 기저에 있는 Sui의 핵심 기능은 임의의 양의 온-체인 데이터를 처리하는 능력이다. 재정적으로는, 이 기능은 심각한 시간간 (intertemporal) 문제를 야기할 수 있다. 예컨대, 현재 데이터를 처리하고 이를 저장(Storage)하는 밸리데이터는 미래의 밸리데이터와는 다를 수 있다. 사용자가 쓰기 (write)시 계산 능력에 대한 요금만 지불한다면, 미래의 사용자는 스토리지에 대해 과거 사용자에게 보조금을 지급하고 불균형적으로 높은 요금을 지불해야될 수도 있다. 이러한 부정적인 네트워크 외부성은 해결되지 않은 상태로 유지된다면 장기적으로 Sui에게 상당한 부담을 안길 수 있다.

따라서, Sui의 economy 설계에는 과거 트랜잭션 수수료를 미래 밸리데이터에게 재분배하는 스토리지 펀드가 포함되어 있다. 간단히 말해서 사용자는 계산 및 스토리지에 대한 비용을 선불로 지불해야 한다. 스토리지 수수료는 스토리지 펀드에 예치되는데, 이는

SUI 위임자에 대비한 밸리데이터에게 분배되는 지분 보상 몫을 조정하는데 사용된다. 온-체인 스토리지 요구사항이 높을 때, 밸리데이터는 그에 투입되는 비용에 대한 보상으로 상당한 추가 보상을 받게 된다. 스토리지 요구 사항이 낮을 때는 그 반대다. 여기서 중요한 것은 스토리지 펀드는 절대 원금에서 직접 보상을 분배하지 않으므로 장기적으로 유지가 가능하며 스토리지 비용을 무한정 지원할 수 있는 경제 메커니즘을 제공한다는 것이다.

스토리지 펀드는 Sui economy에 다양하며 바람직한 인센티브를 도입한다. 첫째, 사용자가 이전에 저장된 온-체인 데이터를 삭제할 때마다 해당 스토리지에 대한 수수료 리베이트를 받는 "삭제 옵션"이 포함되어 있다[4]. 이는 스토리지가 재정적으로 사용자에게 더 이상 유리하지 않을 때, 사용자가 스스로 데이터를 삭제하는 쓰로틀 메커니즘을 도입한다. 둘째, Sui 스토리지 펀드는 SUI로 통용되기 때문에, Sui 내에서의 경제 활동이 증가하면 스토리지 요구 사항이 더 높아지고, 더 많은 SUI가 통화 순환에서 제거된다. 따라서, 스토리지는 일석이조의 효과를 얻는다. 즉, 재정적으로 지속 가능한 스토리지 모델을 제공할 뿐만 아니라 SUI에 디플레이션 압력을 가해 네트워크 소유자와 사용자에게 혜택을 준다. 셋째, 스토리지 펀드는 사용자가 기간당 지불 모델을 통해 수수료를 지불하는 임대 모델과 경제적으로 같다는 점에서 자본 효율적이다. 그러나 스토리지 펀드는 많은 사용자가 각 기간마다 개별적으로 임대료를 지불하는 임대 모델을 설정하는 데 발생하는 엄청난 복잡성에 기댈 필요가 없기 때문에 임대 모델에 비해 더 깔끔하다.

본 Sui economics 백서는 다음과 같은 구조를 가진다. Section 2는 Sui 플랫폼의 주요 프리미티브와 작동을 설명하는 것으로 시작하며, Section 3에서는 Sui economy의 주요 구성 요소를 소개하고 Sui의 proof-of-stake economic 모델에 대한 개요를 제공한다. Section 4와 5는 각각 Sui의 가스비 메커니즘과 스토리지 펀드에 대한 설계와 인센티브에 대한 조금 더 자세한 설명을 탐구하며, Section 6에서는 Sui economic 모델의 장기적인 역동성을 논의한다. 마지막 Section 7에서는 몇몇 결론적인 내용이 포함되며, 부록은 모델의 자유 매개변수 요약을 담고 있다.

---

[4] 이를 과거 트랜잭션 삭제와 혼동해선 안된다. Sui의 활동은 각 epoch 경계에서 완료되므로, 과거 트랜잭션은 변경할 수 없으며 되돌릴 수도 없다. 삭제할 수 있는 데이터의 유형은 예를들어 NFT의 메타데이터, 교환된 티켓, 완료된 경매 등과 같이 더 이상 라이브 상태가 아닌 오브젝트에 해당되는 데이터이다.

2. Sui 플랫폼 시초 (始初)

2.1 SUI 토큰

Sui 플랫폼의 고유 자산은 SUI라고 불리우며, 해당 백서에서는 Sui와 대조하여 부르기 위해 SUI를 모두 대문자처리 하여 나타내기로 한다.

Sui 플랫폼은 시간을 e =0, 1, 2... 시간 서브스크립트로 인덱싱하는 순차적인 epoch으로 나눈다. epoch e에서의 총 SUI 공급량은 M_e라고 하며, SUI 토큰의 통화적 규칙은 공급이 시간이 지나도 줄어들지 않는다는 데 있다. 예컨대, SUI 토큰은 소각되지 않으며 모든 e에 대해 $M_e \leq M_e+1$이 된다. 장기 SUI 공급량은 $\lim e \to \infty M_e$= 10,000,000,000 토큰으로 제한된다[5]. 해당 백서에서는 e =0 를 초창기 epoch (genesis epoch)으로 참조할 것이며, 이 시점에서 SUI 토큰의 '0이 아닌 최소 값' (non-zero amount) M0>0은 민팅된다.

SUI 토큰은 Sui 플랫폼에서 네 가지 용도로 사용된다. 첫째, SUI 토큰은 proof-of-stake 메커니즘에 참여하기 위해 epoch 내에서 스테이킹 될 수 있다. 둘째, SUI 토큰은 Sui 플랫폼에서 트랜잭션 또는 기타 작업을 실행하기 위해 가스비를 지불하는 데 필요한 자산 액면가이다. 셋째, SUI는 계정 단위, 교환 매체 또는 가치 저장 따위의 화폐 표준 기능과 스마트 계약, 상호 운용성, Sui 생태계 전반에 걸친 구성 가능성을 통해 구현되는 보다 복잡한 기능을 포함한 다양한 어플리케이션을 위한 유연하고 유동적인 자산으로 사용될 수 있다. 마지막으로, SUI 토큰은 프로토콜 업그레이드 등과 같은 문제에서 온-체인 투표에 참여할 수 있는 권리로 작용하여 거버넌스에서 중요한 역할을 한다.

2.2 Sui 목표와 트랜잭션

Sui 플랫폼은 오브젝트를 주요 구성 요소로서 사용한다. Sui 오브젝트들은 FT 및 NFT를 포함하는 모든 유형의 디지털 자산을 나타낼 수 있다. 본 백서에서는 오브젝트 생성, 변형 또는 전송과 같은 Sui 플랫폼에서의 작업을 트랜잭션이라고 부른다. 일반 트랜잭션은 오브젝트를 입력으로 사용하고, 입력에 대해 지정된 명령 집합을 작동시키며 후속 오브

[5] Sui 프로토콜에는 명시적으로 토큰을 소각하는 메커니즘이 포함되어 있지 않지만, 실제로 다양한 작용들이 소각 토큰과 유사한 디플레이션 효과를 가진다 (섹션 6.1). 각 SUI 토큰은 최대 소수 자릿수까지 나눌 수 있다.

젝트를 출력으로 생성한다.

공유되지 않는 오브젝트 (Non-shared objects) 즉, 단일 주소가 소유하는 오브젝트에는 총 세가지 중요한 특성이 있다. 첫째, 모든 오브젝트는 "주소" 영역을 포함하여 단일 소유권으로 연결된다. 둘째, 오브젝트는 트랜잭션에서만 사용할 수 있지만, 소유 주소의 서명으로 인증된 경우에만 사용 가능하다. 셋째, 오브젝트에는 해당 오브젝트를 출력으로 가진 트랜잭션을 나타내는 다이제스트가 포함된다.

트랜잭션에서 아직 입력으로 사용되지 않은 오브젝트 집합을 "라이브 오브젝트" 집합이라고 하는데, Sui 플랫폼의 프로그래밍 언어는 비활성 오브젝트 (즉, 이전 트랜잭션에서 이미 입력으로 사용된 오브젝트)를 추후 트랜잭션에서 다시 사용하지 못하도록 구축되어 있다. 결과적으로, 모든 epoch에 걸친 전체 오브젝트 및 트랜잭션 집합은 시간에 따른 Sui 상태의 진화를 나타내는 방향성 비순환 그래프 (DAG/Directed acyclical graph)를 구성하는데 사용될 수 있다. 이 DAG에서 오브젝트는 꼭짓점에, 트랜잭션은 가장자리에 해당하며, 라이브 개체 집합은 그래프 상 가장자리가 더 이상 없는 꼭짓점 (childless vertices)과 트랜잭션의 출력보다 나가는 가장자리가 적은 꼭짓점에 해당한다.

오브젝트가 Sui 플랫폼의 핵심 요소를 나타내기는 하지만, Sui의 economy는 트랜잭션이라는 수단을 통해서 접근할 때 가장 잘 이해된다. 이러한 이유로 일반 트랜잭션을 뜻하며, 오브젝트를 명시적으로 모델링하지 않도록 표기법 τ를 사용한다. 그러나, 독자는 모든 트랜잭션 τ가 개체 입력, 출력 및 작업 목록과 관련 있음을 명심해야 한다.

2.3 스테이킹

Sui 플랫폼은 트랜잭션을 처리하는 밸리데이터 집합을 결정하기 위해 위임된 proof-of-stake를 사용한다. 각 epoch e 내에서, 작업은 지분의 양 $S_e(v)$에 참가하는 각 밸리데이터 $v \in V_e$인 일련의 밸리데이터 집합인 V_e에 의해 처리된다. 지분의 양은 각 밸리데이터가 트랜잭션을 처리하는 데 필요한 투표권의 몫을 결정한다는 점에서 중요성을 가진다. 밸리데이터와 위임된 지분 $C_e=(V_e,S_e(\cdot))$을 위원회 (committee)라고 부르고 총 위임 지분 $S_e = \sum_{v\in V_e} S_e(v)$을 나타낸다. 밸리데이터의 지분 몫을 $\sigma_e(v) = S_e(v) / S_e$로 정의하는 것이 도움이 될 것이며, 구성에 의해 다음 조건이 유지된다: 모든 epoch e에 대해 $S_e \leq M_e$ and $\sum_{v\in V_e} \sigma_e(v) = 1$.

Sui 플랫폼은 SUI 토큰 소유자가 보유 자산의 전체 혹은 일부를 특정 밸리데이터에게 위임하고 해당 밸리데이터가 얻은 스테이킹 보상에 참여할 수 있도록 위임을 구현했다. SUI 토큰 보유자가 SUI를 위임하게 되면, SUI 토큰은 전체 epoch 동안 해당 위임자가 선택한 밸리데이터에게 고정적으로 잠금된다.

SUI 토큰 보유자는 epoch이 변경될 때 SUI를 잠금 해제하거나 다른 밸리데이터에게 위임할 수 있다. 이러한 위임 변경의 결과로 위원회는 epoch 경계에서 라이브 밸리데이터 집합과 잠재적으로 변경될 수 있는 관리 지분 분배 둘 모두와 함께 여러 epoch에 걸쳐 진화된다. 즉, 두 epoch e와 e+1 사이에서 $v \in Ve$, Ve+1에 대하여 $Ve \neq Ve+1$와 $Se(v) \neq Se+1(v)$가 모두 일반적으로 참이 된다는 것을 뜻한다. Sui의 운영 작업에서 얻은 보상은 epoch이 종료될 때 밸리데이터 및 SUI 위임자를 포함한 다양한 객체(entities)에 분배된다. 본 백서의 다음 섹션은 사용자, 클라이언트, 밸리데이터가 Sui 플랫폼에서 트랜잭션을 제출, 처리 및 기록하는 절차에 대해 다룰 것이다.

2.4 시스템 운영

Sui의 운영은 지분에 의해 가중된 밸리데이터의 1/3 미만이 비잔틴인 (Byzantine Protocol/Sui 백서 참조) 경우, 즉 프로토콜에서 임의로 벗어나는 한 안전하다. Sui에서 트랜잭션을 처리하려면 두 큰 틀에서의 단계가 필요하다.

1. 첫 번째 단계에서는, 사용자는 개인 키로 트랜잭션 τ에 암호화된 서명을 하고 현재 epoch의 밸리데이터 집합 Ve로 보낸다. 각 밸리데이터는 트랜잭션을 검증하고, 이 트랜잭션이 성공했을 시에는 자신의 개인 키로 트랜잭션에 서명하고, 이 서명된 트랜잭션을 다시 사용자에게 보낸다.
2. 두 번째 단계는 지분에 따른 밸리데이터 수의 최소 2/3의 서명을 받은 후에 발생한다. 수식으로는 이는 사용자가 쿼럼 $Qe \subset Ve$으로부터 $\sum v \in Qe\ \sigma e\ (v) \geq 2/3$의 서명을 받은 후에 발생한다고 할 수 있다. 그런 다음 이러한 응답들은 수집되어 트랜잭션 인증서를 형성하는데 사용된다. 이 인증서는 서명을 확인하고 트랜잭션을 실행하는 검증자에게 전송된다. 밸리데이터 쿼럼이 해당 인증서를 실행하면 해당 단계는 최종 완성된다.

사용자는 밸리데이터 집합의 검증을 위해서 트랜잭션을 제출하는 과정의 맨 처음에만 트랜잭션에 암호로 서명하기만 하면 된다. 따라서, 실제로 후속 프로세스는 사용자가 직접 수행할 필요가 없으며, 제3자 클라이언트 혹은 게이트웨이 서비스에서 관리할 수 있다.

Sui 트랜잭션 흐름의 주요 경제적 이점은 이 흐름을 병렬화할 수 있다는 것이다. 예컨대, 변경 가능한 입력 오브젝트의 두 집합이 분리되도록 두 개의 트랜잭션 τ 그리고 τ′를 가정하면, 위의 두 단계가 τ와 τ′에 대해 동시에 처리될 수 있음을 알 수 있다. 이를 동시에 처리하기 위해 필요한 유일한 조건은 각 밸리데이터가 각 트랜잭션을 처리하기 위해 별도의 리소스를 할당해야 된다는 것이다. 수천 혹은 수백만개의 동시 트랜잭션을 처리해야 되는 경우에도 해당 병렬화가 (일반성을 잃지 않는 선에서) 적용된다. 트랜잭션을 병렬화하는 기능은 Sui의 오브젝트-중심의 설계에서 비롯되며, 이는 프로토콜이 어떤 트랜잭션을 어떤 방식으로 병렬화 할 수 있는지 추적하는 것을 쉽게 만든다.

따라서 Sui 플랫폼은 각 밸리데이터에 더 많은 컴퓨팅 성능을 추가하여 처리량을 선형적으로 확장시키는 동시에 비용 또한 선형적으로 증가시킨다. 이는 네트워크 리소스에 대한 총 수요에 관계없이 빠르고 저렴하며 가격 대비 효율이 높은 플랫폼을 제공한다. 보다 일반적인 상황에서는, τ와 τ′이 동일한 입력 오브젝트를 사용하는 공유 오브젝트(shared objects)의 경우는 조금 더 복잡해질 수 있다. 공유 오브젝트는 모든 트랜잭션이 완전히 병렬화 될 수 없으며, 밸리데이터가 공유 오브젝트의 현재 상태에 동의하기 위해 합의 프로토콜을 실행해야 됨을 의미한다. 이러한 경우들에서, 공유 오브젝트가 인과 종속성(causal dependencies)을 생성하는 동안, 다른 비인과 종속 공유 오브젝트들(non-casually-dependent shared objects)은 병렬화될 수 있다는 점을 유의할 시에 어느 정도의 병렬화는 여전히 가능하다. 상기된 더 가벼운 병렬화(lighter parallelization)와 함께 Sui 플랫폼은 공유 오브젝트를 처리하는 데 있어 더 높은 처리량의 DAG 기반 합의 메커니즘을 통해 합의점을 얻는다. 이 기술의 세부 사항은 Sui 백서에서 참조 가능하다.

3. Sui Economy: 기본 구성 요소

본 백서는 이제 Sui 플랫폼의 단일 epoch 혹은 여러 epoch에 걸친 경제성에 대해서 논할 것이다. 이 논의의 목적을 위해서, 본 백서는 네트워크 경제 및 인센티브와 덜 관련이 있는 공학적 디테일을 조금 완화시키기로 한다.

Sui 플랫폼은 운영자들에게 인센티브를 제공하기 위해 보상을 생성하고, 이러한 SUI 토큰을 네트워크 참여자에게 배포한다. 이 프로세스는 총 세 단계로 나뉘어진다. 먼저, 가스비를 통해 보상을 생성하는 플랫폼의 기능을 설명하고, 둘째, Sui 스토리지 펀드를 소개하며 Sui가 그를 통해 여러 epoch에 걸쳐서 보상을 전환할 수 있는 방법을 설명하며, 마지막으로 주어진 epoch 내에서 보상을 분배하기 위한 플랫폼의 경제학적 모델을 검토한다.

3.1 가스비

Sui 플랫폼은 사용자들에게 가스비를 청구함으로써 보상액을 만들어낸다[6]. τ를 Sui에 대한 임의의 트랜잭션 (예: 오브젝트 생성, 변형, 전송 혹은 삭제)로 할 시, epoch e 동안 트랜잭션 τ 처리와 관련된 가스비는 다음 공식으로 나타낼 수 있다:

$$\mathrm{GasFees}_e[\tau] = \underbrace{\mathrm{ComputationUnits}_e[\tau] \times P_e^C[\tau]}_{\text{computation fees in SUI}} + \underbrace{\mathrm{StorageUnits}_e[\tau] \times P_e^S}_{\text{storage fees in SUI}}. \qquad (1)$$

공식 (1)

가스는 ComputationUnitse[t]를 함수화하고, StorageUnitse[t]는 각각 τ와 관련된 데이터를 처리하고 저장하는 데 필요한 계산과 스토리지 자원에 대한 양을 가늠한다. 본문에서는 프로토콜 업그레이드, 소프트웨어 및 하드웨어의 개선 및 기타 요인으로 인해 계산 및 저장 비용이 epoch에 따라 변할 수 있으므로, 가스 함수를 시간 섭스크립트로 인덱싱한다. 그러나, 한 epoch 내에서 가스 함수는 결정론적이며 모든 네트워크 참여자들에게 공통적이다. 가스 가격 PCe[t] 및 PSe는 각각 계산 또는 스토리지의 한 단위의 비용을 SUI 단위로 책정한다. 계산 및 스토리지 비용은 모두 청구되며, SUI 토큰으로 지불되어야 한다. 중요한 점은, 계산에 대한 가스비는 epoch 내 혹은 전체 epoch에서 트랜잭션마다 유동적일 수 있는 반면에, 스토리지 가스비는 epoch 내에서 일정하나, epoch 전체로 보

[6] 가스비는 네트워크 사용에 0이 아닌 비용을 도입해서 스팸을 억제하는 추가 이점도 있다.

면 다를 수 있다는 점이다.

실제로 Sui 플랫폼의 일반 사용자는 법정 화폐를 표준 계정 단위로 사용하게 된다. 이는 대부분의 사용자에게 중요한 것은 가스의 SUI 가치가 아니라 달러 가치임을 의미한다. P$e를 epoch e 시작 지점의 SUI 토큰 달러 가격이라고 할 때, 트랜잭션 처리 비용 τ는 다음과 같다:

$$\begin{aligned}\text{GasFees}_e^{\$}[\tau] &= \text{GasFees}_e[\tau] \times P_e^{\$}, \\ &= \underbrace{\text{ComputationUnits}_e[\tau] \times P_e^{C}[\tau] \times P_e^{\$}}_{\text{computation fees in \$}} + \underbrace{\text{StorageUnits}_e[\tau] \times P_e^{S} \times P_e^{\$}}_{\text{storage fees in \$}}.\end{aligned}$$

Sui economy는 가스비를 달러 기준으로 낮게 유지하도록 설계되어 있다. 위에서 논의된 바와 같이, 가스 함수 ComputationUnitse[t]와 Storageunitse[t]는 기술적 제약에 의해 결정되는 반면, SUI의 달러 가격 P$e는 시장 요인에 의해 결정된다. 따라서, GasFee$e[t]의 유일한 자유도는 가스비 PCe[t] 및 PSe에 있다. 이에 따라, 가스비를 달러 기준으로 낮게 유지하려면 가스비가 SUI의 달러 가격과 함께 경기 역행적으로 움직여야 한다. P$e가 높을 때, PCe[t]와 PSe는 낮아야 한다. P$e가 낮을 때는 그 반대의 경우가 된다. Sui economy는 시장 기반 인센티브를 통합하여 제품 PCe[t] x P$e 및 PSe x P$e를 거의 낮고 일정하게 유지함으로써 상기 공식을 달성할 수 있다. 이 속성을 달성하는 가스비 메커니즘은 섹션 4에 상세히 설명되어 있다.

3.2 Sui 스토리지 펀드

Sui 플랫폼은 잠재적으로 임의의 양의 온-체인 데이터를 저장하는 동안에도 높은 처리량과 낮은 대기 시간을 제공할 수 있도록 최적화 되어있다. 이는 경제적인 관점에서 중요한 어려움을 발생시킨다. 이는 Sui 네트워크는 트랜잭션을 처리하고 실행하기 위해서 밸리데이터에 의존하여 작동하지만, 이러한 서비스를 제공하려면 과거 트랜잭션과 관련된 데이터를 보유하고 있어야 한다.

여기서 말하는 경제적 어려움이란, 사용자가 계산에 대한 가스비만 지불하는 경우에 밸리데이터는 현재 계산의 가스비로 현재 작업과 스토리지 오버헤드 모두에 자금을 지원해야 된다는 것이다. 이는 현재의 사용자가 미래의 밸리데이터들에게 부과하는 스토리지

비용을 포함하지 않기 때문에 시스템에 대한 세금으로 이해될 수 있다. 이는 밸리데이터 집합 Ve가 시간이 지남에 따라 변경된다는 사실로 인해 더욱 복잡해지며, 이는 미래에 밸리데이터들이 어차피 보상을 받지 못했을 수도 있는 과거 트랜잭션들의 데이터까지 저장해야 함을 의미한다. 미래의 밸리데이터들은 생존을 위해 실행 가능한 비즈니스 모델이 필요하므로, 향후 계산 비용은 스토리지 비용을 상회해야 한다. 즉, 미래의 사용자들은 과거의 사용자들에게 보조금을 지급해야 하며, 이는 비효율적인 경제적 결과이다.

Sui의 economic 모델은 사용자에게 스토리지 비용을 선불로 청구하여 스토리지 문제를 해결한다. 트랜잭션 τ를 제출하는 사용자는 현재 실행과 향후 스토리지에 대해 모두 지불해야 하며, 실제로 이러한 모델을 지속 가능한 방식으로 운영하는 것은 그 자체로 굉장히 복잡한 소요를 탄생시킨다. 그 이유를 알기 위해서는, 스토리지 비용은 데이터를 영원히 저장해야 될 수도 있기에 잠재적으로 무한한 반면, 스토리지 요금을 청구하는 것은 유한한 SUI 토큰을 제공한다는 점을 주목해야 한다. 또한, 스토리지 비용 자체도 변동성이 크며 예측하기 어렵다. 양 극단의 한 쪽의 해결책은 한정된 시간 내 스토리지에 대한 선불 요금을 청구하고, 만료 시 사용자가 스토리지 요금을 갱신하지 않을 때 시스템에서 자동으로 데이터를 삭제하는 것이다. 다른 쪽의 해결책은 스토리지 비용을 무한으로 충당할 수 있는 스토리지 요금 모델을 설계하는 것이다. 본 백서는 후자의 접근 방식이 사용자 경험과 플랫폼의 전반적인 경제 모델에 다소 낫다는 의견 쪽으로 기운다.

Sui의 economic 모델에는 스토리지 비용에 대해 밸리데이터 보상을 위해 지속 가능하고 실행 가능한 장기 메커니즘을 제공하도록 설계된 스토리지 펀드가 포함되어 있다. 핵심은 스토리지 펀드는 밸리데이터에게 지급되는 스테이킹 보상을 조정하는 데 사용되기 때문에, 밸리데이터는 스토리지 비용을 상쇄하는 데 도움이 되는 추가 보상 소스를 얻을 수 있다는 것이다.

스토리지 펀드는 총 세 가지 주요 기능이 있다. 첫째, 스토리지 펀드는 과거 트랜잭션으로 자금을 조달한다. 이는 향후 밸리데이터가 해당 스토리지 요구사항을 처음 생성한 과거 사용자로부터 스토리지 비용을 보상받게 한다. 즉, 스토리지 펀드는 서로 다른 epoch에 걸쳐 지분 보상을 이동시키기 위한 도구를 제공한다. 둘째, 스토리지 펀드는 SUI 예치금에서 발생한 지분 보상을 통해 간접적으로 토큰을 분배하지만, 실제로 예치금을 직접 지불하지는 않는다. 이렇게 할 시에 펀드의 자본금이 유지되며 무한정 생존할 수 있음을

알 수 있다. 셋째, 스토리지 펀드의 메커니즘은 사용자가 데이터를 삭제하고 해당 데이터를 저장하는 비용이 해당 데이터를 체인에 유지함으로써 얻은 가치를 초과할 때, 스토리지 요금에 대한 리베이트를 얻도록 독려한다. 따라서, 이 설계는 기존 스토리지를 보상하기 위해 보상을 분배하고, 경제적 관점에서 스토리지가 더 이상 매력적인 옵션이 아닐 때 스토리지를 제거하는 시장 기반 메커니즘을 포함하기 때문에 효율적이라고 할 수 있다.

높은 수준에서 스토리지 펀드의 메커니즘은 아래와 같다 (자세한 내용은 섹션 5 참조). 스토리지 펀드의 크기는 epoch 기간 내내 고정되며, epoch이 변경되는 경계에서 조정된다. 유입은 펀드가 자본 수익의 일부를 새로운 원금에 재투자하는 것, 그리고 해당 epoch의 가스비에 해당한다. 유출은 데이터를 삭제한 사용자에게 발생한 리베이트에 해당되며, 공식적으로 e 와 e+1의 epoch 경계에서 스토리지 펀드는 다음과 같은 공식으로 제공된다:

$$\mathbf{F}_{e+1} = \mathbf{F}_e + \underbrace{\text{Reinvestment}_e + \sum_{\tau \in T_e} \text{StorageUnits}_e[\tau] \times P_e^S}_{\text{inflows}} - \underbrace{\sum_{\tau \in R_e} \text{Rebates}_e[\tau]}_{\text{outflows}}, \quad (2)$$

공식 (2)

여기서 Te는 e 전체에 걸쳐 처리된 트랜잭션 집합이며, Re는 e 또는 그 이전부터 데이터가 epoch e 전체에 걸쳐 제거된 과거 트랜잭션 집합이며, 리베이트e[t]는 t와 관련된 데이터를 삭제한 사용자가 적립한 리베이트를 나타내는 함수이다. 스토리지 펀드는 SUI 단위로 표시되었다.

3.3 Proof-of-stake와 스토리지가 있는 Economic 모델

본 섹션은 Sui의 economic 모델을 소개하기 위해 위의 요소들이 어떤 상호 작용을 가지는지 논의한다. 이 섹션 전체에서 논의를 돕기 위해서 그림1의 시각적 표현이 사용될 것이며, Sui의 economic 모델과 전통적인 지분증명 시스템 사이에는 두 가지 중요한 차이점이 있다.

첫째, 시스템 운영에 참여하는 객체는 일부 대체 모델의 변동성 있는 보상 스트림(volatile reward stream)과는 달리, 시간이 지남에 따라 원활한 보상 소스를 얻을 수 있을

것으로 기대할 수 있다. 이는 Sui 밸리데이터가 다른 곳에서 수행하는 능동적인 역할과는 다른, 수동적인 역할을 수행한 결과이다. 각 트랜잭션을 처리하려면 밸리데이터 쿼럼이 참여해야 하기 때문에, 모든 밸리데이터가 정직하게 행동한다면 모든 epoch동안 총 지분에 비례하는 이득을 얻을 수 있다. 이는 주어진 시간에 보상을 받을 확률이 지분 비율에 비례하는 다른 보상 시스템과는 대조되는 것이며, 이 기능은 시간이 지남에 따라 밸리데이터 전체의 스테이크 배포 진화에 중요한 의미를 갖는다 (섹션 6.3 참조). 이러한 설계는 각 밸리데이터가 제공하는 서비스 품질에도 중요한 영향을 미친다.

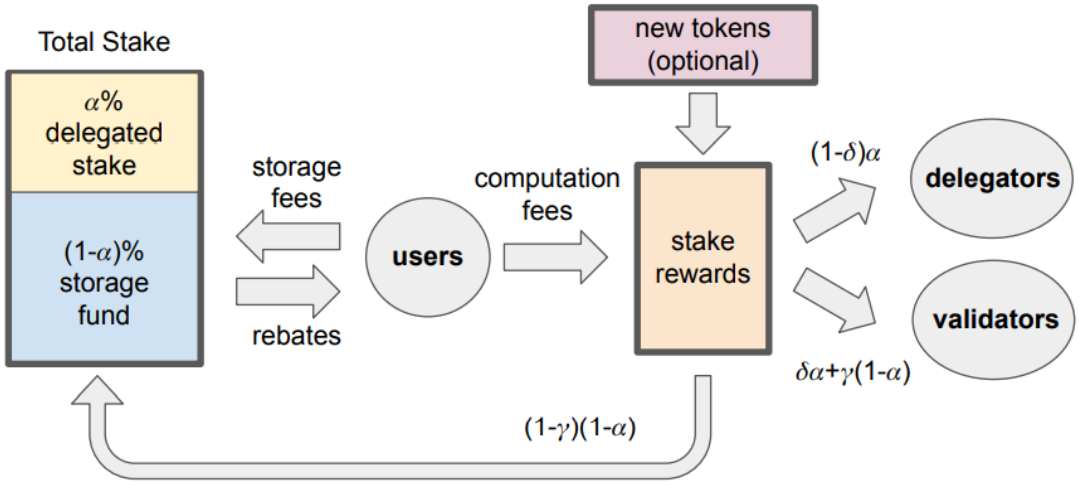

그림 1.

더 큰 지분 점유율을 가지는 밸리데이터는 더 많은 지분 보상을 얻을 수 있지만, 그러한 밸리데이터들은 정기적인 네트워크 운영 중에 고객에 의해 우선 순위로 지정될 가능성도 높아진다. 결과적으로, 더 큰 보상은 확장 작업 비용 증가로 부분적으로 상쇄되며 이에 따라 모든 밸리데이터가 그들에게 위임된 지분 규모와는 무관하게 비즈니스 모델을 누릴 수 있다.

둘째, Sui 스토리지 펀드의 존재는 보상을 epoch에 걸쳐 이동할 수 있는 능력을 제공하며, 이는 스토리지 펀드의 존재를 설명하기 위해서 proof-of-stake 메커니즘을 조정해야 함을 내포한다. 스토리지 펀드에서 발생하는 추가 인센티브를 수용하면서 proof-of-stake 메커니즘을 통해 발생하는 인센티브를 보존하기 위해 economic 모델을 특히 신중하게 설계해야 할 필요가 있다.

Sui economy 모델은 아래와 같은 기제로 작용한다:

Epoch e 시작 시: e-1과 e 사이의 epoch 경계에서 세 가지 중요한 일이 발생한다. 먼저, SUI 보유자들이 일부 토큰을 밸리데이터에게 위임하고, 새로운 밸리데이터 위원회 (Committee) Ce = (Ve, Se (·))가 구성된다. 둘째, 기준 가스비 가격이 설정된다 (섹션 4 참조). 셋째, 스토리지 펀드의 크기가 공식 (2)와 같이 Fe로 업데이트 되며, 이 마지막 액션은 Sui economic 모델이 총 지분 금액을 위임된 지분과 스토리지 펀드의 합계로 이루어진다고 가정할 것이기 때문에 중요하다. 즉, epoch e동안 스테이킹 된 총 SUI 양은 다음과 같은 방식으로 주어진다: Se+Fe에서 Se = ∑v∈V Se (v)일 때. 보조 변수 ae는 위임된 지분의 비율로 정의하면 된다:

$$\alpha_e = \frac{\mathbf{S}_e}{\mathbf{S}_e + \mathbf{F}_e}.$$

여기서 ae는 Sui의 사용자, 위임자 및 밸리데이터의 종합적인 결정에 따라 시간이 지남과 함께 변경되는 내생 변수이다.

Epoch e 진행 중: 사용자는 Sui 플랫폼에 거래를 제출하고 밸리데이터는 이를 처리한다. Te는 epoch동안 처리된 트랜색션 집합이며, 각 트랜잭션 τ ∈ Te에 사용자는 공식 (1)에 설명된 GasFeese[τ]를 지불한다. τ가 과거 트랜잭션 τ′과 관련된 데이터를 삭제하는 트랜잭션에 해당하는 경우에 사용자는 리베이트e [τ′]의 SUI를 전송받는다.

Epoch e 종료 시: 밸리데이터는 현재 epoch을 종료하기 위해 투표하고, 합의 프로토콜의 도움으로 체크 포인트에 커밋하기 위한 정보를 교환한다. Sui 플랫폼의 현재 상태에 동의하기 위해 밸리데이터 쿼럼에 의해 처리되는 모든 트랜잭션의 합집합이 계산된다. 마지막 단계로는 epoch의 보상을 각기 다른 객체에 분배하는 것이며, 이는 총 두 가지 단계로 진행된다:

- 먼저, epoch 동안 생성된 총 보상의 양을 계산할 필요가 있다. 이 보상은 스테이킹 프로세스에 참여한 객체들에게 분배되며, Sui에는 계산 수수료와 새로운 토큰 발행이라는 두 가지 지분 보상 소스가 있다. 이는 공식으로 풀이하면 아래와 같다:

$$\text{StakeRewards}_e = \sum_{\tau \in T_e} \text{ComputationUnits}_e[\tau] \times P_e^C[\tau] + (\mathbf{M}_{e+1} - \mathbf{M}_e).$$

그림 1에서 볼 수 있듯이, 새로운 토큰 발행으로 인한 지분 보상은 일부 epoch에서 이 채널을 통해 제기된 지분 보상이 0임을 볼 수 있다는 점에서 선택적이다. 실제로 장기적으로 유통되는 SUI의 총량이 제한되어 있다는 점을 감안한다면, 새로운 토큰이 발행되지 않는 경우는 필연적으로 존재할 수밖에 없다. 네트워크 활동이 아직 초기 단계일 때, 밸리데이터에게 보조금을 지급하기 위해 지분 보상으로 지정된 대부분의 새로운 토큰 발행은 Sui의 초반 epoch에 지급될 가능성이 더 높다.

- 두 번째로, 네트워크 참여자 간의 지분 보상 분할을 결정한다. 이를 위해서는 Sui economy의 가장 중요한 요소 중 하나인 스토리지 펀드의 역할을 논할 필요가 있다.

  간단히 말해, 스토리지 펀드는 밸리데이터가 스테이킹 보상의 몫을 조정하여 위임자에 비해 받는 SUI 토큰의 수를 늘릴 수 있게 한다. 스토리지 펀드는 총 지분 계산에 집계되기에, 스테이킹 보상의 일부인 1-ae가 스토리지 펀드에 누적된다.

  그러나 위임된 지분과 달리, 스토리지 펀드는 위임자가 소유하지 않으며, 이는 곧 누가 보상을 받아야 하는지에 대한 물음으로 이어진다.

  Sui economic 모델은 스토리지 펀드에 발생하는 보상이 스토리지를 보상하는 데 사용되어야 한다는 관점을 취하는데, 밸리데이터 또한 데이터를 저장하는 객체이므로, 이러한 보상을 받을 자격이 있는 객체여야 한다.

  공식으로 표현하면, 스테이킹 보상의 분배는 다음과 같다. 위임자가 해당 밸리데이터와 계약을 체결하여 밸리데이터가 서비스에 대한 수수료[7] (commission) $\delta \in [0, 1]$을 받을 자격이 있다고 가정할 시 위임자는 아래의 스테이킹 보상을 받는다:

$$\text{DelegatorRewards}_e = (1-\delta) \times \alpha_e \times \text{StakeRewards}_e.$$

  한편, 밸리데이터는 위임된 지분에 해당하는 나머지 보상과 지분에 해당하는 보상의 몫 $\gamma \in [0, 1]$을 스토리지 펀드에서 받는다:

$$\text{ValidatorRewards}_e = (\delta \times \alpha_e + \gamma \times (1-\alpha_e)) \times \text{StakeRewards}_e. \qquad (3)$$

공식 (3)

$\gamma < 1$로 설정 후 스토리지 자금 보상의 전체 금액보다 더 적은 금액을 밸리데이터에게

[7] 이는 각 밸리데이터가 위임자와 별도의 커미션을 협상하고 이 커미션이 시간이 지남에 따라 변경되는 설정으로 쉽게 일반화할 수 있다. 이러한 경우 밸리데이터 $v \in Ve$에게 주어지는 커미션을 $\delta e\ (v)$로 인덱싱한다.

분배하는 것은 스토리지 펀드의 장기적인 재무 건전성을 유지하는 데 유용하다. 실제로 γ는 1에 가까울 가능성이 높으며, 스토리지 펀드의 상태에 따라 거버넌스 제안을 통해 드물게 업데이트 된다. 스테이크 보상에서 스토리지 펀드의 자본 유입은 다음과 같이 제공된다:

$$\text{Reinvestment}_e = (1-\gamma) \times (1-\alpha_e) \times \text{StakeRewards}_e.$$

이 체계는 전체 회계 일정을 나타낸다:

$$\text{StakeRewards}_e = \text{DelegatorRewards}_e + \text{ValidatorRewards}_e + \text{Reinvestment}_e.$$

요약하자면, 스토리지 메커니즘을 통해 밸리데이터는 위임된 지분에 해당하는 지분 이상의 추가 보상을 획득하여 스토리지 오버헤드를 충당할 수 있다. 스토리지 펀드는 SUI 위임자와 밸리데이터 사이의 쐐기 역할을 하며, 후자가 전체 스테이킹 보상에서 자신의 몫을 늘릴 수 있도록 한다. 이를 이해하려면:

$$\underbrace{(\delta \times \alpha_e + \gamma \times (1-\alpha_e))}_{\text{validator rewards with storage pricing}} > \underbrace{\delta}_{\text{validator rewards without storage pricing}} \Leftrightarrow \gamma > \delta.$$

이는 사실상 밸리데이터들이 위임자로부터 빌린 SUI보다 낮은 이자율로 스토리지 펀드에 예치된 SUI를 빌릴 수 있었던 것과 같다. 이는 γ > δ일때만 사실이며, 실제로 위임자는 낮은 수수료 (낮은 δ)으로 제공되는 경우에만 위임하기 때문에, 프로토콜은 스토리지 (높은 γ)에 대해 보상하도록 설계되어 있다.

4. 가스비 메커니즘: 설계와 인센티브

Sui 가스비 메커니즘은 두 가지 중요한 목표를 달성하도록 설계되었다. 첫째, 가스 가격은 $ 조건에서 낮아야 하고, epoch 내에서, 그리고 epoch 전반에 걸쳐 예측 가능해야 한다. 이는 Sui 사용자들이 거래 수수료의 수준과 변동성을 걱정할 일 없이 Sui 네트워크 사용에 집중할 수 있게끔 좋은 사용자 경험을 제공한다. 둘째, 가스비 메커니즘은 Sui의 정규 운영 전반에 걸쳐 양심적인 밸리데이터 행동을 장려하고 보상하도록 설계되어 있다. 이는 SUI 토큰 보유자, 네트워크 운영자 (밸리데이터) 및 사용자 간의 인센티브를 조정한다.

4.1 계산에 대한 가스비

공식 (1)에서 계산 가스비 PCE[t]는 트랜잭션 수준에서 설정되므로, epoch 내에서, 그리고 epoch 전반에 걸쳐 변한다. 더 구체적으로, Sui 네트워크는 계산 가스비를 별도의 고정 요소와 팁 구성 요소로 분리한다:

$$P_e^C[\tau] = \underbrace{\overline{P}_e^C}_{\text{fixed component}} + \underbrace{\zeta[\tau]}_{\text{tip}}, \quad \text{s.t. } P_e^C[\tau] > \underbrace{\underline{P}_e^C}_{\text{price floor}}.$$

상기 식에서, 고정 구성 요소 PCe는 epoch 기간동안 네트워크 수준에서 설정되며, 팁 ζ [τ]는 사용자의 재량에 따른다. ζ [τ]는 음수일 수는 있지만, 전체 가스비를 양수로 유지하고 가격 하한선 PCe 이상으로 유지해야 하므로, t를 제출하는 사용자는 단순히 네트워크 전체 고정 구성 요소에 대해 지불할 의사가 있는 금액을 명시하는 것이다: ζ [τ] = P C e [τ] − PCe. 가격 하한선은 네트워크가 스팸으로 넘쳐나는 것을 방지하기 위해 존재하며, 정규 활동 처리에 영향을 미치지 않아야 한다. 실제로 가격 하한선은 기준 가격에 비례하여 설정할 수 있다. 예를 들면: PCe = βPCe (β < 1)

고정 구성 요소 PCe를 참조 가스비로 볼 때, Sui의 가스 메커니즘은 참조 가스비를 사용자가 네트워크에서 트랜잭션을 제출할 때 사용할 수 있으며 믿을 수 있는 기준점으로 만들도록 설계되어 있다. 즉, 사용자가 참조 가스비 또는 이에 가까운 가스비 (즉, PCe[τ] ≈ PCe 혹은 ζ [τ] ≈ 0)로 트랜잭션을 제출하면 적시에 처리될 것이라고 합리적으로 확신할 수 있다.

가스비 책정 메커니즘은 세 개의 요소를 가진다:

1. 가스비 조사: 전체 0밸리데이터 조사는 각 epoch 시작 시 참조 가격을 설정하는 데 사용된다. 이는 사용자가 가스비 견적 PCE[t]를 제출할 수 있는 조정 가격 포

인트 PCe를 제공한다.

2. 계산 규칙: 전체 밸리데이터 조사는 각 epoch이 끝날 때 스테이크 보상 분배에 대한 입력으로 사용된다. 이는 밸리데이터가 가스 가격 조사 중 결정된 참조 가스비 PCe를 지키도록 인센티브를 제공한다.

3. 인센티브 스테이크 보상 분배 규칙: 각 밸리데이터에게 분배되는 스테이크 보상의 양은 가스 조사 및 집계 규칙의 정보를 사용하여 조정된다. 이는 밸리데이터가 장기적으로 낮은 참조 가스비 PCe를 설정케 하는 인센티브를 제공하며 그들이 시스템을 조작하는 것을 방지한다.

이 세 요소는 함께 사용자에게 더 낮고 안정적이며 신뢰할 수 있는 참조 가스비 PCe를 제공하는 가스비 메커니즘을 생성하는 동시에, 밸리데이터가 이러한 가격을 지키고 적시에 거래를 처리하도록 보장한다. 각 요소에 대한 자세한 디테일은 다음과 같다.

4.1.1 가스비 조사: 가스비란?

가스비 조사는 epoch 경계 바로 전, 위원회가 구성되는 시기에 발생한다. 이는 두 가지 단계에 걸쳐 발생하는데:

- 첫째, 밸리데이터가 다음 epoch의 밸리데이터 집합과 지분 분배 Ce = (Ve, Se (·)를 제안할 때 각 v ∈ Ve에 대한 가스비 제안 pCe(v)도 포함한다.
- 둘째, |Ve| 지분별 제안의 2/3이 이 임계값 이하가 되도록 입찰이 집계되어 참조 가격을 제공한다. 공식으로 풀이하면 (일반성을 잃지 않고) 밸리데이터는 v ≤ v′이 pCe(v) ≤ pCe(v′)임을 의미하도록 명령된다. 참조 가스비는 다음과 같이 설정된다:

$$\overline{P}_e^C = \overline{p}_e^C\left(v^*\right), \quad \text{with } v^* \in V_e \quad \text{s.t.} \quad \sum_{v=1}^{v^*-1} \sigma_e\left(v\right) < \frac{2}{3} \quad \text{and} \quad \sum_{v=1}^{v^*} \sigma_e\left(v\right) \geq \frac{2}{3}.$$

기본적으로 가스비 조사는 각 밸리데이터에게 어떤 가격으로 트랜잭션을 처리할 의향이 있는지를 묻는다. 응답을 집계하면 사용자가 총 2/3의 지분별 밸리데이터 쿼럼에게 트랜잭션을 즉시 처리할 것이라고 합리적으로 판단할 수 있게 하는 기준 가스비 PCe를 제공한다. 여기서 두 문제가 남아있는데, 첫째, 밸리데이터가 가스 조사 중에 예약 가스비를 정직하게 공개하고 쿼럼이 참조 가스비 근처 가격의 거래를 실제로 처리하도록 하는 동기를 부여하는 것은 무엇인가? 그리고 둘째, 밸리데이터가 견적 가격을 존중하더라도 그들이 임의로 높은 가스비를 설정하지 못하게 하는 것은 무엇인가?

4.1.2 집계 규칙: 파이를 어떻게 나눌 것인가

집계 규칙은 epoch e가 끝날 때쯤 적용되는데, 이는 현재 밸리데이터 집합이 해당 epoch 동안 처리된 트랜잭션에 대한 완전한 합의에 도달하고, 스테이크 보상이 지급되기 전을 뜻한다. 집계 규칙은 각 밸리데이터가 다른 모든 밸리데이터에게 얼마나 많은 스테이킹 보상을 분배해야 하는지에 대한 주관적인 측정을 구성하는 데 사용되며, 이 규칙의 목표는 밸리데이터가 가스비 조사 중에 제출된 견적 pCe(v)를 준수하도록 권장하는 커뮤니티-시행 시스템을 갖추는 것이므로, 밸리데이터가 실제로 예약 가격을 공개하도록 장려하는 것이다. 특히, 견적을 존중하지 않는 밸리데이터를 처벌함으로써 이러한 인센티브는 임의로 낮은 가스비 견적을 제출하여 시스템을 조작하려는 밸리데이터들을 예방할 수 있다.

집계 규칙은 세 개의 요소를 가진다.

- 실행된 가스비 분포: Te가 epoch e 동안 실행된 트랜잭션 집합이라고 할 때, 각 트랜잭션 τ ∈ Te에는 계산 가스비 Pce[t]가 포함되므로, 밸리데이터는 실행된 가스비 분포를 구성할 수 있다:

$$T_e[p] = \left\{ \tau \in T_e \text{ s.t. } P_e^C[\tau] \geq p \right\}.$$

  이 분포는 epoch 경계에서 확실한 데이터를 필요로 하므로, 모든 밸리데이터가 알고 있는 공통적이고 객관적인 메트릭이다.

- 합리적인 실행 메트릭: 각 밸리데이터 v는 epoch동안 다른 모든 밸리데이터 v′가 처리한 트랜잭션에 대해 주관적인 평가를 한다. 특히 이 추정치는 가스비 조사 중에 제출된 견적 pCe(v′)에 대해 상대적인 값을 가진다. 공식적으로는:

$$\hat{T}_e^v(v') = \left\{ \tau \in T_e \left[\overline{p}_e^C(v') \right] \text{ s.t. } v' \text{ processed } \tau \text{ in reasonable time} \right\}.$$

밸리데이터 v′가 가스 견적을 제출한 경우에 PCe[τ] ≥ pCe(v′)가 되도록 모든 트랜잭션 τ ∈ Te를 즉시 처리했어야 한다는 것이 주요 내용이다.

합리적인 실행 메트릭은 각 밸리데이터 v에 의해 epoch 동안 수집된 데이터와 epoch 경계에서 모든 밸리데이터에게 알려진 객관적 데이터의 조합에 따라 달라지기 때문에 주관적인 측정이다. 예컨대, 밸리데이터는 그들 사이에 가십을 구현할 수 있으며, 각 밸리데이터는 다른 가십을 듣고, 처리된 트랜잭션에 대한 알림을 받는다. 밸리데이터 간의 차이는, 가십을 들은 밸리데이터 v의 관점에서 각 밸리데이터 v′의 상대적 성능을 추정하는 데 사용할 수 있다. 증명가능한 비잔틴 행동, 알려진 정보 제공 지연, 어떤 밸리데이터가 어떤 트랜잭션을 서명하는지 관찰 혹은 다른 전략들과 같은 추가 정보를 추가 정보 소스로 사용할 수 있으나, 궁극적으로 이 메트릭은 동료에 대한 정보 신호를 얻을 수 있는 각 밸리데이터의 능력에 따라 달라지기 때문에 주관적이다.

- 집계 규칙: 실행된 가스비 분포 및 합리적인 실행 메트릭은 상대적 밸리데이터 성능의 추정치를 구성하는 데 사용된다. 구체적으로, 밸리데이터 v는 서로 밸리데이터 v′에 대해 다음 승수 (multiplier)를 제안한다:

$$\hat{\mu}_e^v\left(v'\right) = \phi^v \times \frac{\sum_{\tau \in \hat{T}_e^v(v')} \text{ComputationUnits}_e\left[\tau\right] \times P_e^c\left[\tau\right]}{\sum_{\tau \in T_e\left[\overline{p}_e^C(v')\right]} \text{ComputationUnits}_e\left[\tau\right] \times P_e^c\left[\tau\right]},$$

에서 각 φ v는 정규화 상수로 아래를 가능케 한다:

$$\frac{1}{|V_e| - 1} \times \sum_{v' \in V_e \setminus \{v\}} \hat{\mu}_e^v\left(v'\right) = 1.$$

승수의 분자는 밸리데이터가 자체적으로 선언한 예약 가스비보다 높은 가스비를 가진 모든 트랜잭션 중, 검증자 v′가 합리적인 시간 내에 실행한 모든 트랜잭션에 대한 계산 가스비를 합산한다. 분모는 가스비가 밸리데이터 v′의 예약 가격 이상인 epoch에서 실행된 모든 트랜잭션에 대한 계산 가스비를 합산한다. 즉, 분모에는 밸리데이터 v′가 즉시 처리해야 했지만 처리하지 않은 트랜잭션이 포함된다. 분자와 분모 모두 실행된 가스비에 의해 가중되며, 이는 이와 관련된 메트릭이 밸리데이터가 처리했어야 하는 트랜잭션에 상대적인 처리된 계산의 양을 뜻하기 때문에 그렇다[8].

[8] Te [p] , Tˆ ve(v′), 및 μˆve(v′)를 포함한 모든 집계 규칙 변수는 실행된 트랜잭션 집합 Te가 클 때 epoch에서 계산 속도를 높이기 위해 샘플링 기술로 근사화(approximated)될 수 있다.

마지막으로, 정규화 φv가 포함되어 각 밸리데이터 v가 다른 모든 밸리데이터 v' ∈ Ve/ {v}에 대해 승수의 집합인 μˆve(v')을 제출하면 평균이 1이 되지만, 상대적으로 우수한 성과의 밸리데이터가 μˆve(v') > 1의 부스트를 받고, 상대적으로 낮은 성과의 밸리데이터는 μˆve(v') < 1로 불이익을 받는다. [9]

요컨대, 집계 규칙은 각 밸리데이터 v가 아래와 같이 생각할 수 있게 하는 승수를 제공한다: 자체 선언한 예약 가스비 이상의 모든 트랜잭션을 합리적인 시간 내에 처리했다는 점에서 밸리데이터 v'가 잘 운영했다면 스테이크 보상이 높아져야 한다. 그렇지 않았다면, 그의 스테이크 보상은 낮아지거나 처벌받아야 한다.

따라서, 집계 규칙은 밸리데이터가 가스비 조사 중에 제출된 가스비 견적을 존중하도록 커뮤니티-시행 인센티브를 생성한다. 이런 인센티브는 분수적이며 (trickle upstream), 밸리데이터가 존중할 수 있는 견적을 제공함으로써 밸리데이터의 보상이 깎이는 것을 방지하기 때문에, 애초부터 정직한 견적을 제출하도록 권장한다.

4.1.3 인센티브 지분 보상 분배 규칙: 공정한 가격을 위한 건전한 경쟁

집계 규칙은 밸리데이터가 존중할 수 있는 가스비 견적을 제출하도록 장려하지만 가스 메커니즘에는 여전히 가스비를 낮게 유지할 인센티브가 없다. 인센티브 지분 보상 분배 규칙은 밸리데이터가 집합적으로 낮은 참조 가스비를 제안하는 균형을 추구하며, 이 규칙은 아래 세 단계로 구현된다:

- 첫째, 프로토콜은 공식 (3)에 설명된 대로 epoch e의 총 밸리데이터 지분 보상을 계산한다.
- 둘째, 프로토콜은 집계 규칙에서 밸리데이터가 제출한 승수 집합을 사용하여 전역 승수 (global multiplier) 집합을 계산한다. 공식적으로 표현하면 밸리데이터 v의 전역 승수는 아래와 같다:

[9] 정규화는 절대적인 성능에 초점을 맞추는 대신 (즉, 레벨 대신 승수의 분산에 초점), 듣는 밸리데이터의 관점에서 다른 밸리데이터의 상대적인 성능에 초점을 맞추기 때문에 중요하다. 결과적으로 승수는 밸리데이터가 서로에 대한 주관적인 정보를 얻는 능력이 크게 다른 경우에도 꽤 유용하게 사용될 수 있다.

$$\hat{\mu}_e(v) = \text{Median}\left\{\hat{\mu}_e^1(v), \ldots, \hat{\mu}_e^{v-1}(v), \hat{\mu}_e^{v+1}(v), \ldots, \hat{\mu}_e^{V_e}(v)\right\},$$

여기서 중앙값 (median)은 밸리데이터 지분 σe (v') 분포에 의해 가중되며, 중앙값 규칙은 Sui 밸리데이터의 하위 집합이 서로에게 지나치게 높은 승수를 제공하여 지나치게 높은 양의 보상을 도용하는 비잔틴 행동으로부터 Sui의 economic 모델을 보호하는데 도움이 된다. 밸리데이터 v는 자체 성과에 대한 견적을 따로 제출하지는 않는다.

- 셋째, 공식 (3)의 밸리데이터 보상 총액은 다음과 같은 인센티브 분배 규칙에 따라 개별 밸리데이터에게 분배된다:

$$\text{ValidatorRewards}_e(v) = \hat{\sigma}_e(v) \times \text{ValidatorRewards}_e$$

여기서 밸리데이터의 몫인 v는 다음과 같다:

$$\hat{\sigma}_e(v) = \begin{cases} \psi \times (1+\kappa) \times \hat{\mu}_e(v) \times \sigma_e(v), & \text{if } v \le v^*, \\ \psi \times (1-\kappa) \times \hat{\mu}_e(v) \times \sigma_e(v), & \text{if } v > v^*. \end{cases}$$

여기서 v ≤ v*는 참조 가격보다 낮은 견적을 제출하는 밸리데이터를 인덱싱한 것이다 (즉, pCe(v) ≤ PCe). 반면, v>v*는 위의 밸리데이터에 해당한다: pCe(v) > PCe

	if validator does process transactions promptly $\hat{\mu}_e(v) \ge 1$	if validator does not process transactions promptly $\hat{\mu}_e(v) < 1$
if validator submits low quote: $\overline{p}_e(v) \le \overline{P}_e$	$\hat{\sigma}_e(v) \ge \psi \times (1+\kappa) \times \sigma_e(v)$	$\hat{\sigma}_e(v) < \psi \times (1+\kappa) \times \sigma_e(v)$
if validator submits high quote: $\overline{p}_e(v) > \overline{P}_e$	$\hat{\sigma}_e(v) \ge \psi \times (1-\kappa) \times \sigma_e(v)$	$\hat{\sigma}_e(v) < \psi \times (1-\kappa) \times \sigma_e(v)$

표 1: 인센티브 스테이크 보상 분배 규칙: 가스 메커니즘은 밸리데이터가 낮은 가스비 견적을 제출하도록 인센티브를 생성하지만, 해당 가스비를 합리적으로 존중할 수 있는 지

점까지만 생성한다. (위->아래, 왼쪽-> 오른쪽 순서로: 밸리데이터가 트랜색션을 신속하게 처리할 때/하지않을 때, 밸리데이터가 낮은 견적을 제출할 때/높은견적을 제출할 때)

인센티브 규칙의 주요 혁신은 K>0이 낮은 가스비, 특히 백분위수의 2/3보다 아래인 견적을 제출하는 밸리데이터가 얻은 보상을 높이기 위해 추가 승수로 포함된다는 것이다. 비슷한 맥락에서 높은 가스비 견적을 제출하는 밸리데이터는 보상에서 불이익을 받게 된다.

표 1은 밸리데이터 인센티브를 요약한 것이다. 두 가지 주요 작용이 존재하는데, 집계 규칙은 밸리데이터가 가스 조사중에 제출된 견적을 존중하도록 인센티브를 제공하는 반면, 분배 규칙은 밸리데이터가 낮은 가스비를 제출하도록 장려한다. 이 두가지 규칙의 상호작용이 매우 중요하다. 실제 가격만 따지고 보면, 가스 가격 메커니즘은 밸리데이터가 낮은 가스비를 제출하도록 권장하지만, 밸리데이터가 너무 낮은 가격을 제출하면 그 가격을 지키기가 어려워질 테니 너무 낮은 가격을 제출할 수는 없게 된다. 따라서, Sui의 가스 가격 메커니즘은 공정한 가격에 대한 건전한 경쟁을 장려하게 된다. 이상적인 균형 상태에서 모든 밸리데이터는 작업과 행동을 최적화하여 우수한 성능을 제공한다. 이러한 대칭 균형에서 밸리데이터는 전체 지분의 몫에 비례하는 보상의 몫을 받는다. 이는 σˆe (v) = σe (v) 이다.

SUI 위임자는 위임된 밸리데이터에게서 발생하는 보상의 비례적 몫을 상속하기 때문에, 동일한 작용의 영향 아래에 있다. 구체적으로 밸리데이터 v의 위임자에게 분배되는 스테이크 보상의 총량은 다음과 같이 나타낼 수 있다:

$$\mathrm{DelegatorRewards}_e(v) = \hat{\sigma}_e(v) \times \mathrm{DelegatorRewards}_e.$$

따라서, SUI 위임자는 밸리데이터 행동에 따라 위임 결정을 최적화하여 중요한 모니터링 역할을 하게 된다. 밸리데이터는 훌륭한 성과에 대해 이중으로 인센티브를 받지만, 그렇지 않을 경우에는 보상 삭감을 통한 직접적 처벌을 받고, 향후 epoch에서 위임된 지분을 잃음으로써 간접적 처벌을 받는다.

4.2 스토리지 가스비

계산 가스비 PCe[τ]와 달리, 저장 가스비 PSe는 한 epoch 내의 모든 트랜잭션에 대해 일정하며, epoch 경계의 경우에만 드물게 달라진다.

스토리지 가스비를 설정하려면 두 가지 이유로 계산 가스비와 다른 메커니즘이 필요한데, 첫째는 스토리지 가격은 현재 밸리데이터가 실행한 트랜잭션에 대해 부과되지만, 미래 밸리데이터들을 보상하는데 사용된다는 점이다. 이는 현재와 미래의 밸리데이터가 관심을 갖는 인센티브 사이에 어떠한 연결고리를 만든다. 둘째는 스토리지 비용이 미래 밸리데이터를 위한 지속 가능한 비즈니스 모델을 생성하기 위한 것일 뿐이며, 계산 가스비처럼 적절한 네트워크 운영을 만들기 위함이 아니다. 이 두가지 이유로, Sui의 스토리지 가격 책정 프레임워크는 계산 가격 책정 메커니즘보다는 더 간단하다.

Sui의 스토리지 가격은 다양한 epoch(예: 몇 개월) 동안 거버넌스 제안을 통해 설정된다. 특히 스토리지 가격 목표는 스토리지 단위의 달러 가치를 고정하여 외생적으로 설정된다. 한 epoch동안 하나의 스토리지 단위를 저장하는 비용을 $x라고 할 때, 저장 가스비는 다음과 같이 설정된다:

$$\overline{P}^S = \frac{\$x}{r P^{\$}},$$

여기서 r은 스테이크 보상에 대한 평균 명목 수익(비연간)이며, P$는 SUI의 평균 달러 가격이다. 둘 다 이전 기간 (예: 지난 주)에 걸쳐 취해진 것이다. 각 후속 epoch PSe=PS의 스토리지 가격은 새로운 거버넌스 제안이 통과될 때까지 이 수준으로 유지된다. 이 목표 설정은 목표가 적용되는 한 스토리지 수수료가 달러 기준으로 대략적으로 고정되도록 하며, 사용자가 트랜잭션 T를 제출하면 다음과 같은 $ 조건으로 스토리지 비용을 지불한다:

$$\text{StorageUnits}_e[\tau] \times P_e^S \times P_e^{\$} \approx \text{StorageUnits}_e[\tau] \times \frac{\$x}{r}.$$

밸리데이터는 스토리지 펀드에서 SUI의 수익을 받기 때문에, 각 epoch 간 위에 명시된 r%를 받게 된다. 본 백서는 SUI 달러 가격이 상당한 수준의 변화를 보일 때 거버넌스 제안을 통해 스토리지 비용이 업데이트될 것으로 보고 있다. 장기적으로 PS는 기술 향상과 함께 스토리지 달러 비용이 하락함에 따라 하락하는 경향을 보인다.

4.3 조정 메커니즘으로서의 가스비

Sui의 가스비 메커니즘은 최종 사용자에게 트랜잭션 제출을 위한 신뢰할 수 있는 기준점

을 제공한다. 밸리데이터가 실제 예약 비용을 산출하고, 이러한 견적을 존중하도록 장려함으로써 Sui 사용자는 계산 참조 가격 혹은 그에 근접한 가격으로 제출된 트랜잭션이 적시에 처리될 것이라고 신뢰할 수 있을 것으로 볼 수 있다. 마찬가지로, 프로토콜은 스토리지 수수료를 스토리지 펀드에 예치하도록 요구하기 때문에, 밸리데이터는 참조 스토리지 가스비보다 많거나 적은 비용을 사용자에게 청구할 인센티브는 없다.

전반적으로, 가스비 PCe[t] = PSe로 트랜잭션 t를 제출하는 사용자는 우수한 사용자 경험을 가지며 지갑과 같은 클라이언트는 이러한 가격을 사용자에게 자동으로 제공해야 한다. Sui의 가스 메커니즘은 사용자가 일반적으로 가스에 대해 초과 지불하는 경매 기반 설정의 함정을 피하는데, 이는 Sui의 가스 메커니즘이 Sui의 수평 확장 능력과 일치한다는 것과 비슷하다. 네트워크 활동이 증가하면 밸리데이터는 더 많은 작업자를 추가하고 비용을 선형적으로 증가시키며 여전히 낮은 가스비로 트랜잭션을 처리할 수 있다. 밸리데이터가 충분히 빠르게 확장할 수 없는 극단적인 네트워크 정체의 경우에, 팁의 존재는 Sui 플랫폼에서 트랜잭션 비용을 증가시켜 추가 수요 급증을 막는 시장 기반 규제 메커니즘을 제공한다.

장기적으로, Sui의 가스 메커니즘은 밸리데이터가 하드웨어 및 운영을 최적화하도록 인센티브를 생성한다. 보다 효율적인 운영에 투자하는 밸리데이터는 낮은 가스비를 존중하고, 1+K의 보상 부스트를 얻을 수 있다. 따라서, Sui 밸리데이터는 최종 사용자의 경험을 혁신하고 개선시키도록 장려된다.

5. 스토리지 펀드: 설계와 인센티브

Sui 스토리지 펀드는 미래의 밸리데이터들에게 실행 가능한 비즈니스 모델을 제공하도록 설계되어있다. 미래의 밸리데이터가 온-체인 데이터를 저장하는 것을 보상하기 위해 현재의 밸리데이터들은 작성 시점에서는 계산 가스비를 받지 못한다. 본 섹션에서는 스토리지 펀드의 세부적인 작업에 대해 설명하고, 그 설계가 스토리지 비용을 영구적으로 충당하는 방법이 설명될 것이다.

5.1 스토리지 펀드의 장기 실행 가능성

스토리지 펀드의 장기 실행 가능성과 관련하여 두 가지 주요 우려사항이 있다. 첫째, 펀드의 자산이 절대 고갈돼서는 안된다. 스토리지 펀드에 기금이 없다면 아무 쓸모가 없다. 둘째, 스토리지 펀드의 크기는 밸리데이터가 스토리지에 보유하고 있는 데이터의 양과 상관 관계가 있어야만 한다. 그렇지 않으면 밸리데이터는 스토리지 비용 구조를 스토리지 자금에서 진행되는 보상과 일치시킬 수가 없기 때문이다.

Sui의 economic 모델은 SUI 토큰의 소스로 직접 사용되지 않는 스토리지 펀드의 자본을 보존하도록 설계되어 있다. 오히려 스토리지 펀드는 단순히 자본 수익 (예: 스테이킹 보상)을 밸리데이터에게 분배한다. 펀드의 원금을 건드리지 않는 이 디자인은 저장에 대한 보상을 무한정 분배하는 펀드의 능력을 보호한다. 이 기능은 펀드 수익의 1-y몫에 해당하는 각 epoch 말에 재투자된 자본에 의해 더욱 강화된다.

Sui의 economic 모델은, 또한, 스토리지 펀드의 규모가 스토리지에 보관된 데이터 양에 비례하도록 설계되어 있다. 이 목표는 데이터가 작성되었을 때 원래 지불한 스토리지 비용 측면에서 데이터 삭제 리베이트를 표시함으로써 달성된다. 공식으로 표현하면, epoch e에서 실행된 트랜잭션 $\tau \in T_e$와 관련된 데이터를 epoch $e' \geq e$ 동안 삭제하면 아래와 같이 표현할 수 있다:

$$\text{Rebates}_{e'}[\tau] = \theta \times \text{StorageUnits}_{e}[\tau] \times P_e^S \qquad (4)$$

여기서 $\theta \in [0, 1]$이다. $\theta = 1$인 극단적인 경우에는 리베이트는 스토리지 비용을 전액 반환한다. 리베이트 기능은 데이터의 수명 주기 동안 스토리지를 보상하기 위해 스토리지 비용이 존재한다는 사실에 의의가 있다. 데이터가 삭제된 후에는 스토리지 비용을 계속 청구할 이유가 없으므로 이러한 요금은 전액 환급된다. 따라서, 사용자는 스토리지 비용을 지불하는 "삭제 옵션"을 사용할 수 있지만, 해당 스토리지가 더 이상 재정적으로 합리적이지 않을 때마다 리베이트를 얻을 수도 있다. 보다 일반적으로, $\theta<1$은 거래 t와 관련

된 일부 데이터가 삭제될 수 있고, 보관 비용의 몫 1- θ가 보관 비용을 영구적으로 보상하기 위해 기금에 남아있는 경우에 유용하다.

리베이트 기능의 주요 속성은 개별 트랜잭션 수준에서 스토리지 펀드 유출을 원래 스토리지 유입보다 항상 작게 제한한다는 것이다. 특히, epoch e′에서 삭제 시점의 저장 가스비 PSe′은 스토리지 리베이트가 쓰기 시점에 예치된 SUI에 비례하기 때문에 관련이 없다. 이 메커니즘은 스토리지 펀드의 크기가 스토리지에 보관된 데이터의 양에 따라 이동하도록 보장한다. 스토리지 펀드를 이해하는 간단한 방법은, 마치 그것이 개인 계정의 모음으로 만들어진 것처럼 생각하는 것이다. 각 계정은 과거 트랜잭션 T와 관련된 객체에 해당하며, 예치된 금액은 T가 처리될 때 지불한 스토리지 비용과 같다. T의 출력 오브젝트의 소유자는 이러한 계정의 소유자이며, 연결된 오브젝트를 삭제한다는 가정하에 자금을 인출할 수 있다. 이 회계방식은 스토리지에 보관된 활성 오브젝트와 관련된 스토리지 비용이 항상 포함되어 있기 때문에, 스토리지 펀드가 고갈될 수 없다는 주장을 증명하는데 유용하다.

결론을 내리자면, 공식 (2)의 스토리지 펀드의 재귀 공식은 상술된 Sui에서 실행된 거래에 해당하는 일련의 개별 계정에 대한 해석에 따라 다시 작성 가능하다. 구체적으로, epoch e 종료 시 스토리지 펀드의 가치는 초창기(genesis) epoch의 펀드의 초기가치, 각 epoch에서 e까지의 자본화 유입 및 삭제 리베이트를 차감한 순 스토리지 비용 유입의 총량과 같다. 이를 공식화하면 다음과 같다:

$$\mathbf{F}_{e+1} = \mathbf{F}_0 + \underbrace{\sum_{\varepsilon=0}^{e} \text{Reinvestment}_\varepsilon}_{\text{capitalizations}} + \underbrace{\sum_{\varepsilon=0}^{e} \sum_{\tau \in T_\varepsilon} \left(1 - \theta \times \mathbb{I}\left[\tau \in \bigcup_{\varepsilon'=\varepsilon}^{e} R_{\varepsilon'}\right]\right) \times \text{StorageUnits}_\varepsilon[\tau] \times P_\varepsilon^S}_{\text{storage fees net of deletions}}.$$

표기법은 I [·] 가 지표 함수를 나타내며, τ ∈ Tε 와 τ ∈ Se ε′=ε Rε′가 모두 참일 때, τ는 epoch ε동안 처리된 트랜잭션으로, 당시와 현 epoch e ≥ ε 사이에 삭제된 트랜잭션이 된다. 이 경우 원래 지불한 스토리지 비용의 1- θ만 스토리지 펀드에 남는다.

6. Sui Economy: 장기 역학

6.1 Sui 디플레이션

Sui 토크노믹스에는 SUI 토큰을 직접 소각하는 메커니즘이 포함되어 있지 않다. 그러나, 장기 공급이 100억 개의 토큰으로 제한되어 있기 때문에, Sui 플랫폼에서의 활동 증가는 사실상 디플레이션 요인이 된다. Sui가 더 많은 사용 사례를 잠금 해제하고, 더 많은 사용자가 플랫폼으로 이동하면 Sui의 상대적 경제 활동량이 오프-체인 세계에서 증가하기 때문에, SUI의 달러 가격이 증가할 가능성이 높다. 결과적으로 가스비를 포함한 온-체인 SUI 가격이 하락하고 Sui economy는 디플레이션에 진입할 수 있다.

상술된 Sui의 한정된 공급에서 파생된 표준 디플레이션 효과 위에도, Sui 스토리지 펀드는 두 가지 추가적인 디플레이션 요인을 도입한다. 하나는 일시적이나, 다른 하나는 영구적이 될 수도 있다. 스토리지 펀드의 일시적인 효과는 스토리지 펀드의 토큰이 잠기고 다른 활동에 사용될 수 없기 때문에 발생한다. 따라서, epoch동안 전체 토큰 공급은 Me와 같지만, Sui에서 스테이킹, 가스비 지불 및 기타 활동에 사용할 수 있는 SUI 토큰의 실제 양은 Me-Fe로 제공된다. 이 효과는 원칙적으로 사용자가 온-체인 데이터를 삭제하고 스토리지 펀드에서 SUI 토큰을 해제할 수 있기 때문에 일시적인 디플레이션일 뿐이다. 그렇다고 하더라도, 스토리지는 네트워크 활동과 함께 증가할 가능성이 높기 때문에 이 디플레이션 요인은 장기적으로 중요할 가능성이 높다.

더 흥미로운 효과는 SUI 토큰 공급에 대한 스토리지 펀드의 반-영구적 효과이다. M~e+1을 e와 e+1 사이의 epoch 경계에서 순환할 수 있는 최대 SUI 토큰수 라고 할 때, 이 용어는 다음과 같이 재귀적으로 계산할 수 있다.

$$\tilde{\mathbf{M}}_{e+1} = \tilde{\mathbf{M}}_e + \underbrace{(\mathbf{M}_{e+1} - \mathbf{M}_e)}_{\text{SUI issuance}} - \underbrace{\text{Reinvestment}_e}_{\substack{\text{storage fund} \\ \text{capitalization}}} - \underbrace{\sum_{\tau \in T_e} \frac{1-\theta}{\theta} \times \text{Rebates}_e[\tau]}_{\text{rebate residual}}.$$

E+1에서 유통되는 유효 토큰수는 e에서 유통되는 유효 토큰수에 새로 발행된 SUI 토큰 값을 더한 것에서 스토리지 펀드를 자본화 하기위해 재투자된 토큰의 새 스토리지 리베이트 잔여분을 뺀 값과 같다. 자본화 기간은 스토리지 펀드에 재투자된 지분 보상이 영구적으로 거기에 예치된다는 것을 이야기한다. 즉, 쓰기 트랜잭션에 의해 간접적으로 소유되지 않으므로, 어떤 당사자도 인출할 수 없다. 유사하게, 리베이트 잔여분은 삭제할 수 없는 데이터의 스토리지에 자금을 지원하기 위해 영구적으로 스토리지 펀드에 남아

있는 스토리지 비용의 몫으로 제공된다. 이 마지막 두 조건은 스토리지 펀드에 영구적으로 예치된 코인을 나타내므로, M~e+1은 모든 사용자가 온-체인 데이터를 삭제하는 극단적인 경우에도 유통될 수 있는 SUI 토큰의 최대 수를 이야기한다.

스토리지 펀드의 반영구적인 디플레이션 효과는 Sui economy의 스토리지 펀드가 너무 커지는 것을 방지하는 안전 장치를 가지고 있기 때문에 "반-영구"적인 것이다. 다만 여기서 위험은 위임 지분 ae의 비율이 너무 작아지면 네트워크 인센티브가 동기화되지 않을 수도 있다는 것이다. 이를 위해 $\alpha \in (0, 1)$은 $\alpha e \leq \alpha$가 스토리지 펀드 원금의 유출을 유발하는 것과 같다. 이 유출은 스토리지 비용이 아닌 스토리지 펀드 자본화 또는 리베이트 잔여액을 통해 부여된 펀드 원금 부분으로만 제한된다. 이는 펀드의 규모를 관리 가능한 수준으로 유지하면서 장기적인 생존 가능성도 보존한다. 하한 α는 온-체인 거버넌스를 통해 시간이 지남에 따라 업데이트 될 가능성이 높으며, 유출 자금은 향후 지분 보상 보조금으로 별도로 설정할 수 있다.

요컨대, 스토리지 펀드는 SUI 토큰에 두 가지 중요한 디플레이션 효과를 도입시키며, 각각 다른 깊이와 지속적인 영향을 미친다. 일시적인 디플레이션 효과는 더 많은 값의 SUI를 순환에서 제거할 수 있기 때문에 더 강력하다. 그러나 일시적인 효과는 언제든지 변경될 수 있는 스토리지의 현재 데이터 양에 의존하기에, 잠재적으로 수명이 짧다. 반영구적인 디플레이션 효과는 영향은 약하되 잠재적으로 영원히 지속될 수 있으며, 스토리지가 삭제되었는지 여부에 관계없이 Sui 플랫폼의 전체 스토리지 기록에 따라 달라진다.

6.2 자본 효율성

스토리지 펀드는 사용자 관점에서 스토리지 비용을 지불하는 자본 효율적인 방법이다. 이는 반 직관적인 것처럼 보일 수 있지만 (이 모델이 스토리지 펀드에 SUI를 고정해야 하기 때문에), 자본 효율성을 달성하는 것이 Sui의 economy 설계에서의 핵심 목표이다. 자본 효율성은 균형 상태에서 SUI를 잠그는 사용자의 기회 비용이 스토리지에 대해 지불하는 비용과 정확히 동일하다는 사실에서 비롯되는데, 이를 이해하려면 Sui economy가 모든 변수가 시간에 따라 일정하고, 시장에 문제가 없으며, SUI의 공급이 완전히 발행된 안정 상태에 있다고 가정해야 한다. 또한, 스토리지 펀드 재투자가 없고, 삭제는 리베이트의 총량을 제공한다고 가정해야 한다 ($\gamma = \theta = 1$). 스테이킹 된 SUI에 대한 수익은 다음과 같다:

$$r = \frac{\text{StakeRewards}}{\mathbf{S} + \mathbf{F}}.$$

시장 균형 및 밸리데이터가 시장을 무료로 사용할 수 있게 하는 조건은 트랜잭션 T의 데이터 스토리지와 관련된 스테이킹 보상이 스토리지 비용을 정확히 충당함을 의미한다. 즉, 트랜잭션 T에 대해 r × StorageUnits [τ] × P S × P$가 T와 관련된 데이터를 저장하는 $ 비용과 동일해야 한다.

스토리지 펀드는 아래 두 옵션에 대해 유저들이 완전히 무관심할 때 자본 효율성을 가진다:

- 스토리지 펀드를 통해 간접적으로 스토리지 비용 지불: 한정된 수의 epoch동안 T를 저장하는 사용자는 쓰기 시 StorageUnits[T] x PS SUI 토큰을 스토리지 펀드에 예치하고 삭제 시 동일한 양의 SUI를 받는다.
- 모든 epoch의 수수료를 통해 직접 스토리지 비용 지불 (임대구조): 한정된 수의 epoch동안 T를 저장하는 사용자는 매 epoch마다 r x StorageUnits[t] x PS의 수수료를 지불한다. 이는 SUI의 StorageUnits[t] x PS 단위를 스테이킹하고, epoch 종료 시 SUI의 (1 + r) x Storageunits [t] x PS를 획득하고 수수료를 지불함으로써 달성할 수 있다. 사용자가 데이터를 삭제하면 더 이상 스토리지 비용이 청구되지 않으며, 사용자에게는 SUI의 StorageUnits [t] x PS가 남는다.

요컨대, Sui economy는 사용자가 데이터를 저장하기 위해 SUI를 잠그지 않는 임대 모델과 동일한 결과를 달성한다. 마치 스토리지 펀드가 스토리지 비용을 지불하기 위해 사용자의 SUI를 수익성 있게 투자한 것과 같지만, 임대 모델에서는 사용자가 이를 직접 수행한다. 따라서, 경제적으로는 Sui와 임대 모델이 동등하다고 볼 수 있지만, Sui의 설계는 스토리지 모델을 Sui economy에 직접 통합하고 스토리지 비용을 조달하는 방법을 개별적으로 알아내야하는 수 백만명의 사용자에게 의존할 필요가 없기에 더 효과적이다.

6.3 스테이크 분배 역학

Proof-of-stake 시스템에 대한 일반적인 비판은, 밸리데이터 간의 지분 분배가 장기적으로 퇴보적인 분배로 수렴될 가능성이 있는 "부자가 더 부자가 되는" 계획을 촉진한다는 것이다. 이는 밸리데이터 중 한 명 또는 일부가 매 기간마다 지분 보상의 전체 금액을 얻

고, 또한 승리할 확률이 밸리데이터의 총 지분에 대한 자기 몫에 의해 결정되는 proof-of-stake 시스템에서 발생한다.

이 결과에 대한 주요 내용은 밸리데이터가 지분 보상을 재투자할 때 전통적인 proof-of-stake가 복리(compounding)를 가능하게 한다는 것이다. 결과적으로, 높은 지분을 가진 밸리데이터는 낮은 지분을 가진 밸리데이터보다 더 일찍 복리를 시작할 가능성이 더 높다. 이 효과는 시간이 지남에 따라 악화되어 지분이 높은 밸리데이터가 높은 가능성을 가진 대부분의 지분을 가지게 된다. 흥미롭게도 "부자가 더 부자가 되는" 효과는 악의적이거나 전략적인 행동에 대해 유발되지 않으며, 모든 밸리데이터가 정직하게 작업하더라도 발생한다. "부자가 더 부자가 되는" 효과는 전적으로 임의성에 의해 좌우된다.

Sui의 proof-of-stake 모델은 모든 정직한 밸리데이터가 각 epoch이 끝날 때 스테이킹 보상 중 자신의 몫을 확실하게 받기 때문에 "부자가 더 부자가 되는" 효과를 상쇄한다. 이는 곧 밸리데이터들이 무작위성에 의해 좌지우지되지 않는다는 말이다. 이 사실을 활용하여 지분 분배가 시간이 지남에 따라 고정된 상태로 유지된다는 것을 증명할 수 있다. 공식적으로 표현하면, 이것은 모든 밸리데이터가 가스 조사 중 동일한 가격 견적을 제출하고, 합리적인 시간 내에 모든 거래를 처리하며 모든 SUI 위임자와 밸리데이터가 시간이 지남에 따라 동일한 밸리데이터에게 지분 보상을 재투자하는 특별한 경우로 나타낼 수 있다:

$$\begin{aligned}\sigma_{e+1}(v) &= \frac{S_e(v) + \sigma_e(v) \times (\text{DelegatorRewards}_e + \text{ValidatorRewards}_e)}{\mathbf{S}_e + (\text{DelegatorRewards}_e + \text{ValidatorRewards}_e)}, \\ &= \sigma_e(v).\end{aligned}$$

즉, 각 밸리데이터 v ∈ Ve , Ve+1는 epoch e+1 시작 시 epoch e에서 보유한 지분과 동일한 위임 지분을 갖게 된다. 귀납에 따라, 이 증명은 모든 epoch e에 적용되며, 스테이킹 분포가 시간에 따라 일정함을 의미한다. 이 사실은 Sui의 네트워크 보안에 중요한 결과인데, 왜냐면 일부 밸리데이터가 불균형한 의결권을 가질 수 있다는 우려를 잠식시킬 수 있기 때문이다. 위의 증명은 양식화된 설정에 불과하나, 결과는 Sui의 proof-of-stake 구현에 존재하는 중요한 힘을 암시한다.

7. 결론

Sui의 디자인은 공학 및 economic 블록체인 연구의 최전선에 있다. MystenLabs에서는 다양한 커뮤니티와 협력하고, Sui의 economic 모델에 대한 피드백을 econ@mystenlabs.com에서 받아 보기를 기대한다.

APPENDIX 부록

다음 표는 Sui economic 모델의 자유 시스템 매개변수를 요약한 것이다. 빈도 열은 매개변수를 이전 섹션에서 설명한 대로 epoch별로 수정되는 매개변수와, 거버넌스 제안을 통해 드물게 변경되는 매개변수로 분류한다.

매개변수	빈도	내용
PCe	Epoch 당 일정	계산에 대한 참조 가스비 가스 조사를 통해 밸리데이터가 집합적으로 설정
PCe	Epoch 당 일정	계산에 대한 층 가스비 PCe에 비례하여 설정 가능. 예: PCe = βPCe with β < 1.
PS	일정하지 않음	스토리지 가스비 스토리지의 달러 비용을 타겟하기 위해 고정됨
δ	일정하지 않음	밸리데이터 커미션 몫 시스템 수준에서 설정하거나, 각 밸리데이터가 협상 가능
γ	일정하지 않음	밸리데이터에게 분배되는 스토리지 펀드 스테이크 보상의 몫 거버넌스에 의해 설정된 시스템 매개변수
Θ	일정하지 않음	스토리지 삭제 리베이트 몫 거버넌스에 의해 설정된 시스템 매개변수
α	일정하지 않음	최대 스토리지 펀드 크기에 구속 거버넌스에 의해 설정된 시스템 매개변수
κ	일정하지 않음	낮은 가스비 제출자들을 위한 지분 보상 부스트 거버넌스에 의해 설정된 시스템 매개변수