

Augur: 분산화된 오라클과 예측 시장 플랫폼

Jack Peterson, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander
Forecast Foundation
(Dated: April 13, 2018)

어거(Augur)는 신뢰를 기반으로 하지 않는 분산화된 오라클(oracle)과 예측 시장(prediction market) 플랫폼이다. 어거 예측 시장에서 결과는 평판 토큰(Reputation token, 이하 REP 토큰) 보유자들에 의해 선택되고, 이들은 보상으로 청산 수수료(settlement fees)를 받는다. 어거는 토큰을 보유하는 이들이 정확하고 정직하게 결과를 보고했을 때 가장 많은 수익을 얻을 수 있도록 보상 체계가 설계 되어 있다. 토큰 보유자들은 기(既) 제안된 결과에 반하여 분쟁(dispute)하기 위해 점진적으로 더 많은 토큰을 사용할 수도 있다. 만약, 토큰 사용량이 일정 수준에 달하면 제안된 결과는 둘 이상으로 갈릴 수 있고, 토큰 보유자들은 각자 자신의 토큰을 걸고 특정 결과(outcome)를 선택해야 한다. 하지만 실제 일어난 결과와 다른 거짓의 결과는 시장이 정확한 결과를 선택할 것이라 생각하는 참여자들에게 사실상 슬모 없는 선택지이다. 그러므로 토큰 보유자는 실제 결과를 반영한 가치 있는 평판을 선택할 것이다.

어거는 신뢰에 기반하지 않는(trustless) 분산화된(decentralized) 오라클과 예측 시장 플랫폼이다. 예측 시장의 각 참여자들은 미래에 일어날 일의 결과에 투자한다. 결과를 맞게 예측한 이는 수익을 얻고, 다르게 예측하여 틀린 경우 손실을 입는다 [1-3]. 예측 시장에서 책정된 가격은 해당 사건이 일어날 가능성을 가늠하는 계산된 척도로 활용할 수 있다 [4-7].

어거를 통해 사람들은 저비용으로 예측 시장을 이용할 수 있다. 가장 큰 비중을 차지하는 비용이라고 해봐야 개설자에 대한 보상과, 실제 결과가 발생했을 때 이를 보고한 이들을 위한 보상이다. 때문에, 요구되는 신용의 정도, 마찰 그리고 비용을 경쟁 시장보다 낮은 수준으로 유지할 수 있다.

역사적으로 예측 시장은 중앙집중화 방식이었다. 예측 시장 속의 거래를 합산하는 가장 간단한 방식은 신뢰할 수 있는 독립체가 원장(元帳)을 관리하는 것이다. 결과를 정리하고 보상을 지급하는 것도 이와 마찬가지로 신뢰할 수 있는 판단주체가 이를 담당하는 것이 가장 쉽다. 하지만 중앙집중화된 예측 시장은 많은 제한요소와 문제점을 지니고 있다. 중앙집중화 방식은 글로벌 참여가 허용되지 않는 경우가 많고, 개설하고 거래할 수 있는 시장의 종류가 제한적이며, 시장을 운영하는 측이 자산을 훔치거나 결과를 제대로 반영하지 않는 문제가 발생할 수도 있다.

어거는 이를 탈중앙화 방식으로 해결하고자 한다. 비트코인[8]이나 이더리움[9]처럼 탈중앙화되고, 신뢰를 기반으로 하지 않는 네트워크를 통해 사익의 추구가 부패나 사기로 변질될 우려를 제거하였다. 어거 개발진의 유일한 역할도 이더리움 네트워크에 스마트 컨트랙트를 등록하는 것으로 한정된다. 어거의 계약은 완전 자동화되어 있다. 아무리 개발자라도 시장에서 에스크로 형태로 모인 자금을 마음대로 이용할 수 없고, 결과를 조작할 수도 없으며, 거래나 주문을 승인 혹은 거부하거나 취소하는 등의 어떠한 권한도 가지고 있지 않다. 어거의 오라클은 현실 세계의 정보를 블록체인으로 가져올 때 신뢰받는 중재인을 사용하지 않는다. 어거는 세계 최초의 분산화된 오라클이 될 것이다.

I. 어거의 구현 원리

어거의 시장은 개설(creation), 거래(trading), 보고(reporting) 그리고 청산(settlement)까지 4단계를 거친다. 누구나, 현실 세계의 어떤 사건이라도 이를 토대로 예측 시장을 생성할 수 있다. 일단 시장이 생성되면 그 즉시 거래가 시작된다. 누구나, 어떤 시장이건 참여할 수 있다. 예측 시장이 기준으로 삼는 사건이 실제로 발생하면, 어거의 오라클에 의해 결과가 확정된다. 결과가 확정되면, 거래자들은 자신의 포지션에 따라 보상을 받고, 시장은 청산된다.

어거의 시스템은 내부에서 사용하는 별도의 토큰이 있다. 이 토큰은 평판 토큰이라 하는데, 이 REP 토큰은 어거 플랫폼에 현실 세계의 결과를 보고하기 위해 사용한다. 보고자들은 시장에서 일어날 수 있는 결과에 REP 지분(staking)을 참여하는 형태로 보고 과정에 참여한다. 이 과정을 통해 보고자들은 현실의 결과를 블록체인으로 가져오게 된다. 시장 보고자들의 합의는 결과를 판단하기 위한 근거가 되는 일종의 진실이다. 만약, 보고 결과가 다른 보고자 집단이 선택한 합의의 결과와 다르다면 어거는 지분 참여된 REP 토큰을 합의되지 않은 결과를 선택한 집단으로 부터 합의 완료된 결과를 선택한 집단으로 재분배할 것이다.

REP를 보유하고, 정직하게 결과에 참여함으로써 REP 보유자는 거래 수수료의 일부를 받을 수 있다. REP 보유 비율에 비례한 권리를 통해 수수료의 일부를 나눠 갖게 된다. 다양한 REP를 보유한 이가 안정적인 시스템을 위해 정직한 결과를 입력할 수록 더 많은 보상을 받는 구조다.

REP가 어거 시스템의 중추적 역할을 하긴 하지만, 시장에서 거래의 수단으로 사용되지는 않는다. 거래 참여자들이 결과 입력에 참여하고자 하지 않는다면, REP를 사용할 이유는 없다.

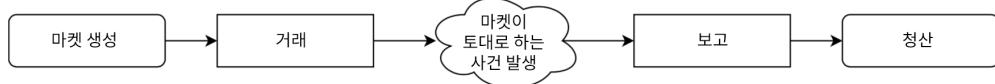


Figure 1. 단순화한 예측 시장의 순환 과정

A. 예측 시장 개설

어거 플랫폼에서는 누구나, 어떤 미래의 일이든 예측 시장의 형태로 개설할 수 있다. 시장 개설자(*market creator*)는 종료 시간(*event end time*)과 함께, 현실 세계의 결과를 보고할 지정된 보고자(*designated reporter*)를 선택한다. 지정된 보고자의 보고는 참여자들에 의해 거부되거나 정정될 수 있기 때문에, 지정된 보고자가 일방적으로 결과를 선택하는 것은 아니다.

다음으로, 개설자는 결과를 판단하는 근거(*resolution source*)를 무엇으로 할 것인지 정해야 한다. 이 근거는 상식적이거나, “The United States Department of Energy”, bbc.com, 처럼 정확한 대상을 지목하거나, 특정 API로 연동되는 프로그램 등의 정확한 주소를 지정하는 것처럼 명확해야 한다.¹ 또한, 개설자 수수료(*creator fee*)를 설정해야 하는데, 이 수수료는 청산 시점에서 거래자가 시장 개설자에게 지불하는 수수료이다(자세한 내용은 섹션 ID 의 수수료 부분을 참조하기 바란다). 마지막으로 개설자는 유효 채권(*validity bond*)과 지정된 보고 미이행 채권(*designated report no-show bond*) 두 개를 발행해야 한다(앞으로 줄여서 미이행 채권(*no-show bond*)이라 하겠다).

예측 시장이 무효(*invalid*)가 아니라 정상적(*valid*)으로 해결되었다면, 유효 채권은 ETH의 형태로 시장 개설자에게 제공된다.² 이는 개설자가 모호하지 않은, 명확한 시장을 개설하도록 독려한다. 유효 채권의 양은 최근 시장에서 발생한 잘못된 결과의 비율에 의해 동적으로 결정된다.³

미이행 채권은 두 가지로 나뉜다: 하나는 미이행 가스 채권(*no-show gas bond*)(이는 ETH로 처리된다)이며, 다른 하나는 미이행 REP 채권(*no-show REP bond*)이다(REP로 처리된다). 이 채권들은 시장 해결의 기준이 되는 사건 종료 시점(*event end time*)에서 3일이 지나기 전에 미리 지정된 보고의 형태로 결과가 보고될 경우 시장 개설자에게 환원된다. 만약 3일 내에

지정된 보고자 누구도 보고하지 않으면 해당 시장에 최초의 공개 보고자(*first public reporter*)에게 주어진다. (섹션 IC 6을 참조하기 바란다). 이는 개설자가 신뢰할 수 있는 보고자를 선택하여 시장이 빨리 청산되도록 유도하는 효과가 있다.

미이행 가스 채권은 최초의 일반 보고자의 가스 비용으로 사용된다. 이를 통해 최초의 일반 보고자가 가스 비용의 부담으로 참여하지 않는 것을 방지한다. 이 채권은 이전 가스 비용의 두배로 책정된다.

지정된 보고자의 보고가 실패한 경우, 미이행 REP 채권은 결과가 일치하는 측의 최초 공개 보고자에게 주어진다. 때문에 공개 보고자 역시 정확한 결과를 보고해야 한다. 유효 채권과 마찬가지로 이전 비용에 따라 동적으로 결정된다.⁴

시장 개설자는 위의 모든 채권을 하나의 이더리움 거래로 공개한다. 이 거래가 승인을 받으면, 해당 예측 시장의 거래가 시작된다.

B. 거래

시장 참여자는 주식(*shares*) 거래와 유사한 형태로 예측 결과에 참여한다. 결과에 연결된 총 발행 증권(*complete set of shares*)은 정상적인(무효가 아닌) 결과와 연결된 증권의 총 합이다 [10]. 전체 증권은 거래의 완료를 위해 어거의 매칭 엔진에 의해 구성된다.

예를 들어 A와 B 두개의 결과가 가능한 시장이 있다고 하자. Alice는 0.7 ETH를 사용하여 A 증권 한 주를 사고 싶고, Bob은 0.3 ETH를 사용하여 B 증권 한 주를 사고 싶다.⁵ 우선, 어거는 이 두 거래를 모아 총 1 ETH를 Alice와 Bob으로부터 모은다.⁶ 그리고 어거는 Alice에게는 A 증권 한 주를, Bob에게는 B 증권 한주를 제공한다. 이 과정을 통해 가능한 결과 A, B가 증권의 형태로 시장에 등장하게 된다. 증권이 생성되면 자유롭게 거래가 가능하다.

어거의 거래 계약은 주식 시장과 비슷한 오더 북의 형태로 모든 시장마다 존재하게 된다. 누구나 새로운

¹가령, “2018년 4월 10일 샌프란시스코 국제 공항의 화씨 최고 기온은 Weather Underground 기준 몇도인가?”라는 예측 시장이 있다면 보고자들은 제시된 단서인 <https://www.wunderground.com/history/airport/KSFO/2018/4/10/DailyHistory.html>, 를 방문하여 최고 기온을 보고하면 된다.

²무효 시장 보고자들에 의해 무효 처리된 시장을 무효 시장이라 한다. 시장 개설자가 입력한 선택 가능 결과가 없거나, 기술이 모호하거나 주관적인 경우가 이에 속한다; 섹션 III F 에서 더 논의하도록 하겠다.

³Appendix E 1에서 자세히 다루도록 하겠다.

⁴Appendix E 2에서 자세히 다루도록 한다.

⁵어거의 예측 시장 내 거래는 이더리움 생태계에서 사용하는 Ether(ETH)를 사용한다. 차후의 어거 시장에서 법정 화폐와 가치 보존되는 토큰(안정화 코인)처럼 이더리움 네트워크의 토큰이 사용될 수 있다.

⁶여기서 1 ETH라 한 것은 논의의 편의를 위해서이다. 실제 주식의 전체 총 비용은 이보다 작다; docs.augur.net/#number-of-ticks를 참조하기 바란다.

거래를 만들거나, 제시된 거래를 수용할 수 있다. 주문은 어거 스마트 컨트랙트 내부의 매칭 엔진을 통해 완료된다. 구매나 판매 주문은 기준에 제시된 거래가 있다면 즉시 체결된다. 다른 참여자로부터 증권을 구매하거나 증권을 판매하는 것으로 구성되며, 이는 결과에 연결된 전체 증권을 새로 생성하거나 이를 종료하는 결과를 가져올 수도 있다. 어거의 매칭 엔진은 위험으로부터 보호하는 최소 주식량과 현금을 격리하도록 되어 있다. 만약 거래를 체결할 기준 주문이 없거나 수량이 부족한 경우, 남은 수량은 새로운 주문의 형태로 오더북에 등록된다.

주문은 거래자가 제시한 가격보다 나쁜 가격으로는 체결되지 않지만 더 나은 조건으로 체결될 수 있다. 완료되지 않았거나 부분적으로 완료된 거래는 다른 거래자의 주문에 의해 언제든지 완료될 수 있다. 거래자가 지불하는 수수료는 전체 주식이 매도될 때에만 부과된다; 청산 수수료에 대한 더 자세한 사항은 섹션 ID에서 논의하도록 하겠다.

대부분의 거래가 청산 직전 시점에 몰리겠지만, 예측 시장이 생성된 이후부터는 언제든 거래가 가능하다. 어거 내부에서 사용되는 모든 자산 – 예상 결과에 따른 증권, 수수료, 채권, 시장에 대한 소유권 등 –은 언제든 이동이 가능하다.

C. 보고

마켓의 대상으로 하는 사건이 발생하면, 종료와 청산 개시를 위해 결과가 밝혀져야 한다. 결과는 어거의 오라클에 의해 밝혀지는데, 이들은 실제 세계의 결과를 보고하는 것에 동기 부여된 보고자들이다. REP를 보유한 누구나 결과 보고에 참여할 수 있다. 합의에 달한 결과를 보고한 이는 보상을 받고, 그렇지 않은 이는 불이익을 받는다 (섹션 ID 3를 참조하기 바란다).

1. 수수료 구간

어거의 보고 체계는 7일간 이어지는 수수료 구간(*fee windows*)의 연속 위에 구현된다. 주어진 수수료 구간 동안 모든 수수료는 보고 수수료 저장소(*reporting fee pool*)에 수집된다. 수수료 구간이 끝나면 보고 수수료는 보고 체계에 참여한 REP 보유자들에게 주어진다. 배분은 참여한 REP의 지분율에 따라 결정된다. 참여는 다음의 방식으로 가능하다: 초기 보고 기간동안 지분 참여하는 것, 논란의 소지가 있는 결과에 반박하는 것 또는 참여 토큰(*participation tokens*)을 구입하는 것이다.

2. 참여 토큰

수수료 구간동안 REP 보유자는 누구나 attorep⁷당 한주의 참여 토큰을 구입할 수 있다. 기간이 끝나면 참여 토큰은 1 attorep으로 환원되는 것은 물론, 수수료 기간 동안 모집된 수수료(*reporting fee pool*)의 일정 부분을 받을 수 있다. 만약 특별한 일 (e.g., 보고가 접수되지 않거나, 접수된 보고에 분쟁이 발생하는 등)이 발생하지 않으면, 보고자는 참여 토큰을 구입하여 수수료 구간에 참여하는 의사를 밝힐 수 있다. REP 지분 참여처럼 참여 토큰의 보유 비율은 수수료를 배분 받는 척도가 된다.

섹션 II의 내용에서 알수 있듯이, 포크(fork)가 발생하는 시점에 REP 보유자가 시장을 해결할 준비가 되어 있는 것이 중요하다. 참여 토큰은 REP 보유자들이 최소 1주일에 한 번은 모니터링을 하고자 하는 동기를 부여한다. 보고 체계에 참여할 의사가 없는 REP 보유자라도 수수료 징수 기간 동안 참여 토큰을 구입하고 수수료를 받도록 유도하는 것이다. 이러한 규칙적인 참여는 어거 시스템에 친숙해지는 것을 돋고, 포크에 대한 경계를 높여 실제 포크가 발생하더라도 대처가 용이하게 만드는 효과가 있다.

3. 시장의 진행 단계

어거의 시장은 아래 7개 중 하나의 단계에 속하게 된다::

- 보고 전
- 지정된 보고
- 공개 보고
- 다음 수수료 구간을 위한 대기
- 분쟁
- 포크
- 종료

각 단계 간의 상관관계는 Fig. 2에서 확인할 수 있다.

4. 보고 전

보고 전 단계(*pre-reporting*) 혹은 거래 단계(*trading phase*)(Fig. 1)는 거래가 시작된 이후의 기간부터 대상 사건의 발생 전까지에 해당한다. 이는 일반적으로 거래가 행해지는 기간이기도 하다. 거래 종료기간이 지나면 시장은 지정된 보고(*designated reporting*) 단계 (Fig. 2a)로 진행된다.

⁷ 1 attorep 은 10^{-18} REP 이다.

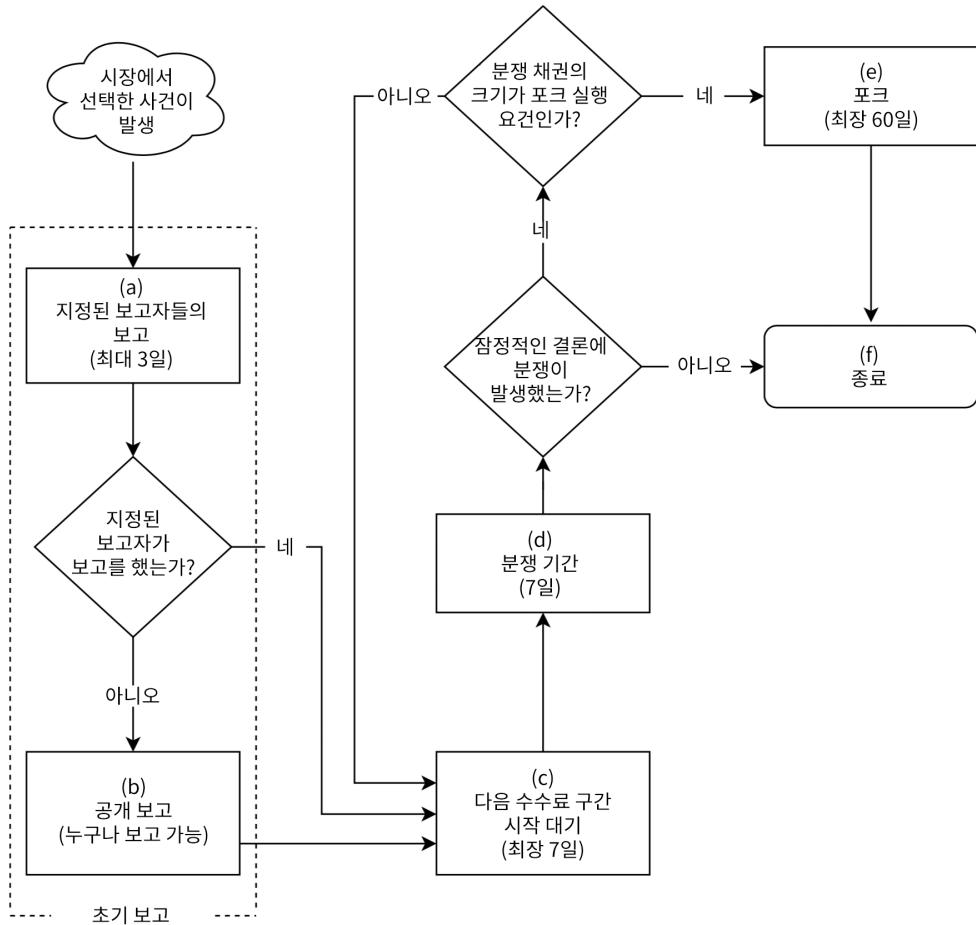


Figure 2. 보고 흐름도.

5. 지정된 보고

시장을 개설할 때, 개설자는 지정된 보고자를 선정하고 미이행 채권을 발행해야 한다. 지정된 보고의 단계 (Fig. 2a)에서 선정된 보고자들은 최장 3일 동안 결과를 보고해야 한다. 지정된 보고자들이 보고를 행하지 않을 경우 개설자의 미이행 채권은 몰수되며, 시장은 자동으로 공개 보고(open reporting)의 단계(Fig. 2b)로 전환된다.

만약 지정된 보고자들이 기간 내 보고를 마치면, 미이행 채권은 개설자에게 환원된다. 지정된 보고자들은 지정된 보고를 위해 지분 참여⁸를 하며, 이 지분은 보고자가 보고한 결과와 다른 결과가 선택될 경우 몰수된다.⁹ 지정된 보고자들의 보고가 끝나면, 시장은 다음 수수료 구간을 위한 대기(waiting for the next fee

window to begin)의 단계(Fig. 2c)로 접어들고, 보고된 결과는 시장의 잠정적인 결과(tentative outcome)가 된다.

6. 공개 보고

지정된 보고자들이 3일 내에 보고를 행하지 못하면 시장 개설자의 미이행 채권은 몰수되며, 시장은 공개 보고(open reporting)의 단계(Fig. 2b)로 진행된다. 시장이 공개 보고의 단계에 접어들면, 누구나 시장의 결과를 보고할 수 있다. 이 경우, 가장 처음으로 공개 보고를 행하는 이를 최초의 공개 보고자(first public reporter)라 한다.

⁸Appendix E 3 참조

⁹몰수된 지분은 현재 수수료 구간 중 보고 수수료 저장소에 보관되

며 분쟁에 성공한 이들과 정직한 보고자들을 위한 보상에 사용된다; 섹션 ID 3에 설명되어 있다.

최초의 공개 보고자는 몰수된 미이행 채권을 선택한 결과에 따라 지급 받는다. 즉, 보고된 결과가 시장의 최종 선택 결과와 일치할 경우에만 미이행 REP 채권을 받는 것이다.

최초의 공개 보고자가 결과를 보고할 때는 REP를 통해 지분 참여할 필요는 없다. 때문에 지정된 보고의 단계가 실패한 경우 최대한 빠른 시간안에 공개 보고가 이루어질 수 있다.

*초기 보고(initial report)*의 단계에서 초기 보고(지정된 보고자이건, 공개 보고자이건)가 행해지면 보고된 결과는 시장의 잠정적인 결과가 되며, 시장은 다음 수수료 구간을 대기하는 단계(Fig. 2c)로 진입한다.

7. 다음 수수료 구간 대기

시장이 초기 보고의 단계를 지나면, 다음 수수료 구간을 대기하는 단계(Fig. 2c)에 진입한다. 이 기간 동안 현재 수수료 구간이 끝나길 기다린다. 다음 구간이 시작되면, 시장은 분쟁의 단계(dispute round)로 접어든다.

8. 분쟁 단계

분쟁의 단계(Fig. 2d) 7일간 REP 보유자는 누구나 잠정적인 결과에 이의를 제기할 수 있다.¹⁰ (분쟁 단계의 시작 시점의 잠정적인 결과는 REP 보유자들에 의해 분쟁에 성공하지 못할 경우 시장의 최종 결과가 된다.) 분쟁은 시장의 잠정적인 결과가 아닌 다른 (*other than*) 결과에 지분 참여(*staking*)하는 형태로 이루어진다(이를 분쟁 지분(*dispute stake*)이라 한다). 만약 특정 결과의 분쟁 지분이 요구되는 분쟁 채권 크기(*dispute bond*)에 달하면, 분쟁은 성공(*successful*) 한다. 요구되는 분쟁 채권 크기는 다음과 같이 계산된다.

A_n 분쟁 회차 n 의 모든 결과에 대한 지분 총액이라 하자. ω 는 이번 분쟁 회차의 잠정적인 결과가 아닌 다른(*other than*) 결과이다. $S(\omega, n)$ 은 결과 ω 가 이번 분쟁 회차에 가진 총 지분량이라 한다. 그러면, 분쟁이 성공하기 위한 분쟁 채권의 전체 크기 $B(\omega, n)$ a는 다음과 같이 기술할 수 있다:

$$B(\omega, n) = 2A_n - 3S(\omega, n) \quad (1)$$

채권의 크기는 위와 같이 잘못된 결과에 대한 분쟁에 성공한 보고자에게 투자수익률(ROI) 50%를 보장하는 형태로 계산된다. (섹션 IID 참조).

¹⁰ 분쟁기간과 수수료 구간이 일치하는 것은 논의의 편의를 위한 것이다; 기본적으로 분쟁 단계와 수수료 구간의 기간은 다를 것이다.

분쟁 채권은 한 명의 사용자가 지불할 필요는 없다. 어거 플랫폼은 여러명이 분쟁 채권을 조성할 수 있도록 허용한다. 잠정적 결과가 잘못되었다고 판단하는 사용자는 누구나 REP를 통해 지분 참여하여 조성할 수 있다. (잠정적 결과가 아닌) 어떤 결과라도 충분한 분쟁 채권이 조성되면, 잠정적 결과를 뒤집는 분쟁은 성공한다.

분쟁이 성공하면 시장은 다른 분쟁의 단계로 접어들거나, 포크(*fork*) 단계 (Fig. 2e)로 진입한다. 만약 분쟁 채권이 전체 REP의 2.5%보다 크면, 포크 단계가 진행된다. 반면 전체 REP의 2.5% 보다 작으면 새로 선택된 결과가 잠정적 결과가 되며 다시 분쟁의 단계가 시작된다.

모든 분쟁 채권은 분쟁기간동안 에스크로 된다. 분쟁에 실패하면 해당 채권은 최종 분쟁 단계의 소유자에게 환원된다. 7일간의 분쟁 기간동안 분쟁이 발생하지 않으면 시장은 종료(*finalized*)의 단계(Fig. 2f)로 들어가며, 잠정적인 결과는 최종 결과(*final outcome*)로 받아들여진다. 즉, 최종 결과는 어떠한 분쟁에도 살아남고, 포크도 되지 않는 잠정적인 결과를 뜻한다. 어거 플랫폼은 최종 결과를 진실(*truth*)로 받아들여 결산하게 된다.

분쟁에 성공하지 못한 모든 채권은 분쟁 최종단계에서 원 소유자에게 환원된다. 분쟁에 성공한 채권은 시장이 종료되기까지(혹은 다른 어거 시장으로 포크될 때까지) 보관되어 최종 결과보고의 지분으로 사용된다. 모든 분쟁 채권(성공했건 성공하지 못했건 간에) 수수료 구간에 조성된 수수료(*reporting fee pool*)¹¹의 일정 부분을 받게 된다.

9. 포크

포크(Fig. 2e)는 60일 동안 진행되는 특수한 단계이다. 포크는 시장이 해결의 최후의 보루다; 매우 꺼려운 방식이고 흔히 발생하지는 않을 것이다. 포크는 분쟁 채권이 전체 REP의 2.5% 이상일 때 발생한다. 이러한 시장을 포크 시장(*forking market*)이라 한다.

포크가 시작되면, 60일¹²간의 포크 기간(*fork period*)동안 포크 단계가 진행된다. 다른 모든 완결되지 않은 시장은 포크 기간동안 해결되지 않고 남게된다. 포크 단계의 기간동안 REP 보유자와 서비스 제공자(지갑이나 거래소)에게 충분한 준비 시간을 부여해야 하기 때문에 일반적인 수수료 구간 보다 길다. 포크를 통한 최종 결과는 분쟁의 대상이 되지 않는다.

¹¹ 수수료 구간 중 수집된 청산 수수료와 유효 채권은 보고 수수료 저장 공간에 보관된다. 수수료 구간이 끝나면 보고 수수료 저장소는 수수료 구간 중 지분 참여한 REP의 비율에 따라 사용자에게 보상을 지급한다.

¹² 포크 기간은 60일 보다 짧을 수 있다: 포크 기간은 60일 이 경과하거나, 50% 이상의 제네시스 REP가 특정 자식 공간에 이전될 때까지 지속된다.

어거의 모든 시장과 REP 토큰은 어떤 공간(*universe*)에 존재한다. REP 토큰은 결과를 보고하는데 사용되며(이를 통해 수수료 수익을 얻고), 이는 REP와 같은 공간에 속한 시장에 한한다. 어거가 처음 공개되면 모든 시장과 REP는 제네시스 공간(*genesis universe*)에 함께 속해있다.

시장이 포크되면, 새로운 공간이 생성된다. 포크는 가능한 결과별로 새로운 자식 공간(*child universe*)을 만든다 (섹션 ID 2에서 설명한 무효인 것을 포함하여). 가령 선택지가 두 개인 “이진” 시장이 3개의 가능한 결과가 있다고 하자: A, B 그리고 무효. 이진 포크 시장은 세 가지 새로운 자식 공간을 만든다: A 공간, B 공간 그리고 무효의 공간. 초기에 이 세 공간은 비어있다: 어떠한 예측 시장, REP 토큰도 포함하고 있지 않다.

포크가 실행되면, 부모 공간(*parent universe*)은 영원히 잠긴(*locked*) 상태가 된다. 잠긴 공간은 새로운 시장이 생성될 수 없다. 사용자들은 잠긴 공간에서도 거래하는 것이 가능하고, 초기 보고를 받을 수도 있다. 그러나 보고에 대한 보상은 지급되지 않으며, 시장이 종료되지도 않는다. 시장과 REP 토큰이 유효하려면 일단 자식 공간으로 이전하여야 한다.

REP 보유자는 부모 공간에서 자식 공간으로 토큰을 이전하는 선택을 할 수 있다. 이전은 한 방향으로만 이루어지기 때문에 신중히 선택해야 한다; 원래대로 복구하는 것은 불가능하다. 같은 형제 레벨의 공간으로 토큰을 이전할 수는 없다. 이전은 특정 결과의 공간으로 REP 토큰을 영원히 보내는 선택이다. 다른 자식 공간으로 보내진 REP 토큰과는 별개의 것으로 취급된다. 지갑이나 거래소 등의 서비스 제공자의 경우도 마찬가지이다.

포크가 시행되면 이전에 지분 참여된 모든 REP는 참여가 취소되어(*unstaked*) 포크 기간동안 자식 공간으로 이전이 가능하게 된다.¹³

포크 기간이 종료되고 가장 많은 REP가 이동한 공간이 승자 공간(*winning universe*)가 된다. 그리고 이 공간이 선택한 결과가 최종 결과가 된다. 부모 공간에 존재하던 미결 시장은 모두 승자 공간으로 이전된다. 만약 최초 보고가 완료된 시장이면 다음 수수료 구간을 기다리게 된다.

부모 공간에서 자식 공간으로 토큰을 이동하는 것에 제한된 시간은 없다. 토큰은 포크 기간이 종료된 후 이전되지만, 항상 승자 시장으로 향하지는 않는다. 포크 기간동안의 참여율을 높이기 위해, 60일 포크 기간 내에 REP를 이동한 이들은 5%의 추가 REP를 받는다¹⁴. 이 보상은 새로 발행된 REP 토큰으로 주어진다.¹⁵

포크 시장의 결과에 REP 지분 참여한 보고자들은 자신이 참여한 결과를 포크 기간동안 변경할 수 없다. 하나의 결과에 지분 참여된 REP는 해당 결과의 자식 공간으로만 이전이 가능하다. 예를 들어, 분쟁에 참여하여 A 결과에 지분 참여한 경우 포크된 A 공간으로만 이전할 수 있다.

형제 공간은 완전히 별개이다. 각 공간의 REP는 다른 공간의 사건에 보고를 하거나 보상을 받는데 사용할 수 없다. 아마도 사용자들은 신뢰할 수 없는 오라클이 존재하는 공간에 시장을 개설하고자 하지 않을 것이다. 해당 공간의 REP는 현실을 반영할 수 없으므로 어떠한 가치도 지니고 있지 않다. 이는 중요한 보안의 요소이며 섹션 II에서 자세히 다루도록 하겠다..

10. 종료

시장이 분쟁이 성공하지 않거나, 포크의 단계에 들어가지 않으면 종료 단계(*Fig. 2f*)로 진행된다. 포크를 통한 결과는 분쟁의 단계를 거치지 않고 최종 결과로 받아들여진다. 시장이 종료되면 거래자들은 시장을 통해 청산이 가능하다. 시장이 종료의 단계에 들어가면 선택된 결과를 최종 결과(*final outcome*)라 한다.

D. 시장 청산

거래자는 자신이 보유한 증권을 거래를 통해 다른 거래자에게 팔거나, 시장을 통해 청산될 때까지 기다릴 수 있다. 어거에 의해 1 ETH가 에스크로 되었던 상황을 다시 떠올려보자. ⁶ 에스크로 된 이 1 ETH를 돌려받으려면, 거래인은 어거에 해당 결과에 해당하는 증권의 전체 총량을 지불하거나, 시장이 종료된 이후 승자 결과로 선택되어야 한다. 이 거래가 발생하면, 우리는 시장 계약에 의해 거래가 청산되었다고 한다.

예를 들어, A와 B 결과가 가능한 종료되지 않은 시장이 있다고 하자. Alice는 A 결과의 주식을 0.7 ETH에 팔고자 하고, Bob은 B 결과의 주식을 0.3 ETH에 팔고자 한다. 우선 어거는 이 거래를 조합하여 A와 B의 주식을 수집한다. 그리고 0.7 ETH(마이너스 수수료)를 앤리스에게, 0.3 ETH(마이너스 수수료)를 Bob에게 지급한다.

두번째로 A 결과가 승자가 된 시장을 가정해보자. Alice는 A 주식을 보유하고 있고 이를 출금하고자 한다. Alice는 A 결과의 주식을 어거에 보내고 1 ETH(마이너스 수수료)를 받는다

¹³유일한 예외는 REP 지분 참여한 이가 초기 보고를 했을 경우다. 이 REP는 승자 공간인 자식 공간으로 자동으로 이전된다.

¹⁴이 현상은 특정 자식 공간으로 50% 이상의 REP가 이전하여 포크가 일찍 종료될 경우에 발생한다.

¹⁵이로 인해 REP 통화 공급량의 증가 효과는 그리 크지 않다. 가령 20%의 REP가 이전한다면 이로 인해 발생하는 REP 공급량 증가

는 1%에 지나지 않는다. 그리고 무엇보다 포크는 거의 발생하지 않는 일이다.

1. 청산 수수료

어거가 추가 수수료를 부과하는 경우는 시장 계약에 의해 청산이 진행될 때이다. 청산 과정에서 어거는 두 종류의 수수료를 부과한다: 개설자 수수료와 보고 수수료이다. 이 수수료는 모두 청산 금액의 일정 비율의 형태이다. 청산이 진행되지 않은 위의 예에서 Alice는 0.7 ETH, 밥은 0.3 ETH를 받는다. 결국 Alice는 70%를, Bob은 30%를 받는 셈이다.

개설자 수수료는 시장 개설자에 의해 결정되며, 청산 과정에서 개설자에게 지급된다. 보고 수수료는 동적(섹션 II C 참조)으로 결정되어 보고 과정에 참여한 보고자들에게 지급된다.

2. 무효처리된 시장의 청산

시장이 무효 처리되면, 거래자들은 각 결과에 모인 ETH를 동일한 양으로 분배받게 된다. 만약 시장이 N 개의 가능한 결과(무효 처리된 경우를 제외하고)가 있고 전체 발행량이 C ETH라면 거래자는 시장이 청산되는 시점에 C/N ETH를 받게 된다.¹⁶

3. 평판의 재분배

만약 시장이 포크 없이 종료되면, 시장이 선택한 최종 결과가 아닌 다른 결과에 기반 참여된 모든 REP는 몰수되어 분배된다. 분쟁에 성공한 이들은 분쟁 채권에 참여한 지분 중 50% 투자수익률을 기준으로 보상받게 된다 정리 3 Appendix A 참조. 이는 잘못된 잠정 결과를 분쟁으로 유도하는 효과적인 유인책이 된다.

II. 유인책과 보안

REP의 시가총액과 어거의 포크 프로토콜의 신뢰도는 긴밀한 관계에 있다. REP의 시가총액이 충분하고¹⁷, 공격자가 경제적으로 합리적이라면, 포크의 승자가 되는 결과는 현실을 반영할 것이다. 사실, 어거는 지정된 보고자들과 분쟁의 단계가 없어도 작동이 가능하다. 포크 단계만 존재하더라도, 오라클은 진실된 결과를 보고할 것이다.

하지만, 포크는 번거롭고 시간 소요가 많다. 포크는 60일이나 소요되며, 한번에 하나의 시장만 해결이 가능하다. 하나의 시장이 해결되는 60일 동안 종료되지

않은 다른 시장은 대기 상태가 된다.¹⁸ 서비스 제공자는 업데이트를 해야하며, REP 보유자는 새로운 자식 공간으로 REP를 이전해야 한다. 그러므로 포크는 정말 필요한 경우에만 사용되어야 한다. 마치 포크는 핵(nuclear) 옵션과도 같다.

다행히도, 포크가 진실로 향할 것이라는 신뢰가 형성되면, 참여자들로 하여금 진실되게 행동하여 포크가 발생하지 않도록 행동하게 하는 일종의 동기부여가 된다. 이는 포크가 정상적으로 진행된다는 신뢰를 바탕으로 한 암묵적인 선의의 협박이며, 어거의 보상 시스템의 주춧돌이 된다.

다음으로 포크 시스템이 진실로 향하는 조건에 대해 살펴보겠다. 그리고 보상시스템과 이 시스템이 어떻게 시장을 빠르고 정확하게 해결하도록 유도하는지 살펴보자.

A. 포크 프로토콜의 무결성

이제 포크 절차의 진실성과 이 과정이 신뢰할 수 있는지 살펴보자. 포크로 인해 이동되는 자식 공간은 참의 공간이라 하고 이 외의 다른 자식 공간은 거짓의 공간이라 하자. 가장 많은 REP가 이동하는 공간을 승자 공간이라 하고, 이를 제외한 공간은 패자 공간이라 한다.

기본적으로, 우리는 참의 공간이 승자 공간이 되고, 거짓의 공간이 패자 공간이 되길 원한다. 거짓의 공간 중 하나가 승자 공간이 되는 것을 공격이 성공했다고 하며, 이는 포크 시장(잠재적인 모든 미결 시장을 포함하여)이 부정확한 지불을 행한 것이다 된다.

안전한 오라클을 위해 우리는 성공한 공격자가 가져가는 수익이 공격을 행하는 최소 비용을 넘지 못하도록 만들 필요가 있다. 이 방식은 아래와 같다.

1. 공격자가 취할 수 있는 최대 수익

오라클 공격에 성공한 공격자는 모든 미결 예측 시장을 거짓의 공간으로 보내게 된다. 만약 공격자가 거짓의 공간에서 REP의 과반이상을 점유한다면, 공격자는 모든 미결 시장을 원하는 결과가 선택되도록 만들 수 있다. 가장 극단적인 경우, 공격자는 모든 시장의 에스크로 된 자금을 가져가고자 할 것이다.¹⁹

정의 1. I_a 를 어거의 원(原) 미청산계약(native open interest), 즉 종료되지 않은 시장에 에스크로 된 자금의 총 합이라 한다.²⁰

¹⁶기술적인 제약으로 인해 시장이 무효화되더라도 거래가 간단히 풀리지는 않는다. 결과에 따른 주식은 단순한 토큰이며 사용자들 간에 직접 거래될 수 있다. ETH와 이러한 주식은 어거의 통제 하에 있지 않으며 마켓이 무효화되었다고 하여 원 소유주에게 돌려줄 수는 없다.

¹⁷섹션 II A에서 자세히 설명하도록 한다.

¹⁸해당 시장에서 거래는 지속할 수 있으나 포크 기간이 끝나기 전까지 종료될 수는 없다.

¹⁹이는 공격자로 하여금 해당 결과로 시장을 종료하기 위해 모든 주식을 소유하도록 만든다.

²⁰이는 어거에 보고 수수료를 지불하는 외부 시장을 포함한다.

정의 2. 기생 시장(*parasitic market*)은 원 예측 시장의 결과에 따라 해결되지만, 어거에는 어떠한 보고 수수료도 지불하는 않는 시장을 뜻한다.

정의 3. I_p 를 어거의 원 예측 시장 결과에 따라 해결되는 기생 시장의 총 미청산계약(*parasitic open interest*)이라 한다.

가장 극단적인 경우 공격자는 기생시장의 전체 자금 또한 차지할 수 있다.

고찰 1. 성공적으로 오라클을 공격한 공격자의 최대(총) 수익은 $I_a + I_p$ 이다..

2. 예측 불가능한 기생 시장의 총 미청산계약

어거 시스템은 정확하고 효율적으로 I_a 를 측정할 수 있다. 하지만 오프라인 기생시장은 얼마든지 많이 존재할 수 있으며, 그에 따라 총 미청산계약의 규모도 클 수 있다. 따라서 I_p 를 측정하는 것은 일반적으로 불가능에 가깝다. 공격자의 최대 수익이 I_p 를 포함하고, 이 수치를 알 수 없다면 오라클이 객관적으로 안전하다고 말할 수 없다.

그러나 I_p 를 실질적인 수준에서 합리적으로 추론한다면, 우리는 어떠한 조건을 만들 수 있고, 이 조건 하에 오라클은 안전하다고 할 수 있을 것이다.

3. 공격 성공을 위한 최소의 비용

다음으로, 오라클을 공격하는데 소요되는 비용을 생각해보자. REP의 가격을 P 라 한다. ϵ 는 1 attorep²¹이고, M 은 REP의 총 공급량이다. (the “money supply” of REP). S 는 전체 REP의 총 공급량인 M 중에서 참의 공간으로 이전한 REP의 비율이다.

위와 같이 정의하면 SM 은 포크기간 중 참의 공간으로 이동한 REP의 총 수량이며, PM 은 REP의 시가 총액이다.

P_f 를 공격자가 선택한 거짓의 공간으로 이동한 REP의 가격이라 하자. 만약 $P \leq P_f$ 이면 오라클은 합리적인 경제관념을 가진 공격자로부터 안전하다. 거짓의 공간으로 REP를 이전하는 것은 오히려 손실을 입는 행동이므로 그렇게 행동하지 않을 것이기 때문이다.

4. 무결성

가정 1. 포크의 단계에서 공격자가 아닌 보고자는 절대로 REP를 거짓의 공간으로 이전하지 않는다고 가

정하자.²²

포크 기간동안 공격에 성공하기 위해서는 참의 공간보다 거짓의 공간으로 이전하는 REP가 더 많아야 한다. 위에 정의한 가정에 의해 거짓의 공간으로 REP를 이전하는 이는 공격자 뿐이다. 참의 공간으로 이전하는 REP의 총 수량은 SM 이다. 따라서, 공격자가 성공하기 위해서는 최소한 $SM + \epsilon$ REP가 필요하다. 무시해도 될 수준의 ϵ 를 제거하면 최소한 SM REP를 필요로 하며, 이전하기 전의 가치는 SMP 로 계산할 수 있다.

만약, 공격자가 SM REP를 포크기간동안 이전하면, 자식 공간에서 SM 를 받게 된다.²³ 거짓의 공간에서 이는 SMP_f 만큼의 값어치를 지니게 된다. 따라서 공격자의 최소 비용은 $(P - P_f)SM$ 이다.

고찰 2. 공격의 성공을 위해 거짓의 공간으로 이전해야하는 REP의 최소 수량은 SM 이며, 이로 인해 공격자가 부담해야 하는 비용은 $(P - P_f)SM$ 이다.

만약 $S > \frac{1}{2}$ 라고 하면, 공격자는 참의 공간보다 거짓의 공간으로 이전하기 위해 충분한 REP를 보유할 수 있으므로, 공격은 불가능하다.

공격을 성공해서 얻을 수 있는 수익보다 소요되는 비용이 많다면, 합리적인 경제관념의 공격자이므로 객관적인 사실을 보고하는 오라클을 안전하게 유지할 수 있다. 고찰 1 & 2에 따르면, $S > \frac{1}{2}$ 이거나 $I_a + I_p < (P - P_f)SM$ 이면 이 조건은 유지된다. 이 수식을 통해 무결성을 확인할 수 있다.

정의 4. (무결성 속성) 포크 프로토콜은 $S > \frac{1}{2}$ 이거나 $I_a + I_p < (P - P_f)SM$ 이면 무결성 상태이다.

위 부등식은 PM 을 기준으로 풀이할 수 있으며, 이를 통해 포크 프로토콜의 무결성과 REP 시가 총액과의 상관관계를 살펴볼 수 있다.

정리 1. (시가 총액 안정성 정리) 포트 프로토콜은 아래 조건을 만족하는 한 무결성 상태이다:

$$1. S > \frac{1}{2}, \text{ 이거나}$$

$$2. P_f < P \text{ 이고 } REP \text{ 시가총액이 } \frac{(I_a+I_p)P}{(P-P_f)S} \text{ 보다 클 경우이다.}$$

²²악의가 없음에도 실수나 부주의로 거짓의 공간에 REP를 이전하는 보고자도 있을 수 있다. 하지만 이 행위가 공격자와 협력하는 것인지 아닌지를 구별할 방법은 없다.

²³사실 공격자는 1.05SM REP에 해당하는 REP를 자식 공간에서 받게된다. 60일 포크 기간 내에 이전하면 5%의 추가 REP를 받기 때문이다. 5%의 보너스는 논의의 편의를 위해 고려하지 않았다. 5%를 포함한 논의에 대해 살펴보려면 Appendix C를 참조하기 바란다.

²¹1 attorep은 10^{-18} REP이다.

Proof. 만약 포크 프로토콜이 무결성 상태라고 하자. 그렇다면 정의한 바에 의해, $S > \frac{1}{2}$ 이거나 $I_a + I_p < (P - P_f)SM$ 이다. $I_a + I_p < (P - P_f)SM$ 라 가정하자. $I_a + I_p \geq 0$ 이고 $SM > 0$ 인 상태에서 $P_f < P$ 임을 알고 있다. $I_a + I_p < (P - P_f)SM$ 를 PM 을 기준으로 정리하면, $\frac{(I_a + I_p)P}{(P - P_f)S} < PM$ 임을 확인할 수 있다. 이를 통해 첫 번째 조건은 증명이 가능하다.

이제 $S > \frac{1}{2}$ 이거나 $P_f < P$ 이고 $\frac{(I_a + I_p)P}{(P - P_f)S} < PM$ 이라 가정하자. 만약 $S > \frac{1}{2}$ 라면 포크 프로토콜은 가정에 의해 무결성 상태이다. 만약 $P_f < P$ 이고 $\frac{(I_a + I_p)P}{(P - P_f)S} < PM$ 이라면 $I_a + I_p$ 를 기준으로 부등식을 풀면, $I_a + I_p < (P - P_f)SM$ 이다. 따라서 포크 프로토콜은 무결성 상태임을 알 수 있다. \square

B. 추정과 그에 따른 결과

우리는 보고자들이 거짓을 보고하는 어거 공간에서 거래하고자 하는 사용자는 없을 것이라 생각한다. 그리고, 거래자들이 존재하지 않는 공간에 예측 시장을 개설하고자 하는 개설자 또한 없을 것이라 생각한다. 시장과 거래자가 없는 공간에서 REP는 어떠한 수익도 창출할 수 없다. 그러므로 거짓의 공간으로 이전한 REP는 유의미한 가치를 가지지 못하며 이를 $P_f = 0$ 으로 표현할 수 있다.

포크 기간동안 최소 20%의 REP는 진실을 선택한 공간으로 이전한다고 합리적으로 추론할 수 있다. 이를 통해 $S \geq \frac{1}{5}$ 이다. 기생 시장의 미청산계약을 어거의 예측 시장의 최대 50% 정도라 하면, 이를 통해 $I_a \geq 2I_p$ 를 도출할 수 있다.

이 가정에 의거하여, 가정 1을 살펴보면, 어거 시가 총액이 어거 시장 미청산계약의 7.5배 이상이면 포크 프로토콜은 무결성을 유지한다는 것을 알 수 있다.²⁴

C. 시가 총액 도달

어거는 REP 가격 정보 또한 다른 실제 세계의 정보를 얻는 방식과 같은 형태로(어거 예측 시장을 통해) 받아온다. 이를 통해 어거는 REP 시가 총액을 계산할 수 있다. 또한 미청산계약을 계산할 수 있으므로 어거의 무결성 유지를 위해 필요한 시가 총액을 계산할 수 있다.

모든 공간은 기본 보고 수수료 1%에서 시작한다. 만약 현재 시가 총액이 기준보다 낮다면, 보고 수수료는 자동으로 올라가고(하지만 33.3%를 넘지는 못한다.) 이는 REP의 가격 상승 요인과 신규 미청산채권의 생성을 억제하는 효과 중 최소 하나의 효과를 가져온다.

만약 현 시가 총액이 목표보다 높으면, 보고 수수료는 자동으로 내려가고(0.01% 보다 작을 수는 없다) 이로 인해 거래자는 시스템 안정화를 위한 비용을 덜 지불하게 된다.

보고 수수료는 다음과 같이 예측할 수 있다. r 을 직전 수수료 구간의 보고 수수료라 하고 t 를 목표 시가총액이라 하며 c 는 현재 시가 총액이다. 그렇다면 현재 수수료 구간의 보고 수수료는 $\max \left\{ \min \left\{ \frac{t}{c}r, \frac{333}{1000} \right\}, \frac{1}{10,000} \right\}$ 와 같다.

D. 포크의 위협에 대한 레버리지

앞서 언급했듯이, 포크는 번거롭고 느린 시장 해결 수단이다. 때문에 어거는 포크의 형태로 시장을 해결하지 않고, 포크의 위협(threat)에 대해 지렛대 효과(leveraging)를 사용하는 방식으로 시장의 효율성을 유지한다.

분쟁에 성공하여 시장의 최종 결과로 받아들여진 지분은 분쟁지분의 50% 투자수익률에 달하는 보상을 받는다고 했던 것을 상기해보자.²⁵ 포크의 단계에서 참의 결과에 지분 참여한 REP는 자식 공간에서 50%의 보상을 받게 되는 반면, 거짓 결과에 지분 참여한 REP는 모두 잃게 된다. 그러므로 만약 포크가 발생한다면, 거짓의 결과에 참여한 REP 보유자들의 REP 가치가 없어지는 반면, 거짓 결과에 분쟁 참여하여 참의 결과를 선택한 이들은 항상 더 나은 수익을 얻게 된다.

우리는 이 상황이 잠정적인 결과가 거짓일 경우 분쟁이 성공할 것이라 믿기에 충분한 조건이라 확신한다.

III. 잠재적인 문제와 취약점

A. 기생 시장

기생 시장은 보고 수수료를 지불하지 않지만 어거의 원 시장을 통해 결과를 해결하는 시장을 뜻한다고 하였다. 기생 시장 내에는 보고 수수료를 보상으로 받는 보고자가 존재하지 않기 때문에, 같은 서비스를 어거보다 저렴한 비용으로 제공할 수 있다. 이는 어거의 포크 무결성에 심각한 영향을 끼칠 수 있다.

만약 기생 시장으로 계약이 몰리게 되면, 어거의 보고자들은 보상으로 받는 보고 수수료 수익이 줄어들게 된다. 이는 REP 시가 총액의 하락 요인이 된다. 만약 REP 시가 총액이 지나치게 낮은 수준으로 떨어지면, 포크 무결성은 위태롭게 된다(정리 1). 결과적으로, 기생 시장은 어거의 시장에 장기적, 잠재적 불안요소 이므로 배척되어야 한다.

²⁴ Appendix B에 몇 가지 변형된 가정과 그 결과에 대해 기술하였다.

²⁵ 시장의 최종 결과에 속한 공간의 REP 중에서 측정한 값이다; Appendix A의 정리 3 참조

기생 시장의 위협으로부터 어거를 보호하는 가장 좋은 방법은 기생 시장에 매력을 느낄 수 없도록, 어거 플랫폼을 (오라클의 무결성을 유지하는 한도 내에서) 가능한 저렴한 수수료로 이용할 수 있도록 만드는 것이다.

B. 미청산약정의 변동성

미청산약정의 크고, 갑작스럽고, 예기치 못한 증가 – 유명한 스포츠 경기에 대한 시장에서 일어나기 쉬운 – 는 포크 무결성을 유지하기 위한 시가 총액의 목표치를 급속도로 증가시킨다 (정리 1). 시가 총액 요구량이 시가 총액을 급격하게 추월하면, 경제적으로 합리적인 공격자가 잘못된 방식으로 시장을 포크할 수 있는 위험한 상황에 처하게 된다. 이와 같은 목표 시가 총액의 증가는(섹션 II C 참조) 다음 7일 이내에 변화되는 수수료 구간에 영향을 미치게 된다.

이는 큰 의미가 없다고 볼수 있으나, 미청산약정의 급증을 확인한 관찰자는 시장이 반응할 것을 예측하고 REP를 구입할 것이다. 이를 통해 REP 가격은 증가하고, 다시 무결성은 위협을 받지 않게 된다. 그러므로 실제 오라클을 공격할 수 있도록 공격자에 주어진 시간은 그리 길지 않다.

C. 모순되거나 악의적인 단서

시장을 개설할 때, 개설자는 보고자들이 결과를 판단하기 위해 사용할 단서를 제공해야 한다. 만약 개설자가 악의적이거나 모순된 단서를 선택하면, 정직한 보고자는 손해를 볼 수 있다.

예를 들어, A와 B의 결과가 가능한 예측 시장이 있다고 하자. 시장 개설자인 Serena는 자신이 직접 운영하는 [attacker.com](#)을 결과 판단을 위한 단서로 설정했다. 시장이 기준으로 하는 사건이 발생한 뒤 개설자이자 지정된 보고자 중 하나인 Serena는 A 결과를 보고하는 동시에 자신의 웹사이트 [attacker.com](#)에는 결과 B를 선택하도록 단서로 입력한다. [attacker.com](#)을 확인한 다른 정직한 보고자들은 최초의 결과보고가 잘못되었다고 보고하고 시장은 첫 번째 분쟁 단계로 돌입하여 결과적으로 분쟁에 성공할 것이다. Serena는 다시 자신의 웹사이트 [attacker.com](#)에 결과 A를 가리키도록 업데이트 한 다음 분쟁에 돌입한다. 다시, 보고자들은 웹사이트를 확인하고 기존의 잠정적 결과였던 B가 틀렸다고 보고하여 분쟁에 또 성공하게 된다. Serena는 이 행동을 시장이 해결될 때까지 계속 반복할 수 있다. 이 경우, 어떤 결과로 해결이 되더라도 정직한 보고자들은 손해를 보게 된다.

몇 가지 다른 방식의 공격도 가능하다. 단순히 의심스러운 해결원을 제공한 시장을 무시하는 것만으로는 부족하다. 이러한 상황이 포크를 유발한다면, 모든 REP 보유자는 REP를 이전할 자식 공간을 선택해야

한다. 보고자들은 의심스러운 해결원을 제시한 시장에 유의할 필요가 있다. 이런 류의 시장은 보고자들이 협심하여 무효 처리할 필요가 있다.

D. 자기지시적 오라클 질의

어거 오라클 자체의 미래 행동을 기준으로 삼는 예측 시장은 오라클의 예기치 않은 행동을 가져올 수 있다 [11]. 가령 다음과 같은 질문을 기준으로 한 예측 시장을 생각해보자, “지정된 보고자들 중 누구도 2018년 12월 31일 전 3일간의 지정된 보고 단계에 답을 하지 않을 것인가?”. 아니오 결과에 투자하는 것은 지정된 보고자들이 고의로 지정된 보고를 누락하는 비뚤어진 행동을 야기할 수 있다. 만약 지정된 보고자들이 네 주식을 낮은 가격으로 충분히 많이 살 수 있어, 이로 인한 이익이 미이행채권의 보상보다 크다면 이들은 고의적으로 보고를 누락할 것이다.

만약 REP 시가총액이 충분히 큰 상태라면(정리 1) 이러한 자기지시적 오라클 질의는 포크 프로토콜의 무결성을 위협하지 않는다. 하지만 이는 시장의 종료를 지연시켜 어거에 부정적인 영향을 끼칠 수 있다. 시장이 정상적으로 종료되더라도 이러한 행태는 껄끄럽고 불편한 일이다.

E. 포크 참여의 불확실성

포크 기간동안 얼마나 많은 REP가 참의 공간으로 이동할 것인지는 알 수 없다. 때문에 오라클의 무결성을 위한 REP의 시가총액도 알 수 없게 된다(정리 1). 포크 프로토콜의 무결성에 대한 신념은 최소한 정직한 참여자의 수량을 넘지는 않을 것이다. 전체 REP 수량 중 적어도 20%가 참의 공간으로 이전할 것이라 가정하지만 장담할 수는 없다.

어거의 포크는 블록체인의 포크와 한가지 다른 특성이 있다. 블록체인의 포크에서 코인 소유자는 포크 이후 부모 체인과 포크 체인 모두에 코인의 소유권을 가진다. 리플레이 어택을 제외하면 소유자에게 그다지 위험이 없는 방식이다. 반면, 어거의 포크는 부모 공간에서 단 하나의 자식 공간으로만 REP를 이전할 수 있다. 따라서 합의되지 않은 자식 공간으로 REP를 이전한 보유자는 모든 가치를 잃게 된다. 때문에 협의가 이루어진 공간을 확인할 수 없는 상태에서 REP를 이전하는 것은 굉장히 위험한 일이다. 이 위험은 포크 기간 동안의 참여를 저해하는 요소가 된다.

이러한 위험을 감수하고 참여하는 것에 대한 보상으로 60일 이내에 REP를 이전하는 보유자들에게 5%에 해당하는 추가 REP를 자식 공간에서 부여한다(섹션 IC9 참조). 그럼에도 5%의 추가 보너스가 위험을 감내하는 것에 대한 충분한 보상인지는 알 수 없다.

F. 모호하거나 주관적인 시장

결과를 객관적으로 판단할 수 있는 사건만이 어거에 적합한 예측 시장의 기준이 될 수 있다. 만약 보고자들이 플랫폼을 통해 해결이 어렵다고 – 가령 모호하거나, 주관적이거나, 지정된 시간에 결과를 알 수 없는 등 – 판단한다면 이들은 시장을 무효라고 보고할 것이다. 시장이 무효로 판명나면, 거래자들은 모든 가능한 결과에 동일한 비율로 분배를 받게 된다. 만약 스칼라 시장일 경우 최대값과 최소값의 중간지점을 기준으로 청산하게 된다.

어떤 이들은 결과를 A라 판단하고, 또 어떤 이들은 결과를 B라 판단하는 시장도 발생할 수 있다. 실제 2006년에 TradeSports는 북한이 2006년 7월 말까지 탄도 미사일 발사에 성공할 것인지를 예측 시장으로 열었다. 2006년 7월 5일에 북한은 실제로 탄도 미사일 발사에 성공했고, 이 사건은 미정부의 다양한 기관과 언론 매체에 의해 확인되었다. 하지만 TradeSports가 기준으로 제시했던 미국방부(U.S. Department of Defense)는 탄도 미사일 발사 성공을 인정하지 않았다. Trade-

Sports는 결국 탄도 미사일은 발사되지 않은 것을 기준으로 해당 시장을 청산하였다.²⁶

이 시장의 조건 – 미사일 발사 –은 확실히 충족되었지만, 시장에서 기술한 조건 – 미국방성의 발표를 기준으로 한다 –은 충족하지 못했다. TradeSports는 중앙집중화 방식의 웹사이트 이므로 명확하게 하나의 조건을 선택하여 제시할 수 있다. 하지만 만약 같은 일이 어거의 시장에서 발생한다면 REP 보유자들은 다른 선택을 할 수도 있다. 죄악의 경우 포크로 이어질 수도 있으며, 이로 인해 시장 가치가 유지되는 두 개의 자식 공간이 존재할 수도 있다.

ACKNOWLEDGMENTS

Abraham Othman, Alex Chapman, Serena Randolph, Tom Haile, George Hotz, Scott Bigelow, 그리고 Peronet Despeignes에게 그들의 유용한 피드백과, 조언에 감사한다는 말을 전합니다.

-
- [1] J. Wolfers and E. Zitzewitz. Prediction markets. *Journal of Economic Perspectives*, 18(2):107–126, 2004.
 - [2] James Surowiecki. *The Wisdom of Crowds*. Anchor, 2005.
 - [3] R. Hanson, R. Oprea, and D. Porter. Information aggregation and manipulation in an experimental market. *Journal of Economic Behavior & Organization*, 60(4):449–459, 2006.
 - [4] D.M. Pennock, S. Lawrence, C.L. Giles, and F.A. Nielsen. The real power of artificial markets. *Science*, 291:987–988, 2001.
 - [5] C. Manski. Interpreting the predictions of prediction markets. *NBER Working Paper No. 10359*, 2004.
 - [6] J. Wolfers and E. Zitzewitz. Interpreting prediction market prices as probabilities. *NBER Working Paper No. 10359*, 2005.
 - [7] S. Goel, D.M. Reeves, D.J. Watts, and D.M. Pennock. Prediction without markets. In *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, pages 357–366. ACM, 2010.
 - [8] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, 2008.
 - [9] V. Buterin. A next generation smart contract and decentralized application platform. <https://github.com/ethereum/wiki/wiki/White-Paper>, 2013.
 - [10] J. Clark, J. Bonneau, E.W. Felten, J.A. Kroll, A. Miller, and A. Narayanan. On decentralizing prediction markets and order books. In *WEIS '14: Proceedings of the 10th Workshop on the Economics of Information Security*, June 2014.
 - [11] A. Othman and T. Sandholm. Decision rules and decision markets. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: Volume 1 - Volume 1*, AAMAS '10, pages 625–632. International Foundation for Autonomous Agents and Multiagent Systems, 2010.
 - [12] J. Peterson and J. Krug. Augur: a decentralized, open-source platform for prediction markets. *arXiv:1501.01042v1 [cs.CR]*, 11 2014.

²⁶자세한 내용은 <https://en.wikipedia.org/wiki/Intrade#Disputes>를 참조하기 바란다.

Appendix A: 종료 시간 & 분배

몇 가지 선언과 정의, 정리를 기반으로 논리를 전개하도록 하자.

정의 5. 주어진 시장 M 의 결과의 공간(혹은 결과의 모음)을 Ω_M 으로 표기하자.

정의 6. $n \geq 1$ 이고 $\omega \in \Omega_M$ 이면, $S(\omega, n)$ 는 분쟁 단계 n 의 시작 시점에서 결과 ω 에 지분 참여된 총량이다. 이는 이전의 결과 ω 에 찬성하는 모든 분쟁에서 성공한 분쟁 채권의 총지분을 포함한다.

정의 7. $n \geq 1$ 이고 $\omega \in \Omega_M$ 이면, $S(\bar{\omega}, n)$ 는 분쟁 단계 n 의 시작 시점에서 결과 Ω_M except for ω 를 제외한 다른 모든 결과의 지분 참여 총량이다:

$$S(\bar{\omega}, n) = \sum_{\substack{\gamma \in \Omega_M \\ \gamma \neq \omega}} S(\gamma, n)$$

정의 8. $n \geq 1$ 인 상태에서 A_n 을 분쟁 단계 n 의 시작 시점에서 가능한 모든 결과 M 의 지분 참여 총량이라 하자:

$$A_n = \sum_{\omega \in \Omega_M} S(\omega, n)$$

고찰 3. 그렇다면, $A_n - S(\omega, n) = S(\bar{\omega}, n)$ 이다.

정의 9. $n \geq 1$ 인 상태에서, $\hat{\omega}_n$ 은 분쟁 단계 n 의 시작 시점에서의 잠정적인 결과이다. 예를 들어 $\hat{\omega}_1$ 은 최초의 보고자에 의해 보고된 결과이다.

정의 10. $n \geq 1$ 이고 $\omega \neq \hat{\omega}_n$ 인 조건 하에서 $B(\omega, n)$ 는 분쟁 단계 n 에서 결과 ω 에 찬성하여 성공적으로 분쟁 채권을 획득하기 위한 지분의 총량이라 정의한다.

분쟁 단계 n 에서 결과 ω 에 찬성하여 분쟁에 성공하기 위해 분쟁 채권을 채우는데 필요한 지분의 양은 Eq. 1에 따라 $\omega \neq \hat{\omega}_n$ 이므로 $B(\omega, n) = 2A_n - 3S(\omega, n)$ 이다.

고찰 4. 만약 분쟁 단계 n 에서 결과 ω 에 찬성하는 분쟁 채권을 성공적으로 획득한다면, $S(\omega, n+1) = B(\omega, n) + S(\omega, n)$ 이다. 다시 말해, 성공한 분쟁 지분은 분쟁 단계 n 의 종료 시점에서 결과 ω 에 새롭게 지분 참여한 양이다.

고찰 5. $\omega \neq \hat{\omega}_n$ 임에도 불구하고, $S(\omega, n-1) = S(\omega, n)$ 이다. 이는 결과 ω 에 찬성하는 분쟁 채권이 완전히 채워지지 않으면, 다음 분쟁 단계의 시작 시점에서 결과 ω 에 추가되는 지분이 없다는 것과 같다. 이는 실패한 분쟁 지분은 분쟁 단계의 종료 시점에 사용자에게 환원되기 때문이다.

고찰 6. $n \geq 2$ 이더라도 $A_n = A_{n-1} + B(\hat{\omega}_n, n-1)$ 이다. 분쟁 단계 시작 시점의 모든 결과에 대한 총 지분은 이전 분쟁 단계의 시작 시점의 총 지분에 이전 분쟁 단계에 성공한 분쟁 지분을 더한 것과 같다. 다른 모든 지분은 이전 분쟁 단계의 종료 시점에 사용자들에게 환원된다.

보조정리 2. $n \geq 2$ 에 대해서, $S(\hat{\omega}_n, n) = 2S(\bar{\omega}_n, n)$ 이다.

Proof. 만약 시장이 분쟁 단계 n 에 접어들었고 $n \geq 2$ 라고 하자. 단계 $n-1$ 의 결과 $\hat{\omega}_{n-1}$ 는 결과 $\hat{\omega}_n$ 에 찬성하여 분쟁에 성공해야만 한다. Eq. 1에 따라 분쟁 채권의 크기는 $B(\hat{\omega}_n, n-1) = 2A_{n-1} - 3S(\hat{\omega}_n, n-1)$ 이다. observation 3를 통해 아래와 같이 기술할 수 있다.

$$B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = 2S(\bar{\omega}_n, n-1) \quad (\text{A1})$$

우리는 분쟁 채권이 단계 $n-1$ 에서 성공적으로 채워질 것을 알고 있다. 고찰 4를 이용하여, $B(\hat{\omega}_n, n-1) + S(\hat{\omega}_n, n-1) = S(\hat{\omega}_n, n)$ 라는 것 또한 알 수 있다. 고찰 5를 통해, $\hat{\omega}_n$ 에 지분 참여된 총량은 단계 $n-1$ 에서 n 으로 변하고, $2S(\hat{\omega}_n, n-1) = 2S(\hat{\omega}_n, n)$ 라도 변화가 없다. 그러므로, Eq. A1은 $S(\hat{\omega}_n, n) = 2S(\hat{\omega}_n, n)$ 으로 감소 한다. \square

정리 3. 시장의 최종 결과에 찬성하여 분쟁에 성공한 REP 보유자는, 다른 시장이 포크를 유발하지 않는 한 그들의 분쟁 지분 중 50% 투자수익률을 기준으로 보상을 받는다(시장의 최종 결과와 부합되는 공간에 존재하는 REP로 계산한다).

Proof. 포크 시장의 최종 결과에 찬성하여 분쟁 채권을 성공적으로 채운 모든 사용자는 그들이 자식 공간으로 지분 채권을 이전할 때 그들의 지분 채권의 50%를(포크로 새로 생성된 코인으로) 받게 된다. 그러므로 포크를 유발한 시장에서 정리는 참으로 판명된다.

포크 없이 다른 시장의 포크로 간접이 발생하지 않고 자체적인 포크 없이 해결된 시장을 살펴보자.

시장의 최종 결과가 ω_{Final} 이고 $n \geq 2$ 인 보고 단계 n 에서 시장이 해결되었다고 하자. 이는 단계 n 의 잠정적인 결과는 ω_{Final} 임을 뜻하고, 단계 n 에서는 분쟁에 성공하지 못했다고 할 수 있다. 다시 말하면: $\hat{\omega}_n = \omega_{\text{Final}}$ 이라 할 수 있다. 그렇다면 보조정리 2에 의해 우리는 $S(\omega_{\text{Final}}, n) = 2S(\bar{\omega}_{\text{Final}}, n)$ 임을 알 수 있다.

시장이 분쟁 단계 n 에서 다른 어떤 결과에도 추가 지분이 없이 해결되면, 위 등식은 최종 결과, ω_{Final} 의 최종 전체 지분 량이고, 시장의 다른 결과 $\bar{\omega}_{\text{Final}}$ 의 전체 지분 량이다. 다른 모든 결과에 비해 최종 결과는 정확히 두배의 지분량을 가지고 있음을 주목하자.

어거는 ω_{Final} 에 지분 참여한 이들에게 종료되지 않은 결과의 총 지분을 지분 참여한 REP의 비율에 따라 재분배한다. 따라서 ω_{Final} 에 찬성하여 분쟁 채권을 성공적으로 채운 모든 사용자는 지분 참여한 REP의 50% ROI를 받게 된다. \square

다음으로, 시장을 해결하기 위해 필요한 최대 분쟁 단계를 고찰해보자. ω 가 최대 수량의 지분으로 시작하는 분쟁 단계에서 장정적이 아닌 결과로 선택될 경우 Eq. 1은 최소화된다. 보조정리 2는 최대 지분의 잠정적 이지 않는 결과는 이전 분쟁 단계의 잠정적 결과임을 나타낸다. 그러므로, 최소한의 가능한 분쟁 채권의 크기는 $n \geq 2$ 이고, $B(\hat{\omega}_{n-1}, n)$ 이면 분쟁 단계 n 에서 성공적으로 채워질 수 있다.

달리 말하면, 두개의 결과가 다른 하나에 대한 찬성에 의해 반복적으로 분쟁이 시작되면 분쟁 채권의 크기는 가장 느리게 증가한다고 할 수 있다. 시장이 포크되기 위해 필요한 분쟁의 단계는 최대화 된다. 그러므로 어떠한 시장이건 포크를 시작하기 전에 진행되는 분쟁의 최대 단계는 두개의 결과가 다른 하나에 반하여 반복적으로 분쟁이 발생하는 경우가 된다. 이러한 경우를 살펴보도록 하자.

모든 분쟁 채권은 이전 분쟁 단계의 잠정적인 결과에 반하여 발생한다고 가정하자. 그렇다면 두 개의 잠정적인 결과 $\hat{\omega}_1, \hat{\omega}_2$ 가 서로 반복적으로 분쟁을 일으키게 된다.

고찰 7. 두 잠정적인 결과가 반복적으로 다른 하나에 대해 분쟁을 일으키고, $n \geq 3$ 인 상태에서 $\hat{\omega}_n = \hat{\omega}_{n-2}$ 이다.

정의 11. d 는 $\hat{\omega}_1$ 에 참여된 지분의 총 량이라 하자. 각 단계의 잠정적인 결과를 이 상황에서 알 수 있으므로, 우리는 분쟁 채권의 크기를 간단히 표기할 수 있다. 약칭 B_n 을 단계 n 에서 필요로 하는 채권의 크기라 하면 $B_1 = 2d$ 이고, $n \geq 2$ 인 상태에서 $B_n = B(\hat{\omega}_{n-1}, n)$ 이다. 이 수식을 통해 보다 직관적으로 확인할 수 있다.

고찰 8. 두개의 잠정적인 결과가 다른 하나에 반하여 반복적으로 분쟁을 일으키는 상황에서, $n \geq 3$ 인 상태에서 $S(\hat{\omega}_{n-1}, n) = S(\hat{\omega}_{n-1}, n-2) + B_{n-2}$ 이다. (이는 다른 모든 성공한 분쟁 채권이 동일한 결과에 더해짐을 뜻한다.)

보조정리 4. 만약 $n \geq 3$ 인 모든 n 회 단계에서 두 개의 잠정적인 결과가 서로에 반하여 반복적으로 분쟁을 일으킨다면:

$$1. S(\hat{\omega}_{n-1}, n) = \frac{2}{3}B_{n-1}$$

$$2. A_n = 2B_{n-1} \text{ 이고}$$

$$3. B_n = 3d2^{n-2}$$

Proof. (n 에 의해 유도)

두개의 잠정적인 결과가 서로에 반해 반복적으로 분쟁이 발생한다고 가정한다.

(기본 사례) 정리와 Eq. 1에 의해 우리는 다음 고찰을 만들 수 있다.

$$\bullet S(\hat{\omega}_1, 1) = d, S(\hat{\omega}_2, 1) = 0, A_1 = d, \text{ and } B_1 = 2d$$

- $S(\hat{\omega}_1, 2) = d, S(\hat{\omega}_2, 2) = 2d, A_2 = 3d, \text{ and } B_2 = 3d$

- $S(\hat{\omega}_1, 3) = 4d, S(\hat{\omega}_2, 3) = 2d, A_3 = 6d, \text{ and } B_3 = 6d$

$$S(\hat{\omega}_{3-1}, 3) = S(\hat{\omega}_2, 3) = 2d = \frac{2}{3}(3d) = \frac{2}{3}B_2 = \frac{2}{3}B_{3-1}, \text{ 따라서 보조정리 첫번째는 } n = 3 \text{인 것에 대해 유지된다.}$$

$$A_3 = 6d = 2(3d) = 2B_2 = 2B_{3-1}, \text{ 따라서 보조정리 2번은 } n = 3 \text{인 조건에 대해 유지된다.}$$

$$B_3 = 6d = 3d2^{3-2}, \text{ 따라서 보조정리 3은 } n = 3 \text{인 조건에 대해 유지된다.}$$

그러므로 보조정리는 $n = 3$ 을 기준으로 한 모든 경우에 성립한다.

(유도) 보조정리는 $3 \leq n \leq k$ 인 모든 n 에 대해 참이라고 가정하자. 우리는 보조정리가 $n = k+1$ 인 상태에서 유지된다는 것을 증명하고자 한다. 이를 살펴보고자 한다면:

$$(a) S(\hat{\omega}_k, k+1) = \frac{2}{3}B_k$$

$$(b) A_{k+1} = 2B_k \text{ 이고}$$

$$(c) B_{k+1} = 3d2^{k-1}$$

우선, (a)를 증명해보자. 고찰 8에 의하면:

$$S(\hat{\omega}_k, k+1) = S(\hat{\omega}_k, k-1) + B_{k-1}$$

고찰 7에 의해 위의 식은 아래와 같이 기술할 수 있다:

$$S(\hat{\omega}_{k-2}, k+1) = S(\hat{\omega}_{k-2}, k-1) + B_{k-1}$$

유도 가설에 의해 $S(\hat{\omega}_{k-2}, k-1)$ 에 $\frac{2}{3}B_{k-2}$ 을 대입하면:

$$S(\hat{\omega}_{k-2}, k+1) = \frac{2}{3}B_{k-2} + B_{k-1}$$

유도 가설에 의해, B_{k-2} 에 $3d2^{k-4}$, B_{k-1} 에 $3d2^{k-3}$ 을 대입하면:

$$S(\hat{\omega}_{k-2}, k+1) = d2^{k-1}$$

고찰 7을 좌변에 적용하면:

$$S(\hat{\omega}_k, k+1) = d2^{k-1}$$

마지막으로, 위 등식과 유도가설에 의해, $S(\hat{\omega}_k, k+1) = d2^{k-1} = \frac{2}{3}(3d2^{k-2}) = \frac{2}{3}B_k$ 이며, (a)는 증명 가능하다.

다음으로, (b)를 증명해보자. 고찰 6에 의하면:

$$A_{k+1} = A_k + B_k$$

유도 가설에 의해, $A_k = 2B_{k-1}$:

$$A_{k+1} = 2B_{k-1} + B_k$$

유도 가설에 의해, $B_{k-1} = 3d2^{k-3}$ 이므로, 우변은 아래와 같이 단순화할 수 있다.

$$A_{k+1} = 3d2^{k-2} + B_k$$

유도 가설에 의해, $B_k = 3d2^{k-2}$ 를 이용하여 우변을 단순화하면

$$A_{k+1} = 2B_k,$$

(b)는 증명되었다.

마지막으로, (c)를 증명해보자. Eq. 1에 의하면:

$$B_{k+1} = 2A_{k+1} - 3S(\hat{\omega}_k, k+1)$$

고찰 8에 의해, $S(\hat{\omega}_k, k+1)$ 는 $S(\hat{\omega}_k, k-1) + B_{k-1}$ 로 기술할 수 있다:

$$B_{k+1} = 2A_{k+1} - 3(S(\hat{\omega}_k, k-1) + B_{k-1})$$

고찰 7에 의해, $\hat{\omega}_k = \hat{\omega}_{k-2}$:

$$B_{k+1} = 2A_{k+1} - 3(S(\hat{\omega}_{k-2}, k-1) + B_{k-1})$$

고찰 6에 의해, $A_{k+1} = A_k + B_k$:

$$B_{k+1} = 2(A_k + B_k) - 3(S(\hat{\omega}_{k-2}, k-1) + B_{k-1})$$

유도 가설에 의해, $A_k = 2B_{k-1}$ 이고 $S(\hat{\omega}_{k-2}, k-1) = \frac{2}{3}B_{k-2}$ 이다:

$$B_{k+1} = 2(2B_{k-1} + B_k) - 3\left(\frac{2}{3}B_{k-2} + B_{k-1}\right)$$

유도 가설에 의해, $B_k = 3d2^{k-2}$, $B_{k-1} = 3d2^{k-3}$ 이고 $B_{k-2} = 3d2^{k-4}$ 이다. 이를 치환하여 단순화하면:

$$B_{k+1} = 3d2^{k-1}$$

이를 통해 (c)를 증명할 수 있고, 보조정리는 증명 가능하다. \square

정리 5. 만약 다른 시장이 포크되는 간섭 현상이 발생하지 않는다면, 시장은 종료되거나 포크되기 전에 많아야 20회의 분쟁 단계를 거치게 된다.

Proof. 주어진 시장은 다른 시장의 포크로 인한 간섭이 발생하지 않는다고 가정하자. 그렇다면 위에서 살펴본 바와 같이, 두 개의 결과가 서로에 반하여 분쟁을 일으킬 때, 포크가 발생하기 위해 필요한 분쟁 단계는 최대화된다. 보조정리 4의 3번은 이런 상황이면 최초 보고의 기간동안 참여된 지분의 양을 d 라 했을 때, 분쟁 단계 n 의 잠정적 결과에 반하여 분쟁에 성공하기 위한 분쟁 채권의 크기는 $3d2^{n-2}$ 임을 알려준다.

우리는 전체 REP 중 최소 2.5%에 달하는 분쟁 채권이 모여 분쟁에 성공하면 포크가 발생한다는 것과, 천백만개의 REP가 존재한다는 사실을 알고 있다. 그러므로, 분쟁 채권의 크기가 275,000 REP이상이면 포크가 발생하게 된다. 또한 $d \geq 0.35$ REP임도 알고 있다. 왜냐하면, 초기보고에 지분 참여된 최소 수량은 0.35 REP이기 때문이다²⁷.

$3(0.35)2^{n-2} > 275,000$ 을 $n \in \mathbb{Z}$ 에 대해 풀면 $n \geq 20$ 이다. 그러므로 시장은 많아야 20회의 분쟁 단계를 거친 뒤 해결되거나 포크를 일으킨다고 보장할 수 있다. \square

Appendix B: 대체 가설과 결과

다음을 다시 상기해보자:

- S 는 포크 기간동안 참의 공간으로 이전한 전체 REP의 비율이다.
- P 는 참의 공간에서 REP의 가격이다.
- P_f 는 공격자가 선택한 거짓의 공간으로 이전한 REP의 가격이다.
- I_a 는 원 어거 시장의 총 미청산계약이다.
- I_p 는 기생 시장의 총 미청산계약이다.

어거는 목표로 하는 시가 총액에 도달하기 위해 S , P_f , 그리고 I_p 에 대해 특정한 가설을 설정한다. 포크 기간동안 적어도 20%의 REP는 참의 공간으로 이전 할 것이고, 거짓의 공간으로 이전한 REP의 가치는 의미가 없으며, 기생 시장의 총 미청산계약은 많아야 원 어거 시장의 총 미청산계약의 50% 정도라고 어거는 가정한다. 다시 말하면: $S \geq 0.2$, $P_f = 0$, 이고 $I_a \geq 2I_p$ 이다. 이 가설 하에서 정리 1은 원 어거 시장의 총 미청산계약보다 REP 시가 총액이 7.5배 이상이면 포크 프로토콜의 무결성은 성립됨을 알려준다.

특정한 상황에서 오라클의 무결성을 유지하기 위한 시가 총액이 얼마인지 S , P_f , 그리고 I_p 를 이용하여 다른 가설을 만들 수 있다. 논의의 편의를 위해 몇 가지 다른 가설을 열거하도록 한다.

시나리오 1. 포크 기간동안 50% 이상의 REP가 참의 공간으로 이동하였다. 이 경우 P_f 와 I_p 는 문제 될 것이 없다. $S > \frac{1}{2}$ 에 부합하는 한, 시가 총액이 얼마이건 포크 무결성은 유지된다. 공격자가 성공하기 위해 이용할 수 있는 REP의 양이 충분하지 않기 때문이다.

시나리오 2. 전체 REP의 48%가 포크 기간 동안 참의 공간으로 이동하였고 기생 시장은 존재하지 않으며,

²⁷appendices E 2과 E 3를 참조하기 바란다.

거짓의 공간으로 이동한 REP는 전혀 가치가 없다. 이 경우 $S = 0.48$, $I_p = 0$, 이고 $P_f = 0$ 이다. 이 가설 하에서 REP의 시가 총액은 원 어거 시장의 총 미청산계약보다 최소 약 두 배가 커야 포크 무결성이 유지된다.

시나리오 3. 포크 기간 동안 전체 REP의 20%가 참의 공간으로 이동하였고, 기생 시장과 원 어거 시장의 총 미청산계약의 크기가 같으며, 거짓의 공간으로 이동한 REP는 참의 공간으로 이동한 REP의 가격의 5% 수준으로 평가된다고 하자. 이 경우 $S = 0.2$, $I_p = I_a$, 이고 $P_f = 0.05P$ 이다. 이 가설 하에서는 REP 시가 총액은 원 어거 시장의 총 미청산계약의 10.5배는 되어야 포크 프로토콜의 무결성이 유지된다.

시나리오 4. 포크 기간 동안 단지 5%의 REP가 참의 공간으로 이동하였고, 기생 시장의 총 미청산계약이 원 어거 시장의 그것보다 두 배에 달하며, 거짓의 공간으로 이동한 REP는 참의 공간의 REP 가격의 5%라고 하자. 이 경우, $S = 0.05$, $I_p = 2I_a$, 이고 $P_f = 0.05P$ 이다. 이 가설 하에서 포크 프로토콜의 무결성을 유지하기 위해서는 REP 시가 총액이 원 어거 시장의 총 미청산계약보다 63배 이상이 되어야 한다.

Appendix C: 포크 프로토콜의 무결성에 조기 이전 보상이 미치는 영향

포크 프로토콜의 무결성에 대한 고찰에서 논의의 편의를 위해, 5%의 조기 이전 보상과 짧은 기간을 무시하여 단순화하였다. 두 조건을 고려한 상태에서 정리 1로 돌아가 보자.

보고 기간동안 참의 공간으로 이동된 REP의 총량을 SM 이라 한다. 그러므로 공격자가 성공하려면, 최소한 $SM + \epsilon$ REP를 이전해야 한다. 이는 거짓의 공간으로 이전하기 전에 $(SM + \epsilon)P$ 의 가치를 가진다.

만약 공격자가 $SM + \epsilon$ REP를 포크 기간 동안 거짓의 공간으로 이전한다면, $1.05(SM + \epsilon)$ REP를 이전한 자식 공간에서 받게 된다. P_f 의 정의에 의해, 이 코인의 가치는 $1.05(SM + \epsilon)P_f$ 이다. 그러므로 공격자의 최소 비용은 $(SM + \epsilon)P - 1.05(SM + \epsilon)P_f$ 이고 이는 $(SM + \epsilon)(P - 1.05P_f)$ 로 기술할 수 있다.

공격자의 최대(총) 수익은 $I_a + I_p$ 이다. 그러므로 포크 프로토콜은 $S > \frac{1}{2}$ 인 상황에서 무결성을 유지한다고 할 수 있다:

$$I_a + I_p < (SM + \epsilon)(P - 1.05P_f) \quad (C1)$$

위 부등식을 시가총액인 PM 에 대해 풀면, 포크 프로토콜은 다음의 조건에서 무결성을 유지함을 알 수 있다:

1. $S > \frac{1}{2}$ 또는
2. $\frac{1.05P_f}{P(I_a + I_p - \epsilon(P - 1.05P_f))} < \frac{P}{S(P - 1.05P_f)}$ 이고 REP 시가 총액이

이를 통해 조기 이전 보상이 시가 총액의 요구 조건에 미치는 영향은 아주 작다는 것을 알 수 있다.

Appendix D: 포크의 최소 비용에 조기 이전 보상이 미치는 영향

포크 기간 동안 더 많은 참여를 유도하기 위해, 포크 시작 후 60일 이내에 REP를 이전하는 모든 토큰 보유자들은 이전한 자식 공간에서 5%의 추가 REP를 보상으로 받게 된다. 이 보상은 인플레이션을 통해 이루어진다.

만약 포크를 시작하는 비용이 너무 적다면, 이는 왜곡된 보상이 될 수 있다. 특히, 공격자가 5%의 추가 REP를 통해 포크의 개시를 방해할 수 있을 정도의 가치를 모을 수 있다면, 포크가 더 자주 발생할 것임을 유추할 수 있다. 이러한 공격을 우리는 인플레이션 밀킹 공격이라 한다. 이로 인해 오라클의 보고 체계가 잘못되진 않지만, 포크가 자주 발생하는 문제를 야기한다.

이를 방지하기 위해 어거는 포크의 시행에 소요되는 비용이 5%의 인플레이션 보상으로 얻은 최대의 가치보다 크게 만들 필요가 있다. 잘못된 보상으로 인한 포크를 방지하기 위해 필요한 비용의 하한값을 유도해보자.

P_0 를 포크 이전의 가격이라 하고 P_1 은 포크 이후의 REP 가격이라 하자. M_0 는 포크 이전의 통화 공급량이고, M_1 은 포크 이후의 통화 공급량이다. S 는 포크 기간동안 참의 공간으로 이전하는 M_0 의 비율이다. b 는 포크를 시행하기 위해 경제적으로 소각되어야 하는(다시 말하면, 거짓의 결과에 지분참여하는) REP의 수량이라 하자. 우리는 $b > 1$ 이라 추정한다.

이 장의 목적에 따라 포크 기간동안 이전한 모든 REP가 공격자의 통제 하에 있다는 보수적인 가정을 해보자. 더 나아가(왜냐하면 이는 이 공격의 비용을 최소화하므로) 우리는 포크 기간동안 모든 REP가 참의 공간으로 이동할 것임을 알 수 있다.

이 정의에 의해, SM_0 은 포크 기간 동안 이동한 REP의 총량이고, 반면 $(1 - S)M_0$ 은 포크 기간 내에 이전하지 않은 REP의 전체량이다.

$$M_0 = SM_0 + (1 - S)M_0 \quad (D1)$$

총 SM_0 REP가 포크 기간 동안 이전했다면 총 $0.05SM_0$ REP가 인플레이션으로 생성된다:

$$M_1 = 1.05SM_0 + (1 - S)M_0 \quad (D2)$$

단순화를 위해 인플레이션의 효과만 주목하면, 포

크²⁸이전과 시가 총액이 같다고 가정할 수 있다:

$$P_0 M_0 = P_1 M_1 \quad (\text{D3})$$

D1과 D2를 통해 단순화하면:

$$P_1 = \frac{20P_0}{20 + S} \quad (\text{D4})$$

포크를 시행하여 조기 이전 보상을 받음으로써 공격자가 얻는 (총) 수익은 이전한 REP의 총 가치에서 이전 전의 총 REP 가치를 제하면 된다:

$$1.05SM_0 P_1 - SM_0 P_0 \quad (\text{D5})$$

D4를 D5에 대입하면 우리는 공격자의 (총) 수익을 다른 형태로 표시할 수 있다:

$$1.05SM_0 \frac{20P_0}{20 + S} - SM_0 P_0 \quad (\text{D6})$$

b 는 포크가 시행되기 위해 경제적으로 소각되어야 하는 REP의 수량임을 상기해보자. 이에 따라 포크의 시행에 소요되는 비용은 bP_0 이다. 그러므로 조기 이전 보상의 이점을 누리기 위해 포크를 시행할 때 소요되는 비용은 아래 등식이 성립하는 한 항상 가치가 있다고 할 수 있다:

$$0 < 1.05SM_0 \frac{20P_0}{20 + S} - SM_0 P_0 - bP_0 \quad (\text{D7})$$

$P_0 > 0$ 이고, $S \neq -20$ 을 b 를 통해 풀면 공격은 다음 상황에서 수익을 얻을 수 있다:

$$b < \frac{21M_0S}{S + 20} - M_0S \quad (\text{D8})$$

잘못된 보상을 방지하기 위해 어거는 위의 상황을 초래해서는 안된다:

$$b \geq \frac{21M_0S}{S + 20} - M_0S \quad (\text{D9})$$

S 가 구간 $[0, 1]$ 에서 금지되는 것 뿐만 아니라, 부등식 우변 D9의 값은 $S = 2\sqrt{105} - 20 \approx 0.4939$ 일 때 최대화되는 것을 알 수 있다. 이는 공격은 포크 기간동안 약 49.39%의 REP가 이전하였을 때 공격자의 수익이 가장 커짐을 뜻한다. 우리는 이를 S 라고 보수적으로 접근하도록 하겠다.²⁹

²⁸우리는 이를 보수적이라 생각한다. 특히, 시가 총액은 포크 이후 감소할 것으로 예상한다.

²⁹특히, 공격자는 포크 기간 동안 다른 참여자가 그들의 REP를 이전하는 것을 막을 수 없다. 또한, S 가 0.4939라는 이상적인 수치를 넘을 것이라 확신할 수도 없다. 그러나, 여기서는 $S = 0.4939$ 라는 최악의 상황을 가정하였다.

D9의 $S = 0.4939$ 로 치환하면 $b \geq 0.012197M_0$ 가 된다. 그러므로 전체 REP 중 최소 1.2197%의 REP가 포크 시행에 소요되는 비용이라면 인플레이션 밀킹 공격은 유효하지 않다.

포크는 분쟁 채권이 전체 REP의 2.5% 이상 모였을 때 발생한다고 하였다. 결과 ω 에 대해 분쟁채권이 모이고 포크가 실행되었다고 하자. 결과 ω 는 참일 수도 거짓일 수도 있다.

만약 ω 가 거짓이면, 최소 2.5%의 REP가 거짓의 결과에 지분 참여되어야 하고, 경제적으로 소각되어야 한다. 그러므로 ω 가 거짓인 상태에서 인플레이션 밀킹 공격은 성립되지 않는다.

만약 ω 가 참이면, 보조정리 2를 통해 최소 1.25%의 REP가 (전체) 거짓의 결과에 지분 참여되어야 하고, 경제적으로 소각되어야 한다. 그러므로 ω 가 참인 상태에서도 인플레이션 밀킹 공격은 성립하지 않는다.

이런 이유로 최소 2.5%의 REP가 참여되었을 때만 포크가 가능하도록 설계되어있다.

Appendix E: 채권 크기 조정

유효 채권, 미이행 채권 그리고 지정된 보고자의 지분은 이전 수수료 구간의 참여자의 행동에 따라 동적으로 조정된다. 이 값들이 어떻게 조정되는지 살펴보자.

함수 $f : [0, 1] \rightarrow [\frac{1}{2}, 2]$ 를 다음과 같이 정의할 수 있다:³⁰

$$f(x) = \begin{cases} \frac{100}{99}x + \frac{98}{99} & \text{for } x > \frac{1}{100} \\ 50x + \frac{1}{2} & \text{for } x \leq \frac{1}{100} \end{cases} \quad (\text{E1})$$

함수 f 는 아래 세부 항목에 기술한 것처럼, 이 조정을 반복 적용하기 위해 사용한다. 간단히, 발생해서는 안될 행동이 이전 수수료 구간동안 1% 발생한다면, 채권의 크기는 동일하게 남는다. 이보다 덜 잦은 빈도라면, 채권의 크기는 반 씩 감소할 것이다. 이보다 더 잦다면, 채권의 크기는 최대 두배 씩 증가할 것이다.

1. 유효 채권

어거의 개설 이후 첫 유효 채권의 크기는 0.01 ETH로 지정된다. 만약 이전 수수료 구간의 1% 이상의 종료된 시장이 무효라면, 유효 채권은 증가할 것이다. 만약 1%보다 작은 시장이 이전 수수료구간 동안 무효 처리되면 유효채권은 감소할 것이다. (하지만 0.01 ETH보다 작아지는 않는다.)

특히, ν 를 이전 수수료 구간동안 무효 처리된 시장의 비율이라 하면, b_ν 는 이전 수수료 구간의 유효

³⁰이 공식은 실제 시장에서 얻어지는 결과에 따라 바뀔 수 있다.

채권의 크기라 할 수 있다. 현재 구간의 유효 채권은 최대 $\max\left\{\frac{1}{100}, b_v f(\nu)\right\}$ 이다.

2. 미이행 REP 채권

어거의 개설 이후 첫 미이행 REP 채권의 크기는 0.35 REP로 지정된다. 유효 채권과 마찬가지로 미이행 REP 채권은 1%의 미이행 비율을 목표로 0.35 REP에 대해 증가하거나 감소하게 된다.

ρ 를 이전 수수료 구간의 해당 시장의 지정된 보고자가 정시에 보고하지 않은 비율이라 하면, 미이행 b_r 은 이전 수수료 구간을 통해 계산한 미이행 REP 채권의 크기이다. 현재 수수료 구간의 최대 미이행 REP 채권의 크기는 $\max\{0.35, b_r f(\rho)\}$ 가 된다.

3. 지정된 보고자의 지분

어거의 개설 이후 첫 지정된 보고자의 지분은 0.35 REP로 지정된다. 지정된 보고자의 지분량은 얼마나 많은 지정된 보고자가 이전 수수료 구간에서 잘못된 보고를 하는지(시장의 최종 결과를 얻는데 실패하는지)에 따라 동적으로 조정된다.

δ 를 이전 수수료 구간에 잘못된 보고를 하는 지정된 보고자의 비율이라 하고, b_d 는 이전 수수료 구간에 지정된 보고자의 지분량이라 하면, 현재 구간에 지정된 보고자의 지분량은 최대 $\max\{0.35, b_d f(\delta)\}$ 가 된다.

Appendix F: 설계의 변경

현재 어거의 설계는 3년간의 연구와 반복을 통해 도출한 것이다. 이 설계는 기존 백서 [12]의 것과 다른 부분이 많다. 중요한 변화 세 가지의 이유를 설명하도록 하겠다.

1. 보고 수수료

기존의 설계에서 시장 개설자는 거래 수수료를 보고자와 50/50으로 나눌 수 있었다. 바뀐 설계에서 시장 개설자와 보고자를 위한 수수료는 별개이며 보고자의 수수료는 어거의 시스템을 안전하게 유지하기 위해 동적으로 변화된다.

보고자에게 지급되는 수수료는 REP 가격에 영향을 미치며 이는 포크 프로토콜의 안정성과 직접적으로 연결되어 있다.(정리 1). 만약 보고자에게 지급되는 수수료가 지나치게 낮으면 오라클의 무결성은 위험에 처하게 된다. 보고자에 지급되는 수수료가 지나치게 많으면, 기생 시장으로 인한 위험이 증가하게 된다. 그러므로, 보고자에 지급되는 수수료를 시장 개설자가

임의로 결정하는 것보다 어거의 안정성을 유지하기 위해 동적으로 결정되도록 하는 것이 좋다.

보고자의 수수료를 시장 개설자의 결정에서 분리함으로써 보고자들(뿐만 아니라 포크 프로토콜의 무결성까지)은 시장 개설자들이 적은 수수료를 경쟁적으로 책정하는 문제를 해결할 수 있다. 양질의 시장과 양질의 보고는 분리되어 측정되고 보상되어야 한다. 시장 개설자들의 수수료를 0까지 낮추는 경쟁을 하더라도 보고자의 수수료까지 낮아지는 일은 발생하지 않는다.

2. 거래 수수료

기존 설계에서는 모든 거래에서 수수료가 수집되었다. 새로운 설계에서 수수료는 시장 계약을 통해 청산될 때에만 수수료가 수집된다. 이 변화는 어거가 오프라인 거래를 막을 수 없기 때문이다. 시장 결과의 주식은 누구나 자유롭게 거래할 수 있는 토큰에 지나지 않는다. 모든 거래에 수수료를 부과하는 것은 불가능하기 때문에, 어거는 어거의 시장 계약을 통해 거래할 때에만 수수료를 수집한다. 이 방식으로 인해 생기는 추가적인 이익은 거래자들이 지불할 수수료의 평균을 낮추어 어거를 더 경쟁적으로 만든다.

3. 공간

이전 설계에는 REP의 버전을 사용했으며 총 공급량이 고정된 상태였다. 새로운 설계에서 REP는 다수의 다른 버전(공간)으로 포크가 가능하며, 원 버전보다 작거나 많은 REP 수량을 지니게 된다. 만약 논쟁적인 포크가 발생하면, 자식 공간의 총 REP 수량은 부모 공간의 것과 다르게 된다. 논쟁적이지 않은 포크의 경우, 포크 참여자에게 제공되는 초기 이전 보상 수량으로 인해 자식 공간은 부모 공간에 비해 더 많은 수량의 REP를 보유하게 된다.

포크를 통해 떨어져 나온 새 버전의 REP는 각기 다른 가치와 공급량을 가진 완전히 다른 토큰이며, 서비스 제공자들도 이를 다른 토큰으로 취급해야 한다. 어거의 첫 개설 시점에서는 하나의 공간(제네시스 공간)만 존재하며 하나의 REP만 존재한다. 그러나 포크가 발생하는 순간 하나의 REP는 다수의 버전으로 분리된다: 가령 포크 시장이 결과 A와 B로 분리되면, 새로운 토큰 REP-A, REP-B, REP-무효의 토큰이 생겨난다. 지갑이나 거래소 서비스 제공자들은 REP-제네시스(사용이 잠기는 원 버전의 REP)까지 총 4개 버전의 다른 REP를 취급해야 한다.³¹

³¹실질적으로, 서비스 제공자는 (일반 사용자들에 비해) 이를 쉽게 찾아 포크 참여를 독려할 수 있으며 포크가 해결되었을 때 승리 공간을 지지할 수 있다.

각각의 자식 공간의 REP 공급량은 얼마나 많은 REP가 이전하는지, 언제 이전이 발생하는지에 따라 달라진다. 아직 자식 공간으로의 합의가 충분히 진행되기 이전에 포크 기간동안 REP를 이전하는 것은 사용자에게 작은(없지는 않다) 위험을 감수하는 일이며 (섹션 III E 참조), 이는 논쟁적인 포크에 참여하는 것을 주저하게 만든다. 포크 기간 동안의 참여를 독려하기 위해 위험에 대해 보상을 제공할 필요가 있다.

포크 기간동안 참여하지 않은 사용자는 REP 보유량의 일정 부분을 잃게 되는 불이익을 받게 된다. 이전 설계의 “사용하거나 모두 잃거나” 방식은 미참여자들을 잘못된 보고를 하는 보고자로 취급하였다. 그러나

미 참여자를 이런 형태로 징벌하는 것은 사용상의 큰 문제를 유발한다. 미참여자에 대한 이와 같은 징벌은 REP를 대신 관리하는 지갑이나 거래소의 경우 문제가 된다. 포크로 인해 거래소는 고객의 REP를 포크 기간 동안 어떤 자식 공간으로 이전하거나 보유한 REP의 일정량을 잃어야 한다.³²

미참여자에 징벌을 가하는 대신, 포크 기간동안 이전한 참여자에게 그들이 이전한 공간에 5%의 새로운 REP를 지급한다. 만약 4.762%의 REP(혹은 그 이상)가 실패한 공간으로 이전하면 – 1.25%에서 2.5%가 이미 분쟁 지분으로 참여한 상태 – 모든 자식 공간은 부모 공간보다 적은 수량의 REP를 보유하게 된다.

³²또한, 포크 보상을 재분배를 통해 실행하는 스마트 컨트랙트 코드가 과도하게 복잡하다고 판단했다. 복잡한 컨트랙트 코드는 보안의 문제를 야기할 수 있다. 따라서 우리는 가급적 단순한 형태로 선언

하고자 하였다.