Cryptoeconomic Analysis of Casper FFG

강보영, 박시은, 이기호, 임호태, 전창석, 홍종화

이더리움연구회 4기 토큰 이코노미 분과

이더리움 연구회

korea ethereum study group

목 차

1. 서론

자본주의 경제 시스템에는 필연적으로 호황과 불황이 공존한다. 1971년 8월 15일, 리처드 닉슨 전 미국 대통령이 브렌트 우즈 체제를 사실상 무너뜨리면서, 정부 또는 소수 집단이 화폐 발행 권한을 독점함과 동시에, 자유 시장과 개인의 사유재산권 행사에 막강한 영향을 미치게 되었다. 정부가 발행한 화폐는 은행으로 흘러 들어가 신용 팽창과 함께 인플레이션을 일으키고, 자본재에 잘못된 투자가 정리되는 과정에서 디플레이션을 일으킨다. 이것이 경제에 호황과 불황이 공존하는 이유다. 가장 최근 발생했던 2008년 리먼 브러더스 사태도 이러한 과정의 하나여야 했다. 그러나 미국 연방준비은행은 '대마불사'를 이유로 공적 자금의 용도로 마음껏 발행한 화폐를 그 누구의 허락도 없이 구제금융으로 제공했다. 이는 많은 이들에게 기존 금융 시스템에 대한 불신을 심어주게 되었고, 우리가 잘 알고 있는 비트코인이 탄생하는 계기가 되었다.

비트코인은 2008년 사토시 나카모토라는 필명으로 발표한 〈Bitcoin: A Peer-to-Peer Electronic Cash System〉이라는 A4용지 9장짜리 논문이 공개되면서 처음 세상에 등장했다. 익명의 한 사람, 또는 집단으로 보이는 사토시 나카모토는 분산화된 전자화폐 시스템을 통해서 기존의 믿을 수 없던 금융 시스템에 어떠한 파장을 일으키고자 한 것 같다. 그는 비트코인의 제네시스 블록에 이러한 메시지를 숨겨두었다. "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."(영국 재무장관, 은행에 두 번째 구제 금융 임박) 영국 신문의 헤드라인을 통해 이 블록이 생성된 날짜를 증명하고자 하는 의도도 있었겠지만, 전 세계적인 금융 위기를 촉발시킨 기존 금융 시스템을 조롱하고자 하는 의도 역시 엿보인다. 그는 논문에서 금융기관이 거래 자체에 직접적인 영향을 미치기 때문에 완전한 비가역적 거래(Completely non-reversible transactions)는 불가능하다고 표현했다. 따라서, 특정 정부나 기관, 소수 집단의 통제를 받지 않는 독립적인 화폐 시스템을 블록체인과 암호 경제학을 통해 구축하고 싶어 한 것으로 생각된다.

비트코인과 이전의 다른 전자 화폐(E-cash, Digicash)의 가장 큰 차이는 비트코인이 화폐에 대한 신뢰를 구축했다는 점이다. 사토시 나카모토는 중앙 주체에 의한 임의적인 화폐 발행을 배제하고, 거래의 내역 역시 분산 네트워크의 참여자가 모두 검증하게 하였다. 이를 통해 화폐의 신뢰를 보장하는 주체를 특정 사상 및 세력에 의해 통제 가능한 제3의 기관에서 탈중앙화 네트워크 전체로 옮겨오고자 했다. 이를 뒷받침하는 것은 비트코인 시스템에서 유래한 블록체인 무결성의 핵심인 엄두도 내지 못할 비가역성(Prohibitively irreversible)에 있다. 이는 완전한 비가역성을 보장하지는 못하지만, 확률적으로 비가역성에 가까울 만큼 거래내역을 조작하는 것이 어렵다는 것을 의미한다. 화폐의 발행도 알고리즘에 의해 실행되므로 제3의 주체가 임의로 변경할 수 없다.

비트코인의 탈중앙화 합의 알고리즘을 가능하게 하는 작업 증명 방식(Proof of Work)은, 거래 내역을 검증하고 해시 파워(Hash power)를 가진 참여자에게 보상 자격을 부여하여, 분산된 환경에서 노드 간 합의가 이루어지도록 한다. 그러나 참여자는 더 많은 보상을 받기 위해 더 많은 컴퓨팅 파워(Computing power)를 소모해야 하므로, 작업 증명 방식은 비효율적인 에너지 소비를 불러일으킨다는 비판을 지속해서 받고 있다. 이외에도 작업 증명 방식은 소수 마이너에 의한 독점, 악의적인 노드에 의한 부정한 블록 생성 등 여전히 해결해야 하는 과제를 많이 가지고 있다.

이러한 작업 증명 방식이 가진 문제점을 인식하고 해결하기 위해 지분 증명 방식(Proof of Stake)이 등장하였다. 지분 증명 방식에서 네트워크의 참여자는 지분율에 따라 네트워크에 참여할 수 있는 권한을 부여받고, 이에 따른 보상을 받는다. 분산 네트워크에서 가장 중요한 결함 내성의 달성 역시 지분 증명 방식에서는 보상을 주는 기존의 방식에 지분을 삭감하는 방식을 더하여 이루어진다. 이는 이전의 PoW에서 결함 내성을 달성하기 위해 사용되었던 에너지의 소모를 피할 수 있게 한다는 측면에서 긍정적이다. 그러나, 네트워크의 참여자가 경제적 이득을 얻기 위해 하는 행동들이 네트워크의 안정성을 보장해야 하고, 네트워크에 해가 되는 행동에 대해서는 적절한 처벌 역시 가해져야 한다. 따라서, 보상과 처벌의 메커니즘에 영향을 끼치는 변수들을

더욱 정교하게 고려하여 설계해야 한다. 암호 경제학은 바로 여기서 힘을 발휘한다.

암호 경제학

암호 경제학은 블록체인과 암호화폐의 확산에 따라 큰 주목을 받는 분야이다. 이더리움의 Casper CBC를 구축하고 있는 Vlad Zamfir는 암호 경제학을 다음과 같이 정의했다.

"분산화된 디지털 경제에서 재화와 서비스의 생산, 분배 그리고 소비에 이르기까지의 활동을 관리하는 프로토콜을 학습하는 학문이다."

블록체인 네트워크에 참여하는 주체는 경제적 인간이다. 경제적 인간은 주어진 정보를 최대한 활용하여, 최대의 이득을 추구한다. 따라서 블록체인 네트워크의 암호 경제를 설계하는 데 있어서 가장 먼저 고려되어야 하는 사항은 경제적 주체의 행동이 네트워크에 가져올 효과를 인식하는 것이다. 그다음은, 경제적 주체의 이득 추구가 가져올 행동을 게임이론에 입각하여 예측하고, 목표 행동과 그 행동을 유도하는 조건을 설정해야 한다. 메커니즘 디자인(Mechanism Design)은 바로 이를 위한 도구이다.

향후 다루어질 내용에서는 분산 네트워크의 특징과 합의 과정에 대해 살펴보고, 네트워크의 안정성을 저해할 수 있는 경제적 주체의 게임이론적 행동 요소에 대해 알아보며, 이를 해결하기 위한 이더리움 Casper FFG에 대해 알아보기로 한다.

2. 게임이론[1]

2.1. 소개

게임이론은 특정 상황에 놓인 플레이어들이 각기 자신의 효용 극대화를 추구하는 과정과 결과를 분석하는 학문으로 플레이어 간의 상호작용이 어떻게 전개될 것이며, 어떠한 결과를 도출하게 될 것인지 수학적으로 해석한다. 해당 보고서에서 다루는 이더리움의 Casper FFG 역시 게임이론을 바탕으로 설계되었음으로, Casper FFG를 이해하기 위해서는 게임이론에 대한 적정 수준의 지식이 필요하다. 해당 챕터에서는 게임이론의 가장 핵심과 기초에 기반하는 몇 가지 예시와 함께 근간 이론들을 다루려고 한다.

2.2. 우월 전략

우월 전략(Dominant Strategy)은 다른 플레이어가 선택할 수 있을 어떤 전략에 대해서도 최선반응인 전략이다. 최선반응(Best Response)이란 각 플레이어가 선택하는 최적의 전략을 말한다. 다음 [표1]은 우월 전략을 이해하기 위한 예시이다. A와 B 두 회사는 같은 제품을 생산하지만 회사 규모의 차이로 인해 이득이 다르다. 두 회사가 제품에 대해 광고를 할 것인지에 따른 이득표(Payoff Matrix)를 [표1]과 같이 표시한다.

		B 회사	
		광고한다.	**광고 안 한다.**
A 회사	**광고한다.**	4, 3	5, 1
	광고 안 한다.	2, 5	3, 2

[표1] 광고 게임

이득표 [표1]을 해석하는 방법은 다음과 같다. A 회사가 광고하고, B 회사는 광고하지 않는다고 할 경우, A 회사의 이득은 5, B 회사의 이득은 1이 된다. 이를 (5, 1)로 기재한다. 이득표에서 왼쪽 플레이어의 이득을 왼쪽에, 오른쪽 플레이어의 이득을 오른쪽

에 기재하는 것이 원칙이다. 그러면 이 게임에서의 우월 전략을 알아보자. A 회사가 광고할 경우, 4 또는 5의 이득을 얻는다. 광고하지 않을 경우, 2 또는 3의 이득을 얻는다. 따라서 A 회사는 광고하는 전략을 무조건 선택할 것이다. 이를 A 회사의 우월 전략이라고 한다. B 회사가 광고할 경우, 3 또는 5의 이득을 얻는다. 광고하지 않을 경우, 1이나 2의 이득을 얻는다. 따라서 B 회사는 광고하는 전략을 무조건 선택할 것이다. 이를 B 회사의 우월 전략이라고 한다. 설명의 편의를 위하여 각 플레이어의 우월전략의 이득을 밑줄로 표기하기로 한다. 즉, A 회사의 우월 전략은 광고하는 것이며, B 회사의 우월 전략도 광고하는 것이다. 각 플레이어는 현재의 우월 전략 이외에 더 나은 이득을 가져갈 수 있는 전략이 존재하지 않는 상태가 된다. 이를 우월 전략 균형이 성립했다고 한다. 따라서 이득표 [표1]에서 두 회사의 우월 전략 균형은 (광고한다, 광고한다)인 (4, 3)에서 성립한다.

2.3. 내쉬 균형

우월 전략 균형은 강력한 균형이지만 현실 사회에서 우월 전략 균형이 성립하는 경우는 극히 드물다. 현실적으로는 상대방의 전략 선택에 따라서 각 플레이어가 선택할 최적의 전략이 달라질 수 있기 때문이다. 즉 우월 전략 균형만으로는 모든 게임을 설명하는 데 한계가 있으며, 대부분의 사례에는 우월전략균형이 아닌 다른 접근법이 필요하다. 앞으로 설명할 내쉬 균형(Nash Equilibrium)은 현실에서 존재하는 다양한 게임에 대해 더욱 폭넓은 분석 방법을 제시한다.

2.3.1. 하나의 균형점을 갖는 내쉬 균형

다음 [표2]의 상황은 두 명의 플레이어가 각기 세 가지의 전략을 취할 수 있는 경우다. 앞서 [표1]에서 설명한 우월전략균형과 다르게, 각 플레이어에게는 우월전략이 존재하지 않으며 플레이어 B의 선택에 따라 플레이어 A의 최선반응 또한 달라지는 것을 확인할 수 있다.

		플레이어 B		
		착한 행동	악의적 행동	No action
플레이어 A	착한 행동	10, 10	-5, 0	-25, 30
	악의적 행동	-5, 0	20, 10	0, -30
	No action	-25, 10	-30, -30	-10, 20

[표2] 하나의 내쉬 균형점을 갖는 게임

상기 [표2]에서 각 플레이어의 최선반응에 따른 균형은 두 플레이어 모두 악의적 행동을 선택할 때 성립함을 알 수 있다. 만약 플레이어 A가 '착한 행동'을 선택한다면 플레이어 B는 'No action'을 선택해 이득을 30으로 극대화할 것이다. 이는 플레이어 A에게는 -25의 손실을 입힌다. 반대로 플레이어 B가 'No action'을 선택했을 때, 플레이어 A의 최선반응을 분석해본다. 이 경우 플레이어 A는 0의 이득을 얻는 '악의적 행동'을 선택하게 될 것이며 이에 따라 플레이어 B는 -30의 손실을 입게 될 것이다. 결국 두 플레이어 모두 '악의적 행동'이라는 전략으로 귀결된다. 우월 전략 균형을 갖지 않는 게임이라도, 각 플레이어가 상대 플레이어의 전략에 대한 최선반응을 선택하면 모든 플레이어는 선택한 전략을 변경할 이유가 없으며, 합리적인 판단 하에 상대 플레이어의 전략을 예측할 수 있다. 이러한 상황을 우리는 내쉬 균형이 성립한다고 한다.

2.3.2. 여러 개의 균형점을 갖는 내쉬 균형

		플레이어 B		
		착한 행동	악의적 행동	No action
플레이어 A	착한 행동	10, 10	-25, 30	-5, 0
	악의적 행동	30, -25	-30, -30	20, -10
	No action	0, -5	-10, 20	0, 0

[표3] 여러 개의 내쉬 균형점을 갖는 게임

[표2]의 이득을 [표3]과 같이 수정하면 내쉬 균형도 변하는 것을 알 수 있다. 이 경우 내쉬 균형은 (No action, 악의적 행동)과 (악의적 행동, No action)의 두 개이다. 이처럼 내쉬 균형은 전략의 이득에 따라 여러 개가 성립할 수 있다.

2.3.3. 균형점이 없는 경우

		플레이어 B		
		착한 행동	악의적 행동	No action
플레이어 A	착한 행동	10, 10	-25, 30	25, 0
	악의적 행동	30, -25	-30, -30	20, -10
	No action	0, 25	-10, 20	0, 0

[표4] 균형점이 없는 게임

[표3]에서 확인하였듯이 하나의 게임 내에 여러 개의 내쉬 균형이 존재할 수도 있지만 이와 반대로 균형점이 없는 경우도 있을 수 있다. [표4]에 따르면, 각 플레이어가 상대방의 전략에 따라 최선반응을 선택하는 경우 게임에는 어떠한 균형점도 존재하지 않는다. 이러한 경우 기존 게임이론에서는 확률 변수를 추가로 고려하여 혼합 전략 균형을 도출해 낼 수 있다. (여기에서 혼합 전략 균형은 다루지 않기로 한다.)

위에서 우리는 내쉬 균형의 장점과 정의 그리고 다양한 예시를 확인하였다. 그러나 내쉬 균형도 현실 상황을 설명하기에는 한계점을 가지고 있다. 그 중 가장 대표적인 한계점인 리스크의 문제를 예시를 통해 확인해보도록 한다.

2.3.4. 내쉬 균형의 한계점, 리스크의 문제

		플레이어 B	
		착한 행동	악의적 행동
플레이어 A	착한 행동	10, 10	-1,000, 9.9
	악의적 행동	9, 10	8, 9.9

[표5] 리스크를 고려하지 못하는 내쉬 균형 게임

[표5]에서 내쉬 균형은 (착한 행동, 착한 행동)에서 성립한다. 그러나 이전 예시

와 달리 [표5]의 플레이어 A에게는 상당한 리스크가 존재한다. 플레이어 B의 입장에서 '착한 행동'과 '악의적 행동'에 대한 이득은 10과 9.9로 큰 차이가 없다. 이와 달리 플레이어 A의 경우 '착한 행동'은 플레이어 B의 전략 선택에 따라 큰 피해를 입을 수 있는 전략이다. 따라서 플레이어 A는 '착한 행동'을 선택할 때, 리스크를 고려해야 한다. 만약 플레이어 A가 리스크 회피적 성향의 사람이라면 플레이어 A의 현실적인 선택은 다소 비합리적임에도 불구하고 '악의적 행동'이 될 것이다.

이처럼 단순한 내쉬 균형은 각 플레이어의 리스크에 따른 선택을 설명하지 못한다. 리스크를 고려하기 위하여 기존 게임이론에서는 완전균형(Trembling Hand Perfect Equilibrium)을 통해 다음과 같은 상황을 설명한다.

2.3.5. 완전균형(Trembling Hand Perfect Eq.)

완전균형(THPE)이란 상대 플레이어가 의도와 달리 실수로 다른 선택을 할 경우까지를 고려하여 자신의 최적대응을 찾은 것이다. 이러한 이유에서 완전균형을 손떨림 완전균형이라고도 한다. [표4]에서 플레이어 A는 만에 하나의 경우에 발생 가능한 플레이어 B의 실수(악의적 행동)에 -1,000 이라는 손실을 입게 된다. 이러한 리스크를 고려하여 플레이어 A는 플레이어 B의 악의적 행동 전략에 최소한의 확률(ε)을 가정한다.

B가 착한 행동을 할 확률: $1-\varepsilon$
B가 실수를 할 확률: ε
B의 착한 행동에 대한 A의 이득: 10
B의 실수에 대한 A의 이득: -1000

이 경우 플레이어 A의 착한 행동 전략 선택에 따른 기대이득은 $10(1-\varepsilon)+(-1000)\varepsilon$ 이다.
마찬가지로, 플레이어 A의 악의적 행동 전략 선택에 따른 기대이득은 다음과 같다.

$9(1-\varepsilon) + 8\varepsilon$

플레이어 A의 기준에서 착한 행동 전략을 취하는 경우는 착한 행동의 기대이득이 더 큰 경우일 것이므로 $10(1-\varepsilon) - 1000\varepsilon > 9(1-\varepsilon) + 8\varepsilon$, 따라서 $\varepsilon < 1/1009$이다.

다시 말해 플레이어 B가 실수(악의적 행동)를 할 확률이 1/1009보다 작다고 판단될 때, 플레이어 A는 착한 행동을 취하게 될 것이며, 그 반대의 경우라면 악의적 행동을 취하게 될 것이다.

2.4. 죄수의 딜레마, 파레토 효율과 사회적 딜레마

2.4.1. 죄수의 딜레마

죄수의 딜레마(Prisoner's Dilemma)는 게임이론에서 널리 인용되는 대표적인 게임이다. 게임의 상황은 다음과 같다. 살인 및 절도 용의자 2명이 체포되었다. 살인 사건의 명확한 증거는 없지만 절도죄에 대한 증거는 존재한다. 서로 다른 취조실에 있는 각 용의자는 아래의 정보를 함께 알고있다.

1. 한 용의자만 범죄 혐의에 대해 자백하고 다른 용의자는 침묵을 지키는 경우, 자백한 용의자는 모든 형량을 감면 받는다. 반면에 끝까지 침묵을 지킨 용의자는 살인죄 형량 9년과 절도죄 형량 1년, 총 10년의 형량을 모두 받는다.

2. 두 용의자 모두 죄를 자백하면, 함께 형을 감면 받아 각각 5년의 형량을 받는다.

3. 반대로 두 용의자 모두 죄를 자백하지 않으면, 살인죄에 대한 증거는 없으므로 두 용의자 모두 절도죄에 대한 형량 1년씩만 받게 된다.

		용의자 B	
		침묵	**자백**
용의자 A	**침묵**	-1, -1	-10, 0
	자백	0, -10	-5, -5

[표6] 죄수의 딜레마

[표6]을 보면 용의자 A는 용의자 B가 무슨 선택을 하든지 '자백'을 선택하는 것이 유리하며, 이는 용의자 B도 마찬가지이다. 그러나 두 용의자가 모두 '자백'을 선택하게 되면, 두 용의자 모두 '침묵'을 선택했을 때보다 더 많은 형량을 받게 된다.

이번에는 용의자 A와 B가 한 공간에 머무르면서 의견을 교환한 후, 둘 다 침묵을 지키기로 약속한 상황을 가정해보자. (물론, 자신의 최종 결정은 개별적으로 한다.) 두 용의자는 협력을 약속하였지만, 둘 중 하나는 자신의 이득을 극대화하기 위해 '자백'을 선택할 수 있고, 이 사실을 두 용의자 모두 인지하고 있다면 결국에는 딜레마에 빠지게 된다. 게임이론에서 각 플레이어는 자신의 이득을 최대화하기 위한 전략을 선택한다. 따라서, 두 용의자 모두 언제나 '자백'을 선택하여 더 많은 이익을 얻을 수 있으므로 두 용의자의 우월전략은 '자백'이 되고, (자백, 자백)은 우월전략균형이 된다.

2.4.2. 3인 이상의 죄수의 딜레마

죄수의 딜레마에서 용의자가 2인이 아니라 3인 이상이라도 결과는 같다. 즉, 게임에 참여하는 플레이어의 수에 관계없이 모든 플레이어는 자백을 선택하는 것이 언제나 유리하다. 따라서 모든 플레이어가 자백을 선택하는 우월전략균형이 성립한다.

2.4.3. 죄수의 딜레마의 응용

죄수의 딜레마 모델은 다양한 사회정치 상황과 비슷하다. 예를 들어, A 기업과 B 기업이 신제품을 두고 가격을 경쟁하는 상황이 있다고 가정해보자. A 기업이 제품 가격을 내리면, B 기업보다 가격 면에서 우위를 차지하기 때문에, 더 많은 소비자의 선택을 얻게 된다. 반대로 B 기업은 가격을 내리지 않아서 매출이 줄어든다. 이는 A와 B 기업의 상황을 바꾸어도 같다. 따라서, A와 B 기업 모두 이득의 최대화를 위해 가격을 내리는 선택을 하게 되고, 이 경우 두 기업 모두 가격 전쟁을 하지 않았을 때보다 총매출이 감소하게 된다.

2.4.4. 반복적 죄수의 딜레마 [3][4]

죄수의 딜레마 모델은 기본적으로 한 번의 상황을 전제로 하기 때문에 '자백' 즉, 배신을 하는 선택이 각 플레이어 모두에게 우월전략이다. 그러나 앞에서 이야기한 기업의 가격 전쟁 사례처럼, 현실 사회에서는 죄수의 딜레마의 사례가 반복적으로 발생한다. 미시간 대학의 로버트 액설로드(Robert Axelrod) 교수는 전 세계의 경제학, 정치학, 수학, 사회학, 심리학 등의 전문가 집단을 초청하여 반복적 죄수의 딜레마 게임(Iterated Prisoner's Dilemma Game) 대회를 열었다.

두 번의 대회가 개최되었는데, 모두 팃포탯(Tit for Tat) 전략[2]을 사용한 경우 우승하였다. 반복적 죄수의 딜레마 게임에서 팃포탯 전략은 우선은 '협력'을 선택하고, 그 다음부터는 상대 플레이어가 선택한 전략을 그대로 선택하는 방법이다. 즉, 상대 플레이어가 '협력'하면 나도 '협력'하고 상대가 '배반'하면 똑같이 나도 '배반'하는 전략이다.

이 게임에서 각 플레이어가 모두 '협력'을 선택한 경우 각 3점, 한 플레이어만 '협력'을 선택하고 상대 플레이어는 '배신'을 선택한 경우 각각 0점과 5점을 얻는다. 양쪽 모두 '배신'을 선택한 경우 각각 1점씩을 얻는다. 총 200회의 양자택일의 결과의 총합이 가장 높은 점수를 얻은 플레이어가 우승한다. 따라서, 이론적으로 한 플레이어가 200번의 게임 모두에서 '배신'을 선택하고, 다른 플레이어는 모두 '협력'을 선택하게 만든다면 '배신'을 선택한 플레이어는 최대 1,000점을 획득하여 우승할 수 있다. 그러나 실질적으로는 두 플레이어 모두 자신의 이득을 최대화하는 전략을 선택하며, 이 경우 두 플레이어의 이득은 모두 1,000점보다 훨씬 낮아지게 된다. 팃포탯 전략을 선택하여 우승한 아나톨 라파포트(A. Rapoport)는 504.5점을 기록하였는데, 협력을 이끌어 내기 위한 팃포탯 전략의 원칙은 다음과 같다.

1. 반드시 협력한다.
2. 단, 상대 플레이어가 배신할 경우에는 반드시 응징한다.
3. 응징 후에는 용서한다.

4. 상대 플레이어가 나의 행동 패턴을 이해하도록 명확한 전략을 사용한다.

이처럼 반복적 죄수의 딜레마 게임 대회의 결과를 통해 협력(Cooperation)이 최선의 전략임을 알 수 있다. 물론 현실 세계에는 게임의 결과에 영향을 끼치는 다양한 변수들이 존재하고 인간이 이기적인 존재라는 점을 감안하면, 플레이어 간의 조건 없는 협력(Unconditional cooperation)을 기대하기는 쉽지 않다. 따라서, 제도적 차원에서 각각의 플레이어들이 최대의 협력을 할 수 있는 장치를 마련하는 것이 중요하다.

2.4.5. 파레토 효율[5]과 사회적 딜레마

앞서 살펴본 죄수의 딜레마의 예에서 우리는 우월전략균형이 언제나 모두에게 최적의 결과를 가져오지는 않는다는 것을 확인하였다. 그렇다면 과연 모두에게 최적인 균형상태는 존재할 것인지, 존재한다면 어떻게 정의할 수 있을 것인지 알아보기 위해, 다시 죄수의 딜레마의 이득표를 살펴보자.

		용의자 B	
		침묵	**자백**
용의자 A	**침묵**	-1, -1	-10, 0
	자백	0, -10	-5, -5

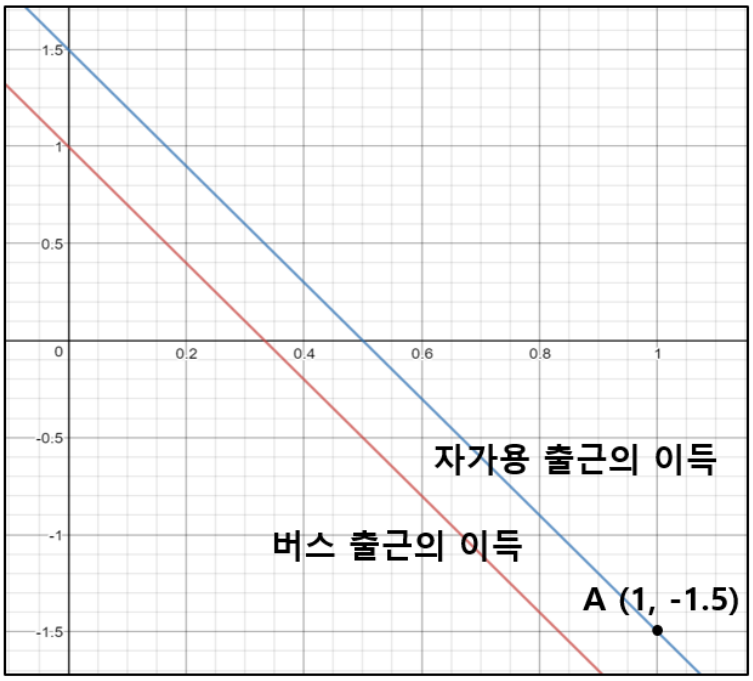
[표7] 죄수의 딜레마

[표7]의 게임에서 모두에게 최적인 균형상태를 찾기 위해 외부 관찰자 1명을 초대하자. 외부 관찰자는 용의자 A와 용의자 B의 이득 중, 어느 것에도 가중치를 두지 않는다. 외부 관찰자는 한 용의자의 이득을 더 나빠지지 않게 하면서, 다른 용의자의 이득을 증가시키도록 상황을 개선하는 역할을 맡는다. 이 경우, 외부 관찰자의 관점에서 두 용의자가 모두 '침묵'을 선택하게 하려면 개입이 필요하다. 두 용의자 모두 '자백'을 선택하는 경우의 이득은 둘 다 -5로 손해이다. 만약 두 용의자가 모두 '침묵'을 선택하는 경우로 균형점을 이동시킨다면, 두 용의자 모두 손해보지 않으면서 다른 한 용의자의 이득을 개선시킬 수 있다. 심지어 이 경우에는 두 용의자의 이득이 모두 개

선된다. 이를 파레토 개선이 가능한 상황이라고 이야기한다. 여기서 재미있는 사실은, 죄수의 딜레마에서의 내쉬 균형은 게임에서의 파레토 비효율 상태라는 점이다. 이것이 이 게임을 딜레마라고 칭하는 이유다.

논의를 조금 더 확장해보면 다음과 같다. 두 가지의 출근 수단만이 존재하는 도시가 있다. 사람들은 아침마다 '자가용 출근'과 '버스 출근' 두 가지의 전략 중 한 가지를 선택한다. '자가용 출근'은 출근지까지 걸리는 시간 및 노력 비용을 감소시키지만, 도시 전체의 혼잡도를 가중시켜 교통 체증을 야기한다.

[도표1]은 이를 그래프로 나타낸 것이다.



[도표1] 출근 게임의 이득

[도표1]을 살펴보면, 자가용 통근자의 비율과 상관없이, 언제나 모든 플레이어는 '자가용 출근'을 선택하는 것이 이득이다. 따라서, 이 경우 모든 플레이어가 자가용 출근을

하는 A(1, -1.5)에서 우월전략균형이 성립한다. 그러나 이 때, 모든 플레이어의 이득은 -1.5가 되어, 사회적 딜레마 또는 공유지의 비극을 가져오게 된다. 만약 이 경우에 객관적인 관찰자가 개입한다면, 죄수의 딜레마처럼 파레토 개선이 가능한지 알아본다. [도표1]을 보면 외부 관찰자가 개입해 자가용으로 출근하는 20%가 버스로 출근하도록 조정하는 경우, 전체 사회적 효용은 모두가 자가용으로 출근했을 시의 사회적 효용보다 높다. 따라서 이 경우 역시 파레토 개선의 사례라고 할 수 있다.

2.5. 3인 게임

3인 게임에서는 위에서 제시했던 2인 게임과는 달리 플레이어가 한 명 더 추가됨에 따라 연합, 훼방, 공공재 문제 등 현실에서 발생하는 폭넓고 다양한 문제들이 발생 가능하며, 고려해야 하는 변수들도 다양해진다. 따라서 3인 게임의 연합, 훼방, 공공재의 문제를 하나씩 짚어보고자 한다.

2.5.1. 연합

		플레이어 C			
		착한 행동		**악의적 행동**	
		플레이어 B		**플레이어 B**	
		착한 행동	**악의적 행동**	**착한 행동**	**악의적 행동**
플레이어 A	**착한 행동**	6, 6, 6	4, 4, 4	4, 4, 4	1, 7, 7
	악의적 행동	4, 4, 4	7, 7, 1	7, 1, 7	0, 0, 0

[표8] 3인 게임

[표8]는 3인 게임의 이득표이다. 왼쪽 플레이어의 이득은 왼쪽에, 오른쪽 플레이어의 이득은 두 번째에 기재되며, 세 번째 플레이어의 이득은 가장 오른쪽에 기재된다. 플레이어 A의 전략은 '착한 행동'과 '악의적 행동' 두 가지이며, 이는 플레이어 B와 C에도 동일하게 적용된다.

플레이어 A의 입장에서 '착한 행동'을 선택하는 경우의 이득은 플레이어 B와 C의 선

택에 따라 달라진다. 플레이어 B가 '착한 행동', 플레이어 C가 '착한 행동'을 하는 경우 플레이어 A의 최선반응은 '착한 행동'이다. 같은 방식으로 플레이어 C는 여전히 '착한 행동'을 선택하는 상황에서, 플레이어 B가 '악의적 행동'을 선택하는 경우, 플레이어 A의 기대 이득은 달라지며, 이 경우의 플레이어 A의 최선반응은 '악의적 행동'이 된다.

같은 방식으로, 각 플레이어의 최선반응은 각 상황에서 상대 플레이어의 전략에 따른 기대이득을 비교하여 정하게 된다. 각 플레이어의 최선반응에 의한 내쉬 균형은 총 4개로, 플레이어 A, B, C 가 각각 (착한 행동, 착한 행동, 착한 행동), (악의적 행동, 악의적 행동, 착한 행동), (악의적 행동, 착한 행동, 악의적 행동), (착한 행동, 악의적 행동, 악의적 행동)을 선택하는 경우이다.

이 게임에서 가장 사회적으로 바람직한 전략은 세 플레이어가 대연합을 하는 경우로, 이 경우 세 플레이어의 전략은 모두 '착한 행동'이 된다. 그러나 만약 별다른 제약사항이 없는 상황에서 두 플레이어가 연합이 가능하도록 상황이 만들어진다면, 연합하는 두 플레이어는 악의적 행동을 통해 6보다 높은 7의 이득을 얻어 가려고 할 것이다. 그 경우 '착한 행동'을 선택한 개별 플레이어는 큰 손해를 보게 된다. 이러한 연합이 발생하는 경우, 명확한 종류의 규칙이나 시행 장치가 없다면 대연합으로 균형을 이루기는 쉽지 않을 것이다.

2.5.1.1. 협조게임과 대연합 균형 달성

게임이론에는 두 가지 종류의 해가 존재한다. 하나는 각자가 자신의 선택이 상대방에게 어떤 영향을 끼칠지 고려하지 않고 자신의 이득만을 최대화하는 비협조(Non-cooperative) 해이다. 죄수의 딜레마의 균형이 이에 해당한다. 다른 하나는 전체 집단을 위한 최선의 결과를 달성하기 위해 플레이어들이 전략을 조정하는 협조(Cooperative) 해이다. 연합은 그 종류에 따라 대연합, 개체연합, n인 연합 등으로 나타낼 수 있다.

[표9]에서 확인할 수 있듯, 3인 연합 혹은 2인 연합 시의 이득이 개별적으로 얻을 수 있는 이득에 비해 크다는 것을 알 수 있다. 다음으로 합리적 연합과 잉여 이득, 그리고 그 분배에 대해 알아보자.

K, L, M	10
K, L	6
L, M	6
K, M	6
K	2
L	2
M	2

[표9] 연합의 이득

현재 3명의 플레이어 K, L, M이 있다. 각 플레이어는 자신의 이득 극대화를 위해 행동하며 연합형태에 따라 [표9]에 상응하는 이득을 가져갈 수 있다.

각 플레이어가 개체연합 즉, 단일 행동을 한다면 각각 2의 이득을 취할 수 있다. 그러나 2인이 연합을 하게 된다면 각 연합은 6의 이득을 취할 수 있다.
y_k, y_l, y_m을 각각 K, L, M의 기대이득이라고 하면 3인 연합의 기대이득은,

$$y_k + y_l + y_m = 10$$

이고, 3인 연합을 이루기 위해서는 각 플레이어의 3인 연합 시 기대 이득이 2인 연합의 기대 이득보다 반드시 크거나 최소한 같아야 하므로 다음과 같이 된다.

$$y_k + y_m \geq 6$$
$$y_l + y_m \geq 6$$
$$y_k + y_l \geq 6$$
$$\rightarrow 2(y_k + y_l + y_m) \geq 18$$
$$\rightarrow y_k + y_l + y_m \geq 9$$

그러므로 각 2인 연합이 3인 연합을 형성했을 시의 기대이익은 $y_k + y_l + y_m \geq 9$이며, 실제 3인 연합 시의 이득은 10이므로, 이 경우 3인 연합에서의 이득은 각 플레이어가 2인 연합을 구성하였을 경우 얻을 수 있는 이득을 보장한다. 이 경우 3인 연합에서 균형이 성립한다.

2.5.2. 훼방

		플레이어 C			
		착한 행동		악의적 행동	
		플레이어 B		플레이어 B	
		착한 행동	악의적 행동	착한 행동	악의적 행동
플레이어 A	착한 행동	45, 50, 1	45, 49, 3	45, 53, 0	45, 52, 0
	악의적 행동	48, 45, 2	47, 46, 3	48, 48, 0	46, 51, 0

[표10] 훼방자가 있는 게임

훼방이란 연합과는 달리 자신은 이길 수 없으나 다른 플레이어가 승리하지 못하도록 막을 수 있는 전략적 선택을 할 수 있는 경우를 뜻한다. [표10]과 같은 경우 플레이어 C는 다른 두 플레이어에 비해 영향력이 크지 않다.

위의 [표10]에서 확인할 수 있듯이 이 경우 내쉬 균형은 A, B, C = (악의적 행동, 악의적 행동, 착한 행동)에서 이루어진다. 여기서 가장 중요한 부분은 내쉬 균형에서 가장 큰 이익을 가져가는 플레이어는 A라는 점이다. 그러나 플레이어 C는 최대 수혜자를 선택할 수 있는 권한을 가지고 있다. 즉 훼방꾼이 될 수 있다. 만약 C가 3이라는 이익을 포기하고 '악의적 행동'으로 전략을 변경한다면 게임은 플레이어 B가 최대 수혜자로 바뀔 수 있다.

2.5.3. 공공재

공공재는 어떠한 경제주체에 의해서 생산이 이루어지면 구성원 모두가 소비 혜택을 누릴 수 있는 재화 또는 서비스를 지칭하는 용어로, 다른 서비스나 재화와 다르

게 두 가지의 고유한 성질을 가진다.

1. 비경합성

재화/서비스의 소비 과정에서 경합이 일어나지 않는 경우이다. 다시 말해 한 사람의 소비가 다른 사람의 소비를 방해하지 않는다는 뜻이다. 예를 들어 음식과 같은 재화는 내가 먹어 버리면 다른 사람이 못 먹게 되지만, 음악은 내가 듣는다고 해서 다른 사람이 못 듣게 되지는 않는다.

2. 비배제성

재화 소비에 대한 비용을 지불하지 않고 소비하더라도, 이를 배제할 수 없는 경우이다. 흔히 무임승차(Free-riding)라 부르며, 공공재가 문제가 되는 것은 바로 이러한 배제 불가능성(무임승차)에 기인한다.

		플레이어 C			
		착한 행동		No action	
		플레이어 B		**플레이어 B**	
		착한 행동	No action	**착한 행동**	No action
플레이어 A	**착한 행동**	15, 15, 15	5, 20, 5	5, 5, 20	-5, 10, 10
	No action	20, 5, 5	10, 10, -5	10, -5, 10	0, 0, 0

[표11] 공공재의 딜레마

[표11]를 보면 게임에 우월전략균형이 존재한다는 것을 확인할 수 있다. 각 플레이어의 우월전략은 별다른 비용을 지출하지 않고 타 플레이어의 착한 행동을 통해 제공되는 서비스를 사용만 함으로써 자신의 이익을 극대화하는 것이다. 결국 그 누구도 공공의 최대이익을 위한 착한 행동을 하지 않게 되고 해당 게임은 아무도 이득을 누릴 수 없는 비효율적 균형에 이르게 된다. 물론 이 경우도 [표11]의 연합과 마찬가지로 두 플레이어 간의 연합을 통해 더 높은 수준의 이득을 얻을 수 있지만, 해당 연합의 결과는 내쉬 균형이 아니므로 결국 플레이어의 배신으로 원래 균형인 모두 'No action' 상태로 회귀하게 될 것이다. 결국, 이러한 공공재적 상황에서는 어떤 형태로

든 강제 협약이 시행되지 않는다면 사회적 딜레마에서 벗어날 수 없다.

2.6. 결론

앞서 우리는 게임이론의 주요 이론과 유형을 함께 살펴보았다. 게임이론에 따르면, 게임에 참여하는 주체들은 합리성과 일관성을 갖추고 있다는 전제하에, 주어진 모든 정보를 활용하여 언제나 이득을 최대화하는 전략을 선택한다. 챕터 4에서는 본 챕터에서 소개한 게임이론이 실제 이더리움 Casper FFG의 설계에 어떻게 반영되어 있는지 알아보기로 한다. 또한 이번 챕터에서 예시로 든 모든 상황을 정규형 표와 이득(Payoff)으로 나타낸 것처럼, 이더리움 Casper FFG에서 문제로 제시한 상황과 그 해법으로 제시한 인센티브 구조를 게임이론적 해석을 통해 정규형 표와 이득(Payoff)으로 풀어서 알아보고자 한다.

3. 분산 시스템에서의 Consensus

3.1. 소개

Casper FFG는 인센티브 메커니즘을 통해 분산 네트워크에 참여하는 경제적 인간이 서로의 이타심에 기대지 않고도 안전하게 네트워크상에서 합의를 이루는 것을 목표로 한다. 따라서, Casper FFG 를 파악하기 위해서는 분산네트워크의 특징에 대한 이해가 필요하다. 본 챕터에서는 분산 시스템의 특성을 설명한 이론 중 FLP impossibility에 대해 알아보고, 분산 네트워크에서의 합의를 위해 필요한 요소로서의 동기성 및 부분 동기성 가정(Partial synchrony assumption)과 PBFT (Practical Byzantine Fault Tolerance)에 대해 알아보고자 한다.

3.2. FLP Impossibility

3.2.1. FLP Impossibility

FLP Impossibility result는 1985년 Fischer, Lynch, Paterson이 공동 저술한 "Impossibility of Distributed Consensus with One Faulty Process"[6] 논문에서 나온 개념이다. 논문에 따르면, 비동기 네트워크 환경에서는 실패할 가능성이 있는 노드가 단 하나라도 있으면, Safety와 Liveness 두 가지 속성을 동시에 만족시키는 합의 방식은 불가능하다. 저자들은 이 공로를 인정받아 2001년 분산 컴퓨팅에서 가장 영향력 있는 Dijkstra Prize를 수상하였다.

3.2.2. Safety and Liveness

분산 시스템에서 합의를 달성하기 위한 가장 중요한 두 가지 속성은 Safety와 Liveness이다. Safety란, '모든 올바른 노드가 같은 상태(State)에 동의해야 한다.' 즉, 노드 간의 잘못된 합의가 없음을 의미한다. Liveness란, 노드가 결국에는 같은 상태에 도달해야 한다. 즉, 노드 간의 합의는 언젠가는 반드시 이루어짐을 의미한다.

3.3. 비동기 시스템, 동기 시스템과 부분동기 시스템

3.3.1. 비동기 시스템(Asynchronous system)

비동기 환경의 특성상 메시지에 대한 응답 시간(Response time)에 제한이 없기 때문에 노드에 직접 문제가 발생한 건지 아니면 단순히 응답 시간이 오래 걸렸는지 확인할 수 없다. 따라서, 이를 극복하기 위해 네트워크의 합의 메커니즘은 반드시 결함 내성(Fault-tolerance)의 특성을 지녀야 한다. 비동기 네트워크에서의 결함 내성(Fault-tolerance)을 달성하기 위해 필요한 추가적인 조건은 네트워크 환경에 따라 크게 동기(Synchronous)와 약한 동기(Partial synchronous/ Weakly synchronous)로 나뉜다.

3.3.2. 동기 시스템(Synchronous system)

노드 간의 메시지 전송 지연에 대해 상한선이 존재한다. 프로세스 요청(Process request) 전송과 결괏값의 응답(reply) 사이에 제한 시간을 설정하고, 프로세스(Process)의 실행 시간에도 제한을 설정한다. 메시지 지연 시간(Message latency)이 엄격히 정의되어 통제되는 경우에만 적용이 가능하다. (제한 시간에서 시간 지연이 조금이라도 발생하는 경우 해당 프로세스는 실패로 처리 된다.) 따라서 실제 분산 네트워크 환경에서 동기식 모델을 도입하는 것은 위험 부담이 될 수 있다.[7]

3.3.2.1. 동기 시스템(Synchronous system)에서의 합의 알고리즘

Nakamoto Consensus

비트코인 창시자로 알려진 사토시 나카모토가 제안한 합의 알고리즘으로서, 오랫동안 컴퓨터 과학에서 어려운 문제 중 하나였던 비잔틴 장군 문제에 대한 솔루션을 제시하였다. Nakamoto Consensus에서는 마이너들이 연산 작업을 통해 주어진 문제의 답을 찾으면 유효한 블록이 생성되어 체인을 이어나간다. 이렇게 만들어진 가장 긴 체인을 정격 체인(기준이 되는 단 하나의 유효한 체인, Canonical chain)이라 한

다. 따라서, 비트코인의 경우 Liveness (Availability)를 우선 확보하고 6컨펌(60분)을 통한 거래의 완결성(Finality)을 확률적(Probabilistic)으로 얻어 Safety (Consistency)를 보완한다.

또한, Nakamoto Consensus는 일반적으로 체인 기반의 합의 알고리즘(Chain-based consensus algorithm)으로 불린다. 초기의 지분 증명 방식(PoS)에서도 체인 기반의 합의 알고리즘을 채택하여 사용하였다. 이 알고리즘은 각 슬롯마다 유사 난수 생성(Pseudo-random number generation) 방식으로 검증인을 선택하여 하나의 블록을 생성할 권리를 주며 생성된 블록은 이전 블록(가장 긴 체인의 마지막 블록)의 뒤에 붙게 된다. 따라서 체인 기반의 지분 증명 방식 또한 Safety를 희생하여 Liveness를 확보하는 방식이지만, Nothing-at-stake와 Long-range attack 등의 문제로 인해 현재는 BFT 기반의 지분 증명 방식이 일반적이다.

3.3.3. 부분 동기성(Partial synchronous/Weakly synchronous)

부분 동기성 시스템은 동기성(Synchronous) 및 비동기성(Asynchronous) 특성이 번갈아 가며 나타난다. 비동기 네트워크에서의 Safety와 Liveness 달성을 위해 타임아웃(Timeout)을 설정 하나, 타임아웃의 상한선은 정해져 있지 않다는 약한 동기성 가정(Weak synchronous assumption)을 추가하여 결함 내성(Fault-tolerant)을 달성한다.

3.3.3.1. 부분 동기 시스템에서의 합의 알고리즘

전통적인 분산 시스템에는 다양한 BFT 계열 합의 알고리즘이 존재한다. 그중 가장 잘 알려진 합의 알고리즘은 PBFT로, 비잔틴 노드가 존재할 수 있는 비동기 네트워크에서 참여자 간의 합의를 이끌어 낼 수 있다는 특성을 지닌다. PBFT 계열의 대표적인 블록체인 합의 알고리즘으로는 Cosmos의 Tendermint가 있다. Tendermint는 부분 동기성 네트워크 모델(Partial-synchronous model)에서 개선된 PBFT 합의 방식과 BPoS(Bonded Proof of Stake)방식을 통해 Safety를 확보한다. 부분 동기성 시

스템에서는 특정 시간 안에 메시지가 도착할 수 있지만 그 특정 시간을 노드는 알 수 없다. 때문에, 이를 약한 동기성(Weakly synchronous)이라 부르기도 한다. (PBFT와 Tendermint에 대한 자세한 설명은 이더리움연구회 4기 기술리서치 분과 보고서를 참고 바란다.)

3.3.3.2. PBFT (Practical Byzantine Fault Tolerance)[8]

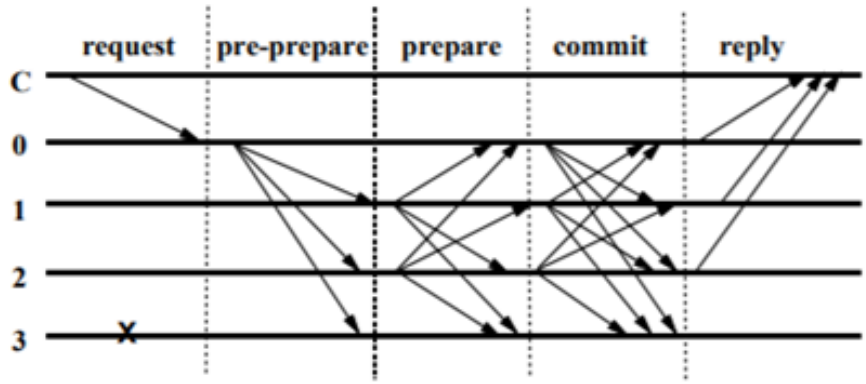
비동기 네트워크에서 악의적인 노드(Faulty node)가 1/3을 넘지 않는다면, 약한 동기성 가정(Weak synchrony assumption)을 통해 Liveness를 달성할 수 있음을 증명하였다. 약한 동기성 가정은 다음과 같다.

- 1/3 이하의 노드(Replica)만이 악의적(Faulty) 노드라면, 시간 지연이 무한하지 않기 때문에, 클라이언트는 결국 요청에 대한 응답을 받는다.
- 시간 지연은 메시지가 처음으로 전송된 시점과 목적지에서 수신된 시점 사이의 시간(보낸 사람이 메시지가 수신될 때까지 메시지를 계속해서 다시 전송한다고 가정)으로 정의할 수 있다.

합의 과정은 다음과 같다.

1. 클라이언트는 리더 노드인 Primary에게 요청(Request)을 전송한다.
2. Primary는 Back-up 노드(Primary를 제외한 나머지)에게 클라이언트의 요청을 정렬하여 전송한다.
3. 각각의 노드는 해당 요청을 실행하고 검증 작업을 진행한다. 검증이 완료되면 해당 요청에 대한 답변을 클라이언트에게 전송한다.
4. 클라이언트는 f+1개 이상의 동일한 결과를 서로 다른 노드로부터 전달받으면 해당

요청은 문제없이 처리된 것으로 확인한다.



[도표2] 정상 상황에서의 PBFT 합의 알고리즘의 합의과정

3.3.3.3. PBFT의 문제점

PBFT 합의 알고리즘에는 다음과 같은 문제점이 존재한다. 먼저, Safety와 Liveness가 달성되기 위한 가장 중요한 조건인 $f \leq \frac{(n-1)}{3}$을 반드시 만족하여야 하며, 이를 만족하지 못하는 경우 Safety와 Liveness는 보장되지 않는다는 단점이 있다. 또한 합의 과정에서의 결괏값은 다수에 의해 지지되는 값이므로 시스템에서 다수의 영향력이 커지게 되고, 영향력이 경제적 유인과 연결되는 경우 다수에 의한 시스템 공격(Traditional 51% Attack, Majority Censorship 및 Discouragement Attack)이 발생할 수 있다는 문제점 역시 존재한다. 다음 챕터를 통해 이더리움이 PBFT 합의 알고리즘의 문제점을 경제적 구조를 통해 어떻게 해결하려 하였는지 알아보고자 한다.

4. Casper FFG – Perspective of Cryptoeconomics

분산 네트워크 환경에서 가장 중요한 것은 네트워크에 참여한 모든 노드가 실행되는 하나의 프로세스(Process)에 대해 동일한 결괏값을 보장받는 것이다. 그러나 챕터 3에서 확인한 내용처럼, 실제 분산 네트워크 환경에서 이를 달성하는 것은 쉽지 않다. Casper FFG는 분산 네트워크 환경에서 합의(Consensus)의 어려움을 메커니즘 디자인을 통해 극복하려는 시도이다.

4.1. Casper FFG의 설계 원칙

4.1.1. Economic Security and Mechanism Design

Casper FFG는 이더리움 재단의 경제 철학이 반영된 Economic protocol이다. 그 첫 번째 철학은, '모든 참여자는 게임이론에 입각하여 의사 결정을 한다.'는 것이며, 두 번째는 '시스템의 설계 시 모든 의사 결정의 결과가 시스템을 유지하는 역할을 한다.'는 것이다. 이를 위하여, Casper FFG는 이더리움 네트워크에 검증인(Validator)으로 참여하는 자격을 지분(Stake)을 예치한 경우로 제한하여 참여에 따르는 의무를 부과한다. 또한 이 의무에 경제적 이득을 연결해, 참여자가 자발적으로 의무를 시행하게 한다. 따라서 Casper FFG는 참여자를 경제적 인간(Econ)으로 가정하며, 이들의 이기적 행위가 시스템에 가할 수 있는 위해를 분석하고, 메커니즘 디자인을 토대로 이 문제점을 극복하기 위한 보상과 처벌 시스템을 설계하였다.

4.1.2. BFT의 문제점을 극복하기 위한 설계

4.1.2.1. 비잔틴 정족수 이상이 (억지로라도) 합의에 동의할 수 있도록 설계

Casper FFG는 비잔틴 결함을 극복하기 위해 경제적 보상과 처벌을 설계하여, Safety와 Liveness 모두 달성하고자 한다. 앞서 살펴본 바와 같이, 부분 비동기 네트워크에서 Safety와 Liveness를 달성하도록 하는 가장 중요한 조건은 비잔틴 정족수의 충족이다. 따라서 비잔틴 환경에서 2/3 이상의 정직한 참여자가 합의 과정에 참여하지 않는다면 Safety 와 Liveness는 달성될 수 없다. 하지만 이더리움 네트워크의 참여자는 경제적 인간이다. 그러므로 이들의 이타심에만 기댄다면 비잔틴 결함 내성(BFT)은 달성되지 않을 것이고, 네트워크의 안정성(Security) 역시 기대할 수 없다.
이를 해결하기 위해 이더리움은 Casper FFG를 통해 Accountable safety와 Plausible liveness의 개념을 도입하였다. 이를 통해 경제적 인간의 전략적인 이득 추구 행위에 의해 네트워크가 Safety와 Liveness를 자발적으로 확보하게 하였다.

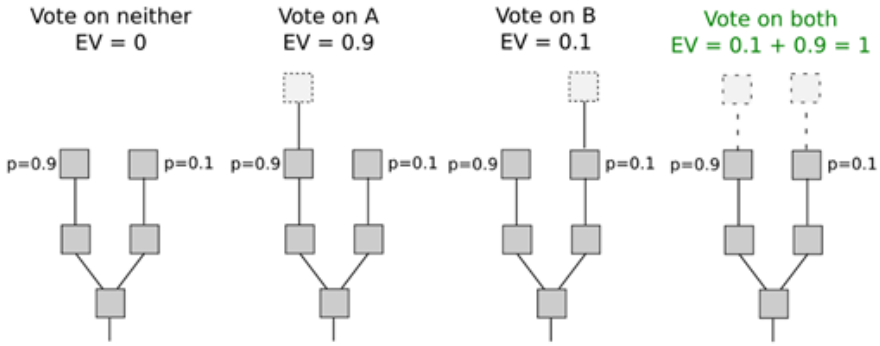
i. Nothing-at-stake; Accountable Safety

Casper FFG에서의 검증인(Validator)의 가장 중요한 역할은 체크포인트(checkpoints, 매 50블록마다 1개씩 생성됨)에서의 투표이며 이는 [v, t, h(t), h(s), S] 형태의 투표 트랜잭션(vote transaction)을 전송하여 이루어진다.
정상적인 상황에서 각 체크포인트는 2/3 이상의 투표를 받아 1차 검증(justified)된다. 연속으로 2개의 체크포인트가 1차 검증(justified)되면, 이전의 체크포인트는 최종 확정(finalized)된다. 이 때, 같은 높이의 두 개의 체크포인트가 동시에 최종 확정(finalized)되는 상황은 네트워크의 분할(fork)을 일으킬 수 있다. 다음은 이러한 상황을 일으키는 Nothing-at-stake에 대한 설명과 그 해결책에 대한 내용이다.

Notation	Description
v	The validator index
t	The hash of the ‘target’ checkpoint
h(t)	The height of the target checkpoint in the checkpoint tree
h(s)	The height of the source checkpoint in the checkpoint tree
S	Signature of (v, t, h(t), h(s)) from the validator’s private key

[표12] 투표 트랜잭션의 내용

Nothing-at-stake[9]란, 네트워크 분할(Fork)이 일어났을 때, 두 개의 체인 모두에 투표하는 것이 가장 이득인 상황이다. 즉, 투표 행위에 대한 보상만이 존재하여, 참여자들이 두 개의 체인 모두에 투표함으로써 지속적으로 네트워크 분할(Fork)이 발생할 가능성이 있는 상황으로 정의할 수 있다.



[도표3] Nothing-at-stake

A에 투표하는 경우의 이득을 ER(Expected Return)이라고 하였을 때, ER은 A가 정격 체인(Canonical chain)으로 채택될 확률(p)‘에 ‘블록 생성 보상(r)’을 곱한 값으로 정의할 수 있다.

$$ER = probability\ (p) \times reward\ (r)$$

따라서 투표를 하지 않는 경우의 ER은 $0.9 \times 0 + 0.1 \times 0 = 0$이 된다. 동일한 방식을 적용하면, A 에만 투표하는 경우의 ER은 0.9, B 에만 투표하는 경우의 ER은 0.1, 두 체인 모두에 투표하는 경우의 ER은 1이 되어, 검증인은 두 체인 모두에 투표하는 전

략을 통해 가장 큰 이득을 얻게 된다.

게임이론적 해석(Game theoretic interpretation)

포크(Fork)가 발생한 상황에서, 두 명의 검증인이 두 체인에 투표하여 이에 따른 경제적 보상을 받는 2인 투표 게임(Voting game)을 가정한다. 게임의 규칙은 다음과 같다.

1. 두 명의 검증인은 두 개의 체인 중 어느 체인에 투표할 지 결정한다.
2. 검증인이 선택할 수 있는 전략은 '두 체인에 모두 투표, 체인 A에만 투표, 체인 B에만 투표, 어느 체인에도 투표하지 않음'의 총 네 가지이다.
3. 이득(Payoff)은 ER로 나타낼 수 있으며, [표14]는 이에 대한 식과 이득표(Payoff matrix)이다.

$$ER = \text{probability } (p) \times \text{reward } (r)$$

		검증인 2			
		Vote on neither	Vote on A (p=0.9)	Vote on B (p=0.1)	Vote on both
검증인 1	Vote on neither	0, 0	0, 0.9	0, 0.1	0, 1
	Vote on A (p=0.9)	0.9, 0	0.9, 0.9	0.9, 0.1	0.9, 1
	Vote on B (p=0.1)	0.1, 0	0.1, 0.9	0.1, 0.1	0.1, 1
	Vote on both	1, 0	1, 0.9	1, 0.1	1, 1

[표13] 2인 투표 게임

이 경우, 검증인 1의 우월전략은 '두 체인에 모두 투표'를 선택하는 것이고, 마찬가지로 검증인 2의 우월전략 역시 '두 체인에 모두 투표'를 선택하는 것이다. 따라서 내쉬균형은 양쪽 투표(Vote on both, Vote on both)에서 성립한다. 하지만 이는 네트워크 분할(Fork)을 조장하는 상황이므로, 이 상황이 지속적으로 발생한다면 시스템은 유지

될 수 없다. Casper FFG에서는 이 문제를 해결하기 위해 몰수 조건(Slashing condition)을 제시한다.

몰수 조건(Slashing condition)

두 개의 체인 모두에 투표하는 명백한 악의적인 행위를 처벌 조건(Penalty condition)으로 정의하여 Nothing-at-stake 문제를 해결한다. 이 처벌 조건(Penalty condition)을 통해 네트워크 내의 내쉬 균형은 '두 체인에 모두 투표'(Vote on both, Vote on both)에서 정격 체인이 될 확률이 높은 한 체인에 투표(Vote on A, Vote on A)로 이동한다.

게임이론적 해석(Game theoretic interpretation)

Nothing-at-skate 에서의 투표 게임(Voting game)과 동일한 게임, 동일한 가정을 적용하나, 다음 두 가지의 가정이 추가된다.

1. 게임에 참여하기 위해서 일정 금액의 보증금을 시스템에 예치한다.
2. 두 개의 체인에 모두 투표한 증거가 있는 경우, 시스템에 예치되었던 보증금은 몰수(Slashing)된다.

이득표(Payoff matrix)는 [표14]와 같다.

		검증인 2			
		Vote on neither	Vote on A (p=0.9)	Vote on B (p=0.1)	Vote on both
검증인 1	Vote on neither	0, 0	0, 0.9	0, 0.1	0, -32 ETH
	Vote on A (p=0.9)	0.9, 0	0.9, 0.9	0.9, 0.1	0.9, -32 ETH
	Vote on B (p=0.1)	0.1, 0	0.1, 0.9	0.1, 0.1	0.1, -32 ETH
	Vote on both	-32 ETH, 0	-32 ETH, 0.9	-32 ETH, 0.1	-32 ETH, -32 ETH

[표14] 몰수 조건이 추가된 2인 투표 게임

이 경우의 검증인 1의 우월전략은 검증인 2가 어떤 전략을 택하든지 A에 투표(Vote on A)이고, 이는 검증인 2의 입장에서도 마찬가지이다. 이전의 이득표와의 차이점은 양쪽 투표의 ER 값을 -32 ETH로 변환시켜 시스템의 내쉬 균형을 이동시켰다는 점이다. 즉, Casper FFG는 보증금과 몰수 조건을 적용하여 양쪽 투표의 유인을 없앤다.

여기서 우리가 앞서 살펴본 비잔틴 합의 가정의 단점을 극복하기 위한 중요한 장치가 등장한다. 바로 PoS 참여를 위한 보증금 예치(Security deposit)이다. 분산 네트워크에서 참여자의 자격을 보증금 예치자로 제한하여, 지분을 예치한 참여자만 네트워크에 참여하고 그에 따른 이득을 얻는다. 이것이 우리가 알고 있는 PoS의 일반적인 설명이다. Casper FFG는 여기에 명백한 몰수(Slashing) 조건 위반 시 보증금의 삭감이라는 페널티 메커니즘을 포함시킨다. 페널티 메커니즘을 통해 Casper FFG는 참여자가 자발적으로 몰수(Slashing) 조건을 위반하지 않도록 한다.

[도표4]는 Casper FFG에서 정의한 몰수(Slashing) 조건이다. 위의 두 가지 조건은 네트워크 분할(Fork)을 일으키는 투표를 방지하는 최소한의 조건이다.

AN INDIVIDUAL VALIDATOR ν MUST NOT PUBLISH TWO DISTINCT VOTES,

$$\langle \nu, s_1, t_1, \mathrm{h}(s_1), \mathrm{h}(t_1) \rangle \quad \text{AND} \quad \langle \nu, s_2, t_2, \mathrm{h}(s_2), \mathrm{h}(t_2) \rangle \ ,$$

SUCH THAT EITHER:

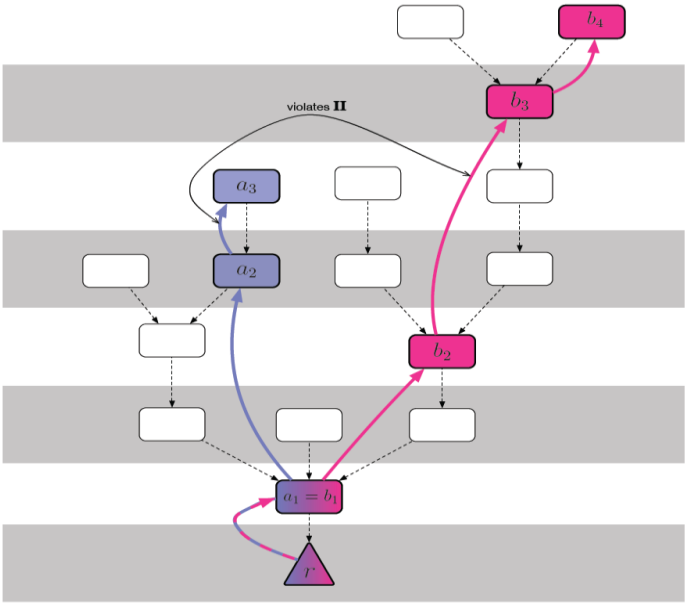
I. $\mathrm{h}(t_1) = \mathrm{h}(t_2)$.
Equivalently, a validator must not publish two distinct votes for the same target height.

OR

II. $\mathrm{h}(s_1) < \mathrm{h}(s_2) < \mathrm{h}(t_2) < \mathrm{h}(t_1)$.
Equivalently, a validator must not vote within the span of its other votes.

[도표4] 몰수 조건

그러면 Casper FFG의 몰수 조건이 실제로 네트워크 분할을 방지하는지 수학적 증명으로 살펴보자



[도표5] 몰수 조건의 수학적 증명[10]

체인 a, 체인 b에 포함된 체크포인트를 각각 $a_n(\mathrm{n}=1,2,3\ldots), b_m(\mathrm{m}=1,2,3\ldots)$이라고 하자. a_2는 최종 확정(Finalized), a_3는 1차 검증(Justified) 된 상황에서 이미 a_1, a_2, a_3 의 체크포인트에 투표한 악의적인 검증인이 체인 b에 되돌리기 공격(Reversion attack)을 시도하고자 한다. 만약 두 개의 동일한 높이의 충돌하는 체크포인트 a_n와 b_m에 모두 투표한다면,

- [도표5]의 조건 I에 의해 몰수(Slashing), 즉, 같은 높이에 있는 체크포인트에 투표 불가

즉 a_2, a_3와 같은 높이에 있는 블록은 최종 확정(Finalized)될 수 없다.

이번에는 높이가 다른 블록에 되돌리기 공격(Reversion attack)을 시도하는 경우에 대해 알아보자. 공격을 성공시키려면 $\mathrm{h}(a_n) < \mathrm{h}(b_m)$ 을 만족하는 b_m 이 최종 확정(Finalized)되어야 한다.

b_m이 최종 확정(Finalized)되었다고 가정한다면 $\mathrm{r} \to \cdots \to b_m$으로 이어지는 Super majority link가 존재할 것이다. 그러나 조건 I에 의하여 $\mathrm{h}(b_{m-1}) = \mathrm{h}(a_{n+1})$ 그리고 $\mathrm{h}(b_{m-1}) = \mathrm{h}(a_n)$ 일 수 없으므로, $\mathrm{h}(b_{m-1}) < \mathrm{h}(a_n)$ 조건이 추가된다. 이에 따라 $\mathrm{h}(b_{m-1}) < \mathrm{h}(a_n) < \mathrm{h}(a_{n+1}) < \mathrm{h}(b_m)$가 형성되며 이는 [도표5]의 조건 II를 위배하므로 처음 제시한 두 개의 충돌하는 체크포인트 a_n와 b_m이 모두 최종 확정(Finalized)될 수 없다.

- [도표5]의 조건 II에 의해 몰수(Slashing), 즉, 포함하는 관계의 체크포인트에 투표 불가

Rule 1. 네트워크 분기를 발생시키는 투표(Voting) 시 반드시 보증금(Deposit)이 삭감된다. 몰수 조건

ii. Plausible Liveness

비잔틴 합의에서 Liveness를 달성하기 위한 가장 중요한 조건은, 비잔틴 정족수의 충족이다. 즉, 하나의 결괏값에 대해 적어도 전체 보증금의 2/3 이상의 규모에 해당하는 검증인이 반드시 합의해야 한다. 따라서 대부분의 비잔틴 합의를 적용하는 블록체인 플랫폼의 경우, '투표행위'에 대해 보상을 적용하여 참여자가 자발적으로 투표를 하도록 한다. 하지만 투표 참여에 대한 이득만 존재하는 시스템의 경우, 각 참여자가 예상하는 이득에 대한 기대치는 각 참여자의 기준점에 따라 달라질 수 있다. 이 경우 이득에 대한 기대치에 따라서 참여자의 투표 참여 여부가 달라지는 상황이 발생한다. 이를 해결하기 위해 Casper FFG는 각 체크포인트에서, 투표에 참여하는 경우 보증금의 크기가 증가하고, 참여하지 않는 경우 보증금의 크기가 감소하는 설계로 모든 참여자의 투표 참여 유인을 강화하였다. 또, 이를 통해 모두가 투표하는 상태가 내쉬 균형이 되도록 하여, 투표 참여 행위에서의 이탈 유인을 없앴다.

게임이론적 해석(Game theoretic interpretation)

Nothing- at-stake에서의 2인 투표 게임(Voting game)에 세 가지의 가정을 추

가하여 새로운 게임을 진행하도록 한다.

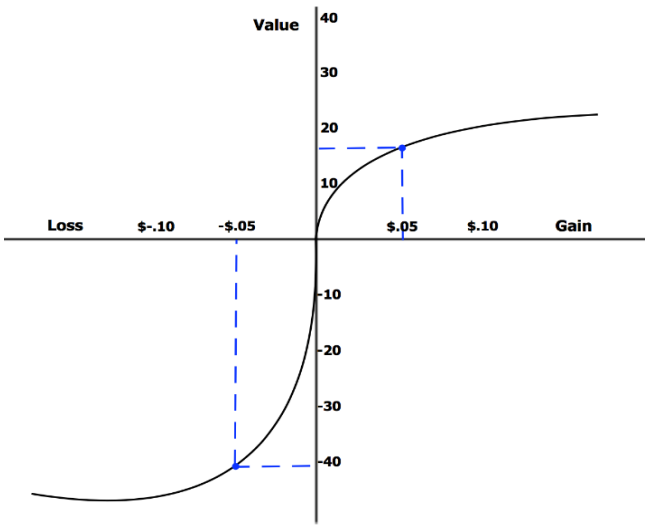
1. 게임의 참여자에게는 투표(Vote) 또는 미투표(Don't vote)의 두 가지 전략이 존재한다.
2. 체크포인트에서 투표자(Voter)의 보증금 규모는 커지고, 미투표자 (Non-voter)의 보증금 규모는 작아진다.
3. 이득(Payoff)은 보증금의 변화량이다. (1은 1만큼 증가, -1은 1만큼 감소)

		검증인 2	
		Vote	Don't vote
검증인 1	Vote	1, 1	1, -1
	Don't vote	-1, 1	-1, -1

[표15] 새로운 2인 투표 게임

[표15]은 이를 간단한 이득표(Payoff matrix)로 나타낸 것이다. 각 경우의 검증인의 우월전략은 모두 'Vote'가 되어, 내쉬 균형은 (Vote, Vote)에서 성립한다.

행동 경제학적 해석(Behavioral Economic interpretation)



[도표6] 손실 회피[11]

[도표6]은 인간의 손실 회피 성향을 나타낸다. 도표에 따르면 0.05달러의 이득에 대한 기댓값은 18이며, 같은 크기의 손실에 대한 기댓값은 -40으로 같은 크기의 이득에 비해 손실은 약 2배 이상으로 평가된다. Casper FFG의 중요한 특징 중 하나는 인센티브 구조 설계에 참여자의 손실 회피 성향이 반영되었다는 점이다. Casper FFG의 보상, 처벌 메커니즘은 '손실 회피 성향'에 따라 단순 보상 메커니즘에 비해 더 많은 투표 참여를 이끌어 낼 수 있을 것이다.

보상만 존재하는 시스템의 경우 보상에 의해 증가하는 투표율을 a%라 하면, 같은 크기의 손실까지 적용하는 경우 손실 회피 심리에 의해 증가하는 투표율은 $(2a + \alpha)\%$가 된다.

Rule 2. 올바르게 투표한 검증인은 체크포인트 이후 보증금의 규모가 늘어나고, 투표를 하지 않은 검증인은 체크포인트 이후 보증금(Deposit)의 규모가 줄어든다.

Rule 3. Safety와 Liveness가 달성된 상태는 내쉬 균형이다.

4.1.2.2. 다수가 절대적으로 옳다는 가정을 하지 않도록 설계

우리는 대부분의 의사결정 과정에서 다수의 의견을 따르는 것을 선호한다. 그 방법이 의사결정 과정에서 필요한 이견 조율의 시간 비용과 노력 비용의 절감을 가져오기 때문이다. 하지만 우리는 다수의 의견이 항상 옳지만은 않다는 것을 알고 있고, 이는 분산 네트워크 환경에서의 컨센서스(Consensus)에서도 동일하게 적용된다. 앞에서 살펴본 비잔틴 합의의 첫 번째 문제점은 비잔틴 정족수가 달성되지 않으면 네트워크가 유지될 수 없다는 것이었다. 이제 두 번째 문제점이 제기된다. 비잔틴 합의는 다수의 선택이 절대적으로 옳다고 가정한다는 것이다.

비잔틴 합의에 따르면, 비잔틴 정족수의 결정은 어느 경우라도 옳다. 물론, 이 가정은 대부분의 경우에는 유효하다. 하지만 다수가 되는 것이 경제적 이득을 더 많이 보장한다면, 이를 악용하는 경우에 대한 대책 역시 필요하다.

만약 다수에게 경제적 이득이 더 많이 돌아간다면, 이로 인해 연합이 발생할 것이다. 이 경우, 다수에 포함되지 못한 참여자들은 경제적 피해를 보게 된다. 따라서 다수에 포함되지 못한 참여자는 이탈할 것이며, 이는 곧 네트워크 전체의 경제적 안전성(Economic security)의 약화를 가져온다.

이더리움은 Casper FFG를 설계하는 과정에서 이를 고려하였다. 분산 네트워크에서 다수가 되는 것이 경제적인 이득을 가져오는 경우를 크게 세 가지로 나누어 각각의 공격이 네트워크에 미치는 효과와 이에 대한 대응을 Casper FFG에 반영하였다.

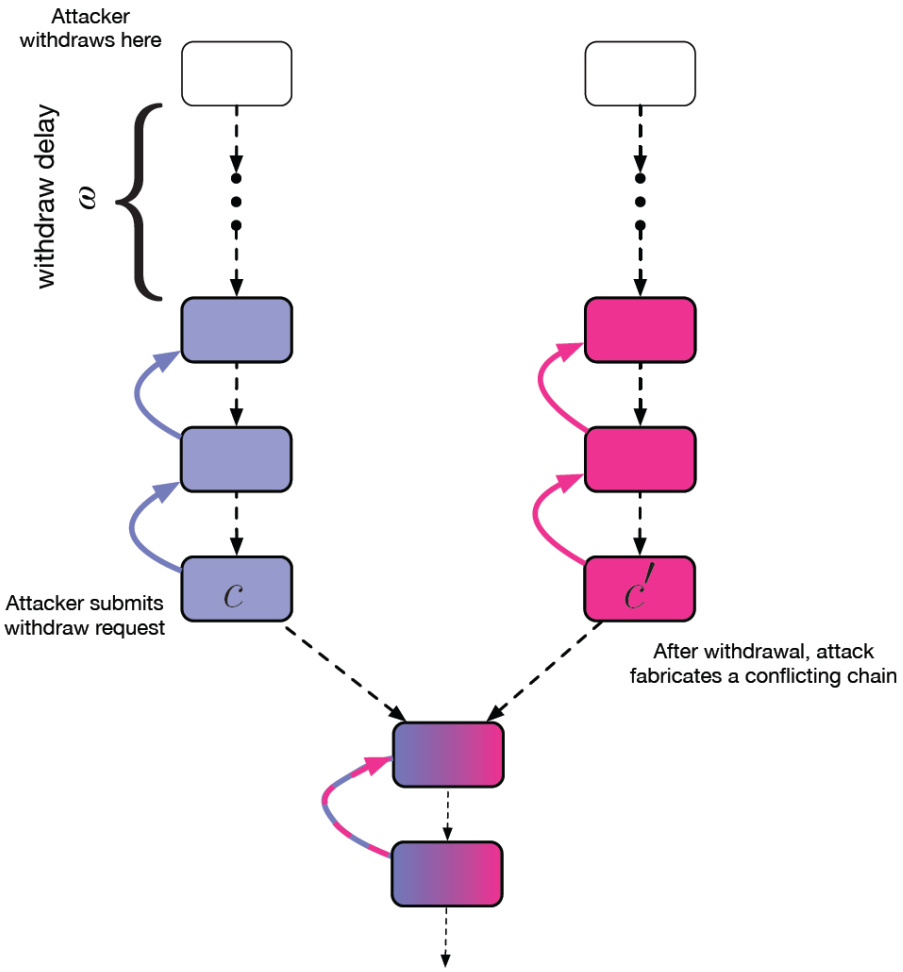
첫째, 네트워크 참여자의 51% 이상이 카르텔을 형성하여 체인의 히스토리(history)를 변경하는 Long-range attack (Traditional 51% attack)이다. 이 경우, 실제 지분 규모의 51%가 담합을 하지 않더라도 공격자(Attacker)의 매수 공격(Bribing attack)만으로도 51% 공격이 가능하다. 공격이 성공하면 체인에 포함된 트랜잭션 히스토리(Transaction history)의 불변성이 지켜지지 않아 네트워크의 무결성이 깨지게 된다.

둘째, 2/3 이상이 카르텔을 형성하여 비잔틴 정족수(Byzantine quorum)을 이루는 다수 검열 공격(Majority censorship)이다. 이 경우, 카르텔에 해당하는 다수가 카르텔에 해당하지 않는 소수의 투표 메시지(Voting message)를 검열하거나 다수의 노드(Node)에서 소수의 투표 메시지를 전달하지 않도록 하여 카르텔 내에서만 경제적 이득을 독점한다. 이 경우, 소수에 해당하는 참여자가 이탈하여 네트워크 보호 효과를 약화시킨다.

셋째, 공격자가 네트워크 내에서 다른 검증인의 이득을 감소시켜서 네트워크에서 이탈하도록 하는 의욕 저하 공격(Discouragement attack)이다. 검증인은 심지어 어느 정도의 공격 비용을 고려하더라도 공격을 감행할 수 있으며, 이 경우 공격자의 이득은 일차적으로 직접적인 경제적 이득을 증가시키는 것을, 이차적으로는 51% 공격과 다수 검열 공격(Majority censorship)이 가능하도록 하는 것을 목표로 한다.

i. Long-range Attack (Traditional 51% Attacks): Economic Finality

장거리 되돌리기(Long-range reversion) 또는 히스토리 되돌리기 공격(History-reversion attack) 이라고도 불리우며, 공격자가 Genesis Block에서부터 유효하지 않은 새로운 체인을 만들어 메인 체인(정격 체인, Canonical chain)을 바꿀 수 있다.



[도표7] 장거리 되돌리기 공격 (Long-range attack)

새로운 체인이 기존의 메인 체인보다 더 길어지면 이중 지불(Double spending) 공격이 성립한다. 컴퓨팅 자원을 사용해 블록을 생성하는 작업 증명은 가장 긴 체인(Longest chain)을 선택하는 방식이 유효하다. 그러나 지분 증명 방식의 경우 새로운

체인을 만들기 쉬울뿐더러 빠르게 블록을 생성할 수 있기 때문에 가장 긴 체인 법칙(Longest chain rule)이 유효하지 않다.

이론상 공격자가 네트워크를 통제하기 위해서는 다수의 지분(Stake)이 필요하지만, 실제로는 과거의 큰 지분을 보유한 계정(Account)만 있더라도 장거리 공격(Long-range attack)을 시도할 수 있다. 즉, 블록 높이 h까지 쌓은 계정은 지분이 인출되면 h+1번째부터는 블록을 쌓을 수 없지만 새로운 체인에서 h번째 이전의 블록까지는 만들 수 있다. 예를 들어, 5천 번째 블록까지 30%의 지분을 가진 계정이, 현재는 보증금을 모두 출금했다고 가정해보자. 해당 계정을 통해 5,001번째 블록부터는 더 이상 블록을 만들 수 없지만, 공격자가 해당 계정의 프라이빗 키(Private key)를 구매 또는 해킹을 통해 얻는다면, Genesis Block부터 새로운 체인을 만들어 5,000번째 블록까지 쌓을 수 있다. 해당 계정의 검증인은 이미 보증금(Deposit)을 모두 출금했으므로 보증금은 몰수(Slashing)되지 않는다. 결론적으로 공격자는 Genesis Block에 예치된 지분의 51%를 직접 소유하지 않고도 51%에 해당하는 소유자의 프라이빗 키를 직접 해킹하거나 프라이빗 키의 소유자에게 약간의 뇌물을 주는 것만으로도 공격할 수 있다. 실제로 보증금을 모두 출금한 해당 프라이빗 키 소유자는 키 관리의 필요성이 사라지므로 뇌물을 받고 프라이빗 키를 공격자에게 넘길 유인이 존재한다. 따라서, 장거리 공격(Long-range attack)을 매수 공격(Bribing attack)이라 칭하기도 한다.

Weak Subjectivity

앞서 보았듯이, 작업 증명 방식과는 달리 지분 증명 방식에서는 블록을 생성하는데 비용이 거의 들지 않기 때문에 가장 긴 체인 법칙(Longest chain rule)은 유효하지 않다. 따라서, 공격자는 언제든지 가짜 체인을 만들어 네트워크에 전파할 수 있다. 이때 발생하는 문제가 Weak Subjectivity이다. Weak Subjectivity는 새로운 노드가 정격 체인(Canonical chain)에 합류하거나, 아주 오랫동안 오프라인이었던 노드가 다시 체인으로 돌아올 때 발생할 수 있는 문제이다. 노드가 네트워크에 합류 또는 재합류하기 위해서는 반드시 현재의 블록 히스토리 정보(최신 블록 해시)를 정확히 알아야

한다. 이를 위해서는 정격 체인(Canonical chain)에서 블록을 쌓고 있었던 기존의 노드로부터 유효한 블록체인 상태 정보(Genesis Block에서부터 현재까지)를 제공받아야 한다. 따라서, 신뢰(Trust)가 절대적인 부분이며 기존의 체인을 유지하고 있던 온라인 노드들은 Weak Subjectivity에 영향을 받지 않는다.

게임이론적 해석(Game theoretic interpretation)

2인의 검증인과 1인의 공격자가 있는 게임으로, 공격자의 공격 성공을 위해 2인의 검증인의 프라이빗 키(Private key)가 필요한 상황을 가정한다.

1. 검증인 A와 검증인 B가 모두 협조하지 않으면 공격은 성공하지 못한다.
2. 이 경우의 이득(Payoff)은 0이다.
3. 공격을 시도하지 않고 혼자 메인 체인(Main chain)을 유지하는 경우의 이득(Payoff)은 5이다

		검증인 B	
		Don't attack	Attack
검증인 A	Don't attack	1, 1	5, 0
	Attack	0, 5	3, 3

[표16] 장거리 되돌리기 공격 게임

[표16]은 매수 공격(Bribing attack)이 발생하기 전의 이득표(Payoff matrix)이다. 검증인 A와 검증인 B 모두가 프라이빗 키(Private key)를 공격자에게 제공해야 공격이 성립하지만, 서로의 전략을 알 수 없으므로, 내쉬 균형은 (Don't attack, Don't attack)에서 성립한다.

		검증인 B	
		Don't attack	Attack
검증인 A	Don't attack	1, 1	5, 3
	Attack	3, 5	6, 6

[표17] 매수 공격이 추가된 장거리 되돌리기 공격 게임

[표17]은 매수 공격(Bribing attack)이 발생한 후의 이득표(Payoff matrix)이다. 공격자는 3의 뇌물을 검증인 A와 검증인 B에게 제공하거나, 혹은 제공한다는 사실을 알린다. 이 경우, 검증인 A와 검증인 B 모두가 프라이빗 키(Private key)를 공격자에게 제공하는 'Attack'을 선택하도록 할 수 있다. 이때, 내쉬 균형은 (Attack, Attack)으로 이동한다.

이를 해결하기 위해 Casper FFG에 경제적 완결성(Economic finality) 및 출금 기간(Withdrawal period)이 도입되었다. 이를 통해 한 번 확정된 에폭(Epoch)에 포함된 트랜잭션 히스토리(Transaction history)는 되돌릴 수 없다. 검증인은 보증금을 예치하고 일정 기간이 지난 후에 투표(Voting)할 수 있으며, 출금 신청하고 일정 기간이 지난 후에 보증금을 찾을 수 있다는 제약조건을 두어 장거리 공격(Long-range attack)의 해결 방법을 제시하였다.

Rule 4. 한번 확정된 에폭(Epoch)에 포함된 트랜잭션 히스토리(Transaction history)는 어떠한 경우에도 변경될 수 없다. 경제적 완결성(Economic finality)

Rule 5. 검증인(Validator)이 합의(Consensus)에 참여하기 위해서는 보증금을 일정 기간 이상 예치하여야 하며, 보증금의 인출 역시 신청하고 일정 기간이 지난 후에만 가능하다.

ii. Majority Censorship

67% 이상의 다수가 카르텔을 형성한 뒤, 소수 참여자의 투표를 무효화시켜 경제적인 이득을 카르텔 내에서만 공유하는 형태의 공격을 다수 검열(Majority Censorship)이라 한다. 다수 검열이 일어나는 경우 33% 이하의 소수에 해당하는 참여자는 올바르게 투표하는 경우에도 투표를 하지 않은 것으로 간주되어 경제적 보상을 받을 수 없게 된다. 뿐만 아니라 Casper FFG의 설계 원칙 중 하나인 '투표하면 보상을 받고 투표하지 않으면 페널티를 받는다.'는 원칙에 의해 보증금의 삭감이 일어나 경제적인 피해를 입는다. Vlad는 비잔틴 합의 과정에서 다수 검열 공격(Majority Censorship)은 막을 수 없음을 다음과 같이 역설했다.[12]

"소수에 해당하는 참여자는 시스템에 남아있을 이유가 없어 시스템을 이탈하게 되고, 참여자가 적을수록 돌아오는 이득이 커지기 때문에 남아있는 참여자 중 2/3에 해당하는 다수가 카르텔을 다시 형성하게 되어, 최종적으로 2명의 참여자만이 남을 것이다"

게임이론적 해석(Game theoretic interpretation)

3명의 참여자가 합의를 달성하여 이에 따른 경제적 보상을 받는 3인 연합게임을 가정한다. 게임의 규칙은 다음과 같다.

- 2/3 이상이 투표하면 합의가 이루어진다.
- 합의가 이루어지는 경우 보상은 3이며, 올바르게 투표한 모두에게 분배한다.
- 참여자는 합의를 이루기 위해 연합을 이룰 수 있으며, 다음의 3가지의 전략 중 선택할 수 있다. (3인 연합, 2인 연합, 연합을 이루지 않음)
- 2명의 참여자가 연합을 이루면 연합에 속하지 않는 참여자의 투표는 제출되지 않는다.
- 투표가 제출되지 않는 경우 보상은 0이다

이 경우의 이득 함수(Payoff function)는 [표18]와 같다.

이제 참가자들의 전략에 따른 이득(Payoff) 및 내쉬 균형을 살펴보면, 참가자가 3인 연합을 이루는 경우 총 이득(Payoff)은 3으로 연합을 이룬 3명의 참가자에게 각 1씩 분배된다. 참가자가 2인 연합을 이루는 경우 총 이득(Payoff)은 역시 3으로 연합을 이룬 2명의 참가자에게 각 1.5씩 분배된다.

	Payoff
(1, 2, 3)	3
(1, 2)	3
(1, 3)	3
(2, 3)	3
(1)	0
(2)	0
(3)	0

[표18] 3인 연합 게임의 이득

이제 참가자들의 전략에 따른 이득(Payoff) 및 내쉬 균형을 살펴보면, 참가자가 3인 연합을 이루는 경우 총 이득(Payoff)은 3으로 연합을 이룬 3명의 참가자에게 각 1씩 분배된다. 참가자가 2인 연합을 이루는 경우 총 이득(Payoff)은 역시 3으로 연합을 이룬 2명의 참가자에게 각 1.5씩 분배된다.

이 경우 3인 연합을 위한 귀속조건은 2인 연합을 이루었을 때보다 3인 연합 시의 각 자의 이득(Payoff)이 더 커져야 한다는 것이다. 귀속을 위한 조건을 식으로 나타내면 다음과 같다.

$$
\begin{aligned}
&Y1 + Y2 \geq 3 \cdots (1)\\
&+ Y1 + Y3 \geq 3 \cdots (2)\\
&+ Y2 + Y3 \geq 3 \cdots (3)\\
&---------------------------\\
&2(Y1 + Y2 + Y3) \geq 9\\
&Y1 + Y2 + Y3 \geq 4.5
\end{aligned}
$$

따라서, 3인 연합으로의 귀속을 위한 필요 조건은 $Y1 + Y2 + Y3 \geq 4.5$가 된다. 하지만 실제 3인 연합의 가치는 3이므로 모든 2인 연합이 3인 연합에 남아있도록 보상을 주기에 충분하지 않다. 따라서, 이 경우 2인 연합에서 균형이 이루어진다.

이를 해결하기 위해, 기존의 3인 연합게임에 다음의 가정을 추가하기로 한다.

1명이 투표를 하지 않는 경우, 투표하지 않은 본인의 이득은 0, 투표를 한 2인의 총 이득을

$$\text{Payoff} \times \frac{\textit{올바르게 투표한 참여자의 수}}{\textit{전체 참여자의 수}} \times \frac{1}{2} \, (2\textit{인 연합을 최소화하기 위한 임의의 상수})$$

로 정하면, 이 경우의 이득 함수(Payoff function)는 [표19]과 같이 변화한다.

	Payoff
(1, 2, 3)	3
(1, 2)	1
(1, 3)	1
(2, 3)	1
(1)	0
(2)	0
(3)	0

[표19] 투표율을 도입한 3인 연합 게임의 이득

3인 연합의 귀속을 위한 필요조건, $Y1 + Y2 + Y3 \geq 1.5$가 되고, 실제 3인 연합의 이득(Payoff)은 3으로 모든 2인 연합이 3인 연합에 남아있도록 보상을 지급하기에 충분하므로 이 경우 3인 연합에서 균형이 이루어진다.

$$\begin{aligned} & Y1 + Y2 \geq 1 \cdots (1) \\ + \; & Y1 + Y3 \geq 1 \cdots (2) \\ + \; & Y2 + Y3 \geq 1 \cdots (3) \\ & - \\ & 2(Y1 + Y2 + Y3) \geq 3 \\ & Y1 + Y2 + Y3 \geq 1.5 \end{aligned}$$

앞서 살펴본 바에 따르면, 2/3 이상의 합의를 요구하는 비잔틴 합의 과정에서 2/3 이상의 다수가 카르텔을 형성할 경제적 유인은 충분하며, 이를 해결하기 위해서는 3인 연합으로 균형이 이동하도록 하는 귀속 필요조건의 설정이 필요하다. Casper FFG 에서는 이득에 투표율을 반영하여 이를 해결하고자 하였다.

Rule 6. 투표하지 않는 참여자의 비율이 커질수록, 보상이 작아지도록 설계하여 카르텔의 생성 유인을 차단한다. Collective Reward Factor

만약 그럼에도 불구하고 카르텔이 형성되는 경우 네트워크는 어떤 대응을 하여야 할까. 다음으로, 카르텔의 구조적 불안정성과 카르텔의 붕괴를 유도하기 위한 조건 설정에 대해 알아보기로 한다. 3인 연합 게임을 다시 살펴보기로 하자.

		검증인 B	
		카르텔 협정 준수	**협정 준수하지 않음**
검증인 A	**카르텔 협정 준수**	8, 8	4, <u>10</u>
	협정 준수하지 않음	<u>10</u>, 4	<u>5</u>, <u>5</u>

[표20] 카르텔 게임

검증인 A, 검증인 B는 카르텔 협정을 맺어 검증인 C를 검열하고 있다.

- 검증인 A, B 모두 카르텔 협정을 준수하는 경우의 이득은 8이다.
- 검증인 A, B 모두 카르텔 협정을 준수하지 않는 경우의 이득은 5이다.
- 한 검증인은 카르텔 협정을 준수하고 다른 검증인은 개별 행동을 하면 협정을 준수한 검증인은 4, 개별행동을 한 검증인은 10의 이득을 얻는다.

여기서 각 검증인의 우월전략은 각 기업이 협정을 준수하지 않고 개별 행동(위반)을 하는 것이며, 이 경우의 우월전략 균형은 카르텔의 붕괴이다. 따라서 우리는 카르텔은 그 특성 때문에 구조적 불안정성을 가지고 있음을 알 수 있으며, 만약 여기서, 카르텔의 붕괴를 위한 촉발 요인을 적용할 수 있다면, 카르텔의 공고화를 더 쉽게 막을 수 있으리라는 점도 알 수 있다.

Casper FFG에서는 검열이 일어나는 경우, 소수의 포크(Fork) 공격을 허용하며 다수의 검열에 대해 Blacklisting(다수 검열을 시스템에 신고하는 제도)을 적용할 수 있게 함으로, 카르텔의 공고화를 막는다. 즉, 다수 검열이 일어나는 경우 소수는 이를 시스템에 신고(Blacklisting)하고, 소수만의 체인을 유지시킨다. 이 경우에 다수의 카르텔에 해당하는 경제적 인간은 다음과 같이 합리적으로 판단한다.

- 이 체인은 신고(black-listed)되었으므로, 이를 인지한 누군가는 카르텔을 떠날 가능성이 있다.
- 현재 2/3가 카르텔 협정을 준수하고 있지만, 카르텔을 떠나는 참여자가 생기며 이 인원이 1/3 이하가 되는 순간 정격 체인(Canonical chain)은 바뀔 것이므로, 현재의 체인에 계속 투표를 하는 것은 보상의 기댓값을 감소시키는 행위이다.

따라서, 이 경우의 경제적 인간의 합리적인 선택은 카르텔을 떠나는 것이며, 이 경우, 소수가 다수의 검열을 신고하는 행위 자체가 카르텔의 붕괴를 촉발하는 요인으로 작용할 수 있다. (다만, 소수에 의해 Blacklisting이 악용되는 경우에 발생할 수 있는 문제에 대한 해결책은 아직 제시되지 않았다.)

Rule 7. 다수의 검열 공격에 대해 카르텔의 붕괴 요인을 적용하여, 카르텔의 공고화를 막는다. 마이너리티 포크와 신고 제도(Minority fork, Blacklisting)

iii. Discouragement Attack

검증인을 네트워크에서 이탈시키는 것을 목표로 하는 공격 행태로, 공격자가 합의 메커니즘(Consensus mechanism)내에서 다른 검증인의 이득을 감소시켜 네트워크 이탈을 유도하는 악의적인 행동이다.

의욕 저하 공격(Discouragement Attack)의 동기는 크게 두 가지로 나눌 수 있다. 첫 번째는 검증인을 이탈시켜서 이탈하지 않은 나머지 검증인에 대한 이득을 증가시키기 위함이다. 물론 나머지 검증인에는 공격자도 포함된다. 첫 번째는 몇몇 검증인을

이탈시켜서 나머지 검증인들에 대한 이득을 증가시킴으로 나머지에 해당하는 공격자의 이득 역시 최대화하기 위함이고, 두 번째는 정직한 검증인(Honest validator)을 이탈시켜 다수에 의한 카르텔 공격 (Traditional 51% and Majority Censorship)의 가능성을 높이기 위함이다. 따라서 전체 보상과 처벌제도(Reward/Penalty system)가 내쉬 균형을 고려하여 설계되었더라도, 이차적인 이득을 얻기 원하는 참여자들에게는 내쉬 균형을 깰 만한 충분한 유인이 있다.

의욕 저하 공격에 대해 Casper FFG는 Griefing Factor(이하 GF)를 통해 공격의 유인이 부족하다는 점을 강조한다. GF는 공격을 받아 발생하는 피해자(Victim)의 경제적 손실과 공격자(Attacker)가 공격을 위해 지불해야 하는 경제적 손실의 비로, 공격이 성공하기 위해 공격자(Attacker)가 감당해야 하는 경제적 손실이 어느 정도인지를 정량화한 변수이다. 물론 이는 공격 자체를 막을 수는 없다는 점에서 소극적 대응에 해당한다.

$$\mathrm{GF} = \frac{absolute\ loss\ for\ victim}{absolute\ loss\ for\ the\ attacker\ suffer}$$

GF를 통해 공격자(Attacker)의 공격 비용과 그로 인한 피해자(Victim)의 손실 비용을 계산할 수 있고, 1차 검증(justified)이 결정되는 비잔틴 정족수에서의 공격 비용을 계산함으로써, 내쉬 균형을 깨기 위해 공격자가 지불해야 하는 비용을 계산할 수 있게 된다.

Rule 8. Attacker의 공격 비용, Victim의 피해 비용을 정량화, Attack에 필요한 비용을 Simulation한다. Griefing factor

4.2. Casper FFG: Reward Mechanism

앞서 살펴본 바와 같이 Casper FFG는 Protocol에 적용된 보상 규칙(Reward rule)을 통해 시스템의 경제적 안전성(Economic security)을 보장하고자 하였다. 앞

서 살펴본 보상 규칙(Reward rule)을 다시 정리하면, 다음과 같다.

4.2.1. Reward Rules for Casper FFG

Rule 1. 네트워크 분기를 발생시키는 투표(Voting) 시 반드시 보증금(Deposit)이 삭감된다. 몰수 조건

Rule 2. 올바르게 투표한 검증인은 체크포인트 이후 보증금의 규모가 늘어나고, 투표를 하지 않은 검증인은 체크포인트 이후 보증금(Deposit)의 규모가 줄어든다.

Rule 3. Safety와 Liveness가 달성된 상태는 내쉬 균형이다.

Rule 4. 한번 확정된 에폭(Epoch)에 포함된 트랜잭션 히스토리(Transaction history)는 어떠한 경우에도 변경될 수 없다. 경제적 완결성(Economic finality)

Rule 5. 검증인(Validator)이 합의(Consensus)에 참여하기 위해서는 보증금을 일정 기간 이상 예치하여야 하며, 보증금의 인출 역시 신청하고 일정 기간이 지난 후에만 가능하다.

Rule 6. 투표하지 않는 참여자의 비율이 커질수록, 보상이 작아지도록 설계하여 카르텔의 생성 유인을 차단한다. Collective Reward Factor

Rule 7. 다수의 검열 공격에 대해 카르텔의 붕괴 요인을 적용하여, 카르텔의 공고화를 막는다. 마이너리티 포크와 신고 제도(Minority fork, Blacklisting)

Rule 8. Attacker의 공격 비용, Victim의 피해 비용을 정량화, Attack에 필요한 비용을 Simulation한다. Griefing factor

4.2.2. 보상 설계 (Reward scheme)

이더리움 재단(Ethereum foundation)과 SUTD (Singapore University of Tech and Design)은 2018년 10월 발표된 "Incentive Analysis of Casper the FFG as a POW/POS hybrid using PRESTO" [13]라는 논문을 통해 Casper FFG protocol 이

제공하는 보상 설계(Reward scheme)를 공개, 효과 차원에서 분석한 바 있다. 하기의 내용은 해당 논문에서 제공하는 보상 설계(Reward scheme) 및 효과 평가 결과를 바탕으로 앞서 살펴본 Casper FFG의 설계 원칙에 해당 내용이 얼마나 부합하는가에 대해 분석한 내용이다.

4.2.2.1. Constants and Variables

Casper FFG에서 투표에 참여하는 검증인과 참여하지 않는 검증인의 보증금의 규모는 매 에폭(Epoch) 마다 달라지며, 이에 영향을 미치는 주요 상수와 변수(Constants and variables)는 [표21]와 같다.

Variables	
Scale factor-related	
$D^*_{v,i}$	Deposit of validator v∈N right before block i * l
$D^{'}_{v,i}$	Scaled deposit of validator v right before checkpoint i
$D_{v,i}$	Scaled deposit of validator v right after checkpoint i
S_i	Deposit scale factor right after checkpoint i
Reward factor-related	
ρ_i	Reward factor, determined by constant γ, β, p and variable S_i
C_i	Collective reward factor
m_i	Weighted fraction of voting validators
Constants	
γ	Base interest factor, 7*10-3
β	Base penalty factor, 2*10-7
p	Deposit scale dependent factor, 12

[표21] 주요 상수와 변수

Epoch $i-1$에서 i 동안의 보증금의 규모 변화

검증인 v의 에폭(Epoch) $i-1$ 직전의 보증금 ($D^*_{v,i}$)의 크기는 에폭(Epoch) i 가 지나며, 검증인의 투표 참여 여부에 따라 변하게 된다. 이를 다음과 같은 식으로 표현할 수 있다.

$$1\mathrm{v,i} = \begin{cases} 1\ if\ validator\ v\ successfully\ voted\ during\ epoch\ i \\ 0\ otherwise. \end{cases}$$

$$\frac{\mathrm{D}^*_{v,i}}{\mathrm{D}^*_{v,i-1}} = \left(1 + 1_{v,i-1} \times \rho_{i-1}\right) - - - (A)$$

block i 직전의 보증금 규모의 변화는 $1_{v,i}$에 의해 투표를 하는 경우 $1+\rho_i$, 투표를 하지 않는 경우 1이 된다. 즉, 투표를 하는 경우 Epoch i 직전의 보증금은 Epoch $i-1$ 직전의 보증금의 크기의 $(1+\rho_i)$의 배수만큼 증가하며, 투표를 하지 않는 경우, Epoch i 직전의 보증금은 Epoch $i-1$ 직전의 보증금의 크기와 같다.

여기에 보상인자 (Reward factor)가 실제 보증금의 크기 변화에 영향을 주는 요소임을 감안하여, 에폭(Epoch) 직전과 직후의 보증금의 크기의 변화율을 보상인자 (Reward factor)로 정의한 규모인자 (Scale factor)를 대입하면, Epoch i, Epoch $i-1$ 직전과 직후의 보증금의 크기 변화율인 Si, $Si-1$는 각각 다음과 같은 식에 의해 표현될 수 있다.

$$D_{v,i} = S_i \times \mathrm{D}^*_{v,i,}\quad \mathrm{D}^*_{v,i} = \frac{D_{v,i}}{S_i} - - - (B1)$$

$$D_{v,i-1} = S_{i-1} \times \mathrm{D}^*_{v,i-1,}\ \mathrm{D}^*_{v,i-1} = \frac{D_{v,i-1}}{S_{i-1}} - - - (B2)$$

B1, B2의 식을 A에 각각 대입하여 풀면,

$$\frac{D_{v,i}}{D_{v,i-1}} = \frac{S_i}{S_{i-1}}\left(1 + 1_{v,i-1} \times \rho_{i-1}\right)$$

이 되고, 여기에 Si를 보상인자(Reward factor)와 Collective reward로 정의한 C_i를 대입하면,

$$\mathrm{Si} = \frac{1 + C_{i-1}}{1 + \rho_{i-1}}(S_{i-1}) - - - (C)$$

$$\frac{D_{v,i}}{D_{v,i-1}} = \frac{1 + C_{i-1}}{1 + \rho_{i-1}}\left(1 + 1_{v,i-1} \times \rho_{i-1}\right)$$

의 식을 얻을 수 있다.

따라서 검증인 v가 투표를 하는 경우, 보증금 크기의 변화율은 $D_{i+1}/D_i = 1 + Ci$가 되어 $(1 + Ci)$ 배만큼 증가하고, 투표를 하지 않는 경우의 보증금 크기의 변화율은 $D_{i+1}/D_i = \frac{1+Ci}{1+\rho i}$ 가 되어, 보증금의 규모는 $\frac{1+Ci}{1+\rho i}$ 배로 감소한다.

여기에서 Ci는 다음과 같이 정의된다.

$$\mathrm{Ci} = \begin{cases} \frac{1}{2} m_i \rho_i \;\; if\; ESF_{i+1} = 2, \\ 0 \;\; ohterwise, \end{cases}$$

$$m_i = \frac{\sum_{v \in V} 1_{v,i} \mathrm{D}^*_{v,i}}{\sum_{v \in V} \mathrm{D}^*_{v,i}}$$

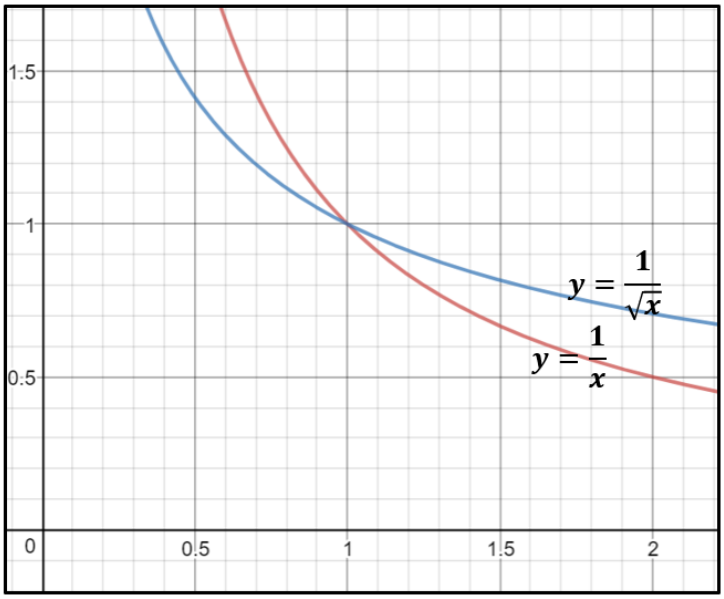
(해석: m_i는 제대로 투표한 검증인(Validator)의 보증금의 총 합을 전체 보증금의 크기로 나눈 값으로, m_i가 클수록 많은 검증인이 투표에 참여, m_i가 작을수록 투표에 참여하지 않은 검증인이 많음을 간접적으로 알 수 있는 변수이다.)

이 경우 Ci는 ρ_i의 $\frac{1}{2}$보다 항상 작거나 같게 되어, 분자 < 분모가 된다. 따라서 투표를 하지 않는 경우 해당 에폭(Epoch)이 지나면 보증금의 크기는 항상 이전 에폭(Epoch)에 비해 줄어든다.

여기에서, 보상 인자(Reward factor, ρ_i)에 대해 정의한 식은 다음과 같다.

$$\rho = \frac{\gamma}{\left(\sum_{v \in V} S_{i-1} D^*_{v,i}\right)} + \beta \times (ESF_i - 2)$$

각각의 변수에 대해 알아보면 먼저 p는 Total dependency factor로 규모의 경제를 방지하기 위해 제시된 임의의 상수(여기에서는 $\frac{1}{2}$)이다. 따라서 $p = \frac{1}{2}$인 경우 분모의 전체 값은 전체 보증금 규모의 Square root가 되어, 전체 보증금 규모가 Reward factor에 미치는 영향을 줄일 수 있게 된다. 이를 그래프를 통해 살펴 보면, [도표8]과 같다.



[도표8] Total dependency factor $(p = \frac{1}{2}, 1)$ 에 따른 Interest factor의 변화

각각은 $y = \frac{1}{x}$, $y = \frac{1}{\sqrt{x}}$를 나타낸 그래프이다. 같은 구간에서 $y = \frac{1}{x}$의 기울기가 더욱 가파르게 감소하는 것을 알 수 있다.

이를 예를 들어 살펴보자. 총 보증금 규모가 10,000 ETH이고 검증인 A가 10 ETH를 예치하고 있는 상황이라면, ρ는 $\gamma/100$에 비례하게 되어 검증인 A의 이자는 $0.01\gamma \times$ 10 ETH, 즉 0.1γ가 된다. 만약 검증인 A가 30,000 ETH를 추가로 예치하면, 총 보증금의 규모는 40,000 ETH 가 되고, ρ는 $\gamma/200$에 비례하게 되어 검증인 A의 이자는 $0.005\gamma \times$30,010 ETH, 즉 150.05 γ가 된다. 결과적으로, 검증인 A가 보증금을 3,001배 늘렸지만 검증인 A의 이자는 1,500.5배 증가되므로 보증금을 늘리는 만큼

혹은 그보다 더 큰 이득을 기대할 수 없다. 따라서 규모의 경제가 성립하지 않는다.

검증인 A는 이번에는 보증금을 늘리는 대신 노드를 더 생성하여 노드 수에 비례해 이득을 늘리려는 시도를 할 수 있다. 그러나 64 ETH를 32 ETH씩 두 개로 나누어 예치함으로써 절대 2배를 초과하는 이득을 늘릴 수 없고, 노드의 추가 생성 비용, 유지 비용 및 보안 비용을 고려한다면, 노드의 추가 생산에 따라 평균 비용이 증가하게 된다. 따라서 이 경우 역시 규모의 경제는 성립하지 않는다.

γ는 기저 보상 인자(Base reward factor) 로, 7×10^{-3}으로 정해진 상수이다. γ가 너무 크면 High operation cost가 필요하고(많은 보상을 주어야 하므로), 너무 작으면 참여자의 참여 유인이 떨어진다는 점을 고려하여 10M ETH 를 예치했을 때, 검증인에게 연 5%의 보상을 지급할 수 있도록 하는 시뮬레이션을 통해 계산되었다.

β는 기저 처벌 인자(Base penalty factor)로, 2×10^{-7}로 정해진 상수이다. β가 너무 크면 검증인들이 온라인 상태를 유지할 유인이 감소되며 너무 낮으면 오프라인 상태로 전환된 검증인이 온라인으로 돌아오는데 시간이 오래 걸리게 된다. Casper FFG는 10M ETH를 예치했을 때, 50%의 검증인이 오프라인 상태로 전환되고 21일이 지나면 보증금의 50%를 잃도록 하는 시뮬레이션을 통해 β를 계산하였다.

ESF(Epoch Since Finalization)는 최종 확정(Finalization)이 일어난 이후의 에폭(Epoch)의 수를 나타내며, 정상적인 상황에서 하나의 에폭(Epoch)은 두 번의 1차 검증(Justified)가 일어나야 최종 확정(finalized)되기 때문에, ESF = 2가 된다. 에폭(Epoch)이 1차 검증(Justified)되지 않는 경우, ESF의 크기는 점점 커지므로 1차 검증 미완료(Non-justified) 상황에서 투표자(Voter)의 보상 인자(Reward factor)는 커지게 되어 투표의 유인을 높인다.

정리하면, Epoch i 직전의 보증금의 크기는 규모인자와 투표인자에 의해 다음과 같이 변화한다.

투표를 하는 경우, 보증금 크기의 변화율은

$$\frac{D_{i+1}}{D_i} = 1 + C_i$$

가 되어, 보증금의 크기가 증가하고

투표를 하지 않는 경우의 보증금 크기의 변화율은

$$\frac{D_{i+1}}{D_i} = \frac{1 + C_i}{1 + \rho_i}$$

가 되어, 보증금의 크기가 감소한다.

이는 우리가 앞서 알아보았던, **Rule 2. 올바르게 투표한 검증인은 체크포인트 이후 보증금의 규모가 늘어나고, 투표를 하지 않은 검증인은 체크포인트 이후 보증금(Deposit)의 규모가 줄어든다.**에 부합하는 조건이다.

투표율에 따른 보증금 크기의 변화

ESF = 2, 즉 계속 1차 검증(justification) 이 일어나는 상황에서, 투표를 한 경우 참여자의 보증금의 크기는 에폭(Epoch) i가 지나면서

$$\frac{D_{i+1}}{D_i} = 1 + C_i = 1 + \frac{1}{2} m_i \rho_i$$

가 된다. 위에서 언급한 수식에 따르면 m_i는 투표율을 나타내는 변수이다. 따라서, 보증금 크기에 투표율이 반영되어 변화함을 알 수 있다.

같은 방법으로 투표를 안 한 경우의 참여자의 보증금의 크기는

$$\frac{D_{i+1}}{D_i} = \frac{1 + C_i}{1 + \rho_i} = \frac{1 + \frac{1}{2} m_i \rho_i}{1 + \rho_i}$$

가 되어, 역시 보증금에 투표율이 반영되어 크기가 변화함을 알 수 있다.

게임이론적 해석(Game theoretic interpretation)

이를 앞서 살펴본 연합게임을 적용하여 다시 한 번 살펴보면 다음과 같다.

3명의 참여자를 가정하여 '3인 연합' - '2인 연합' - '연합을 이루지 않음'에 대한 Collective reward factor (C_i)를 구하면

'2인 연합'의 경우 (이 경우 2명의 참여자의 투표만이 제출되었으므로 $mi = 2/3$)

$$C_i = \frac{1}{2} \times \frac{2}{3} \times \rho_i$$

'3인 연합'의 경우 (이 경우 모든 참여자가 투표하였으므로 $mi = 1$)

$$C_i = \frac{1}{2} \times 1 \times \rho_i$$

가 되어, '3인 연합'의 총 Payoff $(\frac{3}{2}\ i)$가 3인 연합의 귀속 조건인 $\frac{1}{3}\ \rho_i + \frac{1}{3}\ \rho_i + \frac{1}{3}\ \rho_i = \rho_i$ 보다 크게 되므로 '3인 연합'에서 균형이 성립하게 된다.

이는 우리가 앞서 알아보았던, **Rule 6. 투표하지 않는 참여자의 비율이 커질수록, 보상이 작아지도록 설계하여 카르텔의 생성 유인을 차단한다.** Collective Reward Factor 에 부합하는 조건이다.

4.3. 효과 분석

본 논문은 이더리움 Casper FFG의 Reward scheme을 제시하고, 해당 Reward scheme의 구조를 PRESTO framework로 평가한 논문이다. 다음에 이어질 내용을 통해 PRESTO framework에 대해 개략적으로 알아보고, 논문에서 제시하는 평가결과 및 한계점에 대해 고찰, 보완모델을 제안하고자 한다.

4.3.1. PRESTO framework

본 논문을 발표한 Singapore University Technology and Design에서 2018년 6월 발표한 Rethinking Blockchain Security: Position Paper[14]에 처음 등장한 평가 프레임워크(Evaluation framework)이다. 블록체인 플랫폼의 경제적 구조를 분석하기 위한 새로운 Tool을 제시하고자 하는 목표에 의해 설계되었으며, 분석에 필요한 다섯 가지의 속성(Persistence, Robustness, Efficiency, Stability, Optimality)을 제시한다.

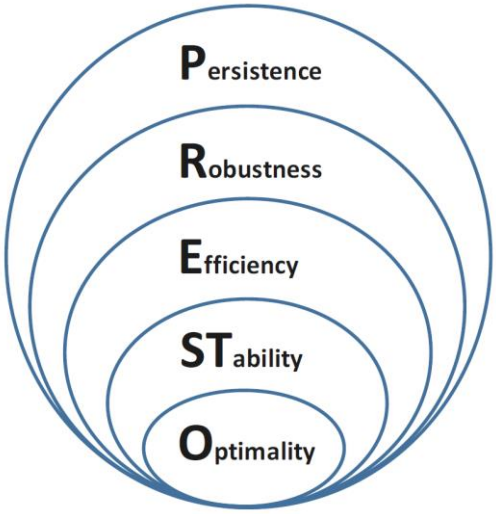
Persistence: 프로토콜이 심각한 공격을 받게 될 경우 얼마나 빨리 복구가 가능한지에 대해 평가한다.

Robustness: 프로토콜이 실제 환경의 취약성을 얼마나 견딜 수 있는지에 대해 평가한다.

Efficiency: 프로토콜이 컴퓨팅 자원을 효율적으로 사용할 수 있도록 설계되었는지 평가한다.

Stability: 프로토콜이 내쉬 균형에 있는지, 즉 모든 의사 결정자의 관점에서 최적의 결과가 내쉬 균형인지 평가한다.

Optimality: 프로토콜이 특정 결과의 quality를 최대화할 수 있도록 설계되었는지 평가한다.



[도표9] PRESTO framework

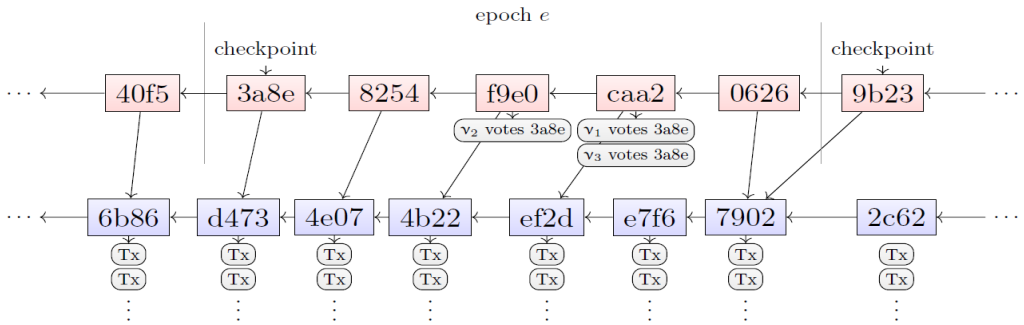
해석 시 주의점

각 속성의 평가방법이 명확히 제시되지 않아 평가자의 평가 방법 설계에 따라 평가 결과의 차이가 크게 발생할 수 있으며 도구의 신뢰도와 타당도에 대한 이전의 연구 결과가 제시되어 있지 않아 해당 결과를 바탕으로 효과를 일반화할 수 없다.

4.3.2. Efficiency

프로토콜에 전송되는 투표 트랜잭션은 다른 정규 트랜잭션과 네트워크 대역 및 연산력을 공유하므로 프로토콜의 효율성에 영향을 끼치게 된다. 한 에폭(Epoch)에서 예상되는 투표 트랜잭션은 참여중인 검증인의 수에 비례하며, 이는 검증인이 예치해야 하는 보증금의 최소량에 의해 결정된다. Casper FFG에서 최초에 제안한 최소 보증금은 1,500 ETH이며, 이 때 예상 참여 검증인의 수는 900여 명이다. 블록 당 평균 125건의 트랜잭션, 에폭(Epoch)당 50 블록이 포함되므로, 에폭(Epoch)당 전송되는 예상 트랜잭션의 수는 6,250건, 한 에폭(Epoch)에 모든 검증인(900명)이 투표한다고 가정하였을 때, 투표에 의한 트랜잭션은 900건으로 이는 전체 트랜잭션의 약 12%에 해당된다. 이더리움 측은 투표 트랜잭션에 (투표 트랜잭션이 들어올 것으로 예상되는

에폭(Epoch)의 마지막 3/4 동안) 다른 모든 거래만큼 많은 'gas'가 지불되어야 한다면, 900명 중 400 ~ 592의 검증인만이 투표에 참여할 것이라는 예측을 한 바 있으며, 이를 해결하기 위한 방법으로 이중 체인(Dual-chain)을 제시한다.



[도표10] 이중 체인(Dual-chain)

이중 체인(Dual-chain) 투표는 이더리움의 다음 단계인 Serenity 론칭 시에 적용될 비콘(Beacon) 체인을 함께 활용하는 방안으로 현재는 간략한 아이디어만 제시되어있다.

현 단일체인(one-chain) 방식으로 Casper 를 적용하게 될 경우 크게 두 가지의 문제가 발생할 수 있다.

- 투표 트랜잭션에 의한 실질 트랜잭션 처리량 감소
- PoW 채굴자에 의한 투표 트랜잭션 검열(Censorship) 발생 가능성

이더리움은 위의 두 가지 문제를 비콘(Beacon) 체인을 통해 다음과 같이 해결하고자 한다.

비콘(Beacon) 체인에는 메인체인의 체크포인트에 대응되는 블록이 존재하며 꼭 메인체인의 블록과 일대일로 대응될 필요는 없다. 비콘(Beacon) 체인에서 전송받은 투표 트랜잭션은 각 블록에 모이고 해당 블록의 해시 값은 메인체인에 전달된다. 메인 체인에서 채굴자는 전송받은 비콘(Beacon) 체인의 블록정보를 메인 체인 블록에 담는

다. 이에 따라 투표 트랜잭션은 기존 트랜잭션과 분리되어 처리되며, 네트워크 거래 처리에 영향을 미치지 않는다. 또한 수 많은 투표 트랜잭션이 하나의 블록 정보에 담겨 전송되므로 특정 주소의 투표 트랜잭션 검열의 가능성을 낮춘다.

이중 체인(Dual-chain)을 사용하는 경우, 더 많은 양의 투표 트랜잭션을 처리할 수 있게 되며, 그에 따라 재단은 더 많은 참여자를 참여시키기 위해 최소 보증금을 32 ETH로 낮추었다. 이 경우 예상되는 참여 검증인의 수는 최대 4.2m이다.

4.3.3. Stability (내쉬 균형, Nash Equilibrium)

앞서 우리는 보상 공식(Reward formula)에 의해 투표자(Voter)와 미투표자(Non-voter)의 이득을 계산하여, 투표를 하는 경우는 해당 에폭(Epoch) 이후 검증인의 보증금의 양이 늘어나고, 투표를 하지 않는 경우에는 보증금의 양이 줄어드는 것을 확인하였다. 여기서는 이를 바탕으로 실제 투표 기권행위(Non-voting)에 따르는 투표자(Voter)와 미투표자(Non-voter)의 손실의 정도를 비교하여, 검증인들이 투표를 하는 내쉬 균형이 성립하는지에 대해 알아보고자 한다.

이를 구하기 위해 먼저, 공격자(Attacker) ν가 α의 보증금 비율(Deposit fraction)을 가지고 네트워크에 투표 기권 공격(Non-voting attack)을 가하는 경우를 가정하고, 각각의 상황에 대한 보증금 변화율(Deposit change rate)을 앞의 보상 공식(Reward formula)에 대입하여 구한다. 이를 각 검증인의 타입(투표자, 미투표자, 공격자)과 체인의 상황(Always justification, Never justification, 공격자에 의해 Justification 여부가 결정)에 따른 보증금 변화율(Deposit change rate)에 따라 [표22]과 같이 나타낼 수 있다.

Scenario	Validator type	$^{Dv,T}/_{Dv,0}$: Relative deposit change
Always Justification	ν	$\left(\frac{1+\frac{1}{2}(\mu-\alpha)\rho}{1+\rho}\right)^{\tau}\left(1+\frac{1}{2}\mu\rho\right)^{T-\tau}$
	voter	$\left(1+\frac{1}{2}(\mu-\alpha)\rho\right)^{\tau}\left(1+\frac{1}{2}\mu\rho\right)^{T-\tau}$
	Non-voter	$\left(\frac{1+\frac{1}{2}(\mu-\alpha)\rho}{1+\rho}\right)\left(\frac{1+\frac{1}{2}\mu\rho}{1+\rho}\right)^{T-\tau}$
Never Justification	ν	$\left(\frac{1}{1+\rho}\right)^{\tau}$
	voter	1
	Non-voter	$\left(\frac{1}{1+\rho}\right)^{T}$
ν is a swing voter	ν	$\left(\frac{1}{1+\rho}\right)^{T}\left(1+\frac{1}{2}\mu\rho\right)^{T-\tau-1}$
	voter	$\left(\frac{1}{1+\rho}\right)^{T-\tau-1}$
	Non-voter	$\left(\frac{1}{1+\rho}\right)^{\tau+1}\left(1+\frac{1}{2}\mu\rho\right)^{T-\tau-1}$

[표22] 보증금의 변화

다음으로, [표22]을 바탕으로 각각의 상황에 대한 절대 손실(Absolute loss)을 계산할 수 있다.

여기서의 절대 손실(Absolute loss)은 공격자(Attacker)의 공격 행위(투표 기권 행위)에 의해 변화하는 보증금 크기의 손실 정도를 의미한다.

즉, 투표자의 손실은 공격자가 α의 지분율로 투표하지 않는 것에 의해 발생하는 피해

정도이며 미투표자의 손실 역시 마찬가지로 공격자가 α의 지분율로 투표하지 않는 것에 의해 발생하는 피해 정도로 계산된다. 이 때, 공격자 자신의 손실은 공격자가 투표를 하여 얻을 수 있는 이득에서 투표를 하지 않음에 의해 발생하는 손실의 차, 즉 투표에 의한 기회비용이 된다.

즉 각 참여자의 손실은 공격자가 투표를 했을 때의 기댓값 - 공격자가 투표를 안 했을 때의 기댓값으로 계산할 수 있다. 이를 위하여 다음의 상황을 가정해보자.

- 전략의 보유현황에 따라 검증인을 3개의 그룹으로 분류한다.
- 투표자에게는 매 에폭(Epoch) 마다 '투표한다'라는 전략만 존재한다.
- 미투표자에게는 매 에폭(Epoch)마다 '투표하지 않는다'라는 전략만 존재한다.
- 공격자(Attacker)는 '투표한다, 투표하지 않는다'의 두가지 전략을 매 에폭(Epoch) 마다 사용할 수 있다.
- 공격자는 이전 에폭(Epoch) 까지는 투표에 참여하였으나, 이번 에폭(Epoch) 부터는 참여하지 않기로 결정하였다.

	Absolute loss per validator type		
Scenario	Voters	Non-voters	Attacker ν
Always Justification	$\text{D vot}, 0 \times \frac{1}{2}\alpha\rho$	$\text{Dvnot}, 0 \times \frac{1}{2}\alpha\rho\left(\frac{1}{1+\rho}\right)$	$\text{Dvnot}, 0 \times \left(\frac{\rho}{1+\rho}\right)\left(1-\frac{1}{2}\mu\right)$
Never Justification	0	0	$\text{D}\nu, 0 \times \frac{\rho}{1+\rho}$
ν is a swing voter	$\text{D vot}, 0 \times \frac{1}{2}\mu\rho$	$\text{Dvnot}, 0 \times \frac{1}{2}\mu\rho \times \frac{1}{1+\rho}$	$\text{D}\nu, 0 \times \frac{\rho}{1+\rho} \times \left(1+\frac{1}{2}\mu(1+\rho)\right)$

[표23] 검증인 type에 따른 보증금의 절대적 손실

공격자의 손실은 기대이득을 포기한 만큼 + 실제 투표를 안함으로 발생하는 손실이므로, 상황에 관계 없이 항상 투표자와 비투표자의 손실보다 커지게 된다. 따라서 이러한 설계 하에서, 공격자는 투표를 기권하지 않는 내쉬균형이 성립한다.

하지만 논문에서 제시한 해석모델에는 다음과 같은 문제점이 존재한다.

- 투표자, 미투표자, 공격자의 전략을 지나치게 단순화하였다. 즉, 투표자와 미투표자의 전략을 각각 투표와 비투표의 단일전략 보유로 고정, 공격자에게만 선택권을 부여하여 공격자의 손실을 선택에 따른 기회비용으로 가정함으로 어느 경우에도 공격자의 손실이 가장 커지는 상황을 설정하였다. (투표자와 미투표자의 손실에는 선택에 따른 기회비용이 포함되어 있지 않기 때문이다.)
- 이렇게 설정된 상황에서는 공격자는 언제나 선택에 따른 기회비용을 치러야만 공격이 가능하다. (이러한 설정으로 공격자의 공격비용을 크게 산정할 수 있으나, 실제 공격을 위한 공격자의 절대적 손실을 정량화하지 못한다.)

따라서, 이를 내시균형을 적용하기 위해 일반화하기에는 해석의 어려움이 있다.

우리는 이 해석모델을 보완하기 위해 한 체크포인트에서 각각 투표와 비투표의 두 전략을 가진 3인의 검증인 게임을 가정하여 해당 게임에서의 내쉬 균형을 찾고, 그 내쉬 균형이 시스템의 안정화를 달성할 수 있는 상황인지에 대해 추가적으로 알아보고자 한다.

게임이론적 해석(Game theoretic interpretation)

[표24]는 어느 한 체크포인트(Checkpoint)에서의 3인의 검증인의 전략을 이득표로 나타낸 것이다. 3인의 검증인에게는 모두 투표/비투표의 두 가지 전략이 존재하며, 각 전략에 의해 해당 에폭(Epoch) 에서의 이득(Payoff)이 결정된다.

이득은 앞서 구한 보상공식(Reward formula)

$$Di + 1/Di = \ 1 + Ci \ = 1 + \frac{1}{2} mi\rho i(\textit{투표하는 경우})$$

$$Di + 1/Di = \frac{1 + Ci}{1 + \rho i} = \frac{1 + \frac{1}{2} mi\rho i}{1 + \rho i} (\textit{투표하지 않는 경우})$$

와

$$\mathrm{Ci} = \begin{cases} \frac{1}{2} mi\rho i \;\; if\; ESFi + 1 = 2, \\ 0 \;\; ohterwise, \end{cases}$$

에 의해 계산할 수 있다.

[표24] 3인 검증인 게임

		검증인 3			
		Vote		Don't vote	
		검증인 2		검증인 2	
		Vote	Don't vote	Vote	Don't vote
검증인 1	Vote	$\frac{1}{2}\rho i, \frac{1}{2}\rho i, \frac{1}{2}\rho i$	$\frac{1}{3}\rho i, -\frac{2}{3}\left(\frac{\rho i}{1+\rho i}\right), \frac{1}{3}\rho i$	$\frac{1}{3}\rho i, \frac{1}{3}\rho i, -\frac{2}{3}\left(\frac{\rho i}{1+\rho i}\right)$	$0, -\frac{\rho i}{1+\rho i}, -\frac{\rho i}{1+\rho i}$
	Don't vote	$-\frac{2}{3}\left(\frac{\rho i}{1+\rho i}\right), \frac{1}{3}\rho i, \frac{1}{3}\rho i$	$-\frac{\rho i}{1+\rho i}, -\frac{\rho i}{1+\rho i}, 0$	$-\frac{\rho i}{1+\rho i}, 0, -\frac{\rho i}{1+\rho i}$	$-\frac{\rho i}{1+\rho i}, -\frac{\rho i}{1+\rho i}, -\frac{\rho i}{1+\rho i}$

여기에서 $\rho i > 0$ 이므로, 모든 검증인의 우월전략은 투표이며, 따라서 우월전략 균형은 (Vote, Vote, Vote)이다.

이는 우리가 앞서 살펴보았던 **Rule 3. Safety와 Liveness가 달성된 상태는 내쉬 균형이다.**에 부합하는 내용이다.

4.3.4. Robustness (Griefing factor and discouragement attack)

앞서 살펴본 바에 따르면, 어떤 검증인도 비투표행위로부터 경제적 이득을 얻을 수 없다. 하지만 검증인 중 어떤 경우는 경제적 유인이 아닌, 외부 동기(External motive)에 의해 네트워크를 방해하려는 시도를 할 수 있고, 우리는 네트워크가 이런 공격에 대해서도 견딜 수 있는지에 대해 생각해 볼 필요가 있다.

논의를 위해, 네트워크 공격이 일어나는 경우의 공격자의 피해 비용과 피해자의 피해 비용의 비를 산정하여, 이 비를 Griefing factor (GFv, t)로 정의하기로 한다.

$$\mathrm{GFv,t} = \frac{Absolute\ loss\ for\ the\ validator\ v\ after\ t\ epoch}{Absolute\ loss\ for\ the\ attaker\ \nu\ \text{after t epoch}} = \frac{Dv,t-Dv,0}{Dv,t-D\ \nu,0}$$

	Griefing factor (GFs) per Validator-type		
Scenario	Voters	Non-voters	Total
Always justification	$\frac{\frac{1}{2}(1+\rho)(\mu-\alpha)}{1+\frac{1}{2}(\mu\rho+a)}$	$\frac{\frac{1}{2}(1-\mu)}{1+\frac{1}{2}(\mu\rho+\alpha)}$	$\sum GFs$
Never Justification	0	0	0
ν is a swing voter	$\frac{\frac{1}{2}(1+\rho)(\mu-\alpha)}{\alpha\left(1+\frac{1}{2}\mu(1+\rho)\right)}$	$\frac{\frac{1}{2}\mu(1-\mu)}{\alpha\left(1+\frac{1}{2}\mu(1+\rho)\right)}$	$\sum GFs$

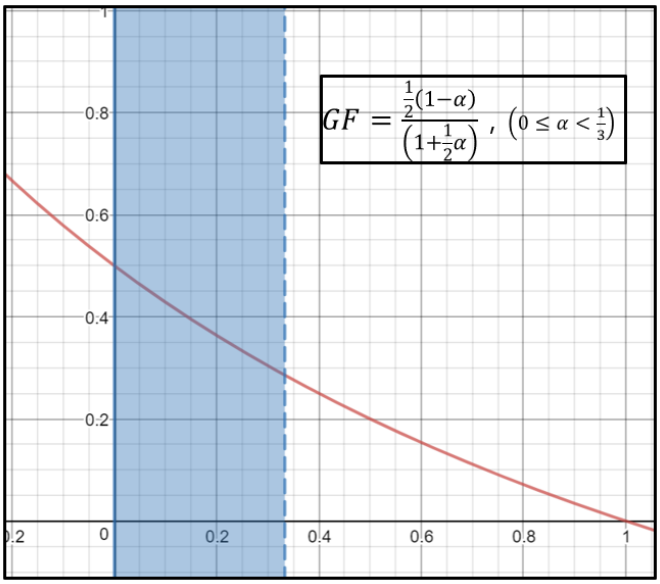
[표25] 검증인 type에 따른 Griefing factor

앞의 Absolute loss를 구하는 식을 통해 도출한 Griefing factor는 [표25]과 같이 나타낼 수 있다.

따라서, 위 표를 바탕으로 항상 1차 검증(Justification)이 일어나는 상황에서의 공격자의 GF의 총 합은 투표자를 공격하기 위한 GF와, 미투표자를 공격하기 위한 GF의 합으로 나타낼 수 있으며, 실제 상황에서 Reward factor (ρ)는 무시할 만큼 작은 수이므로 0으로 둔 논문의 가정을 따르면,

$$\sum GFs\ =\ GF_v + GF_{nv} = \frac{\frac{1}{2}(\mu-\alpha)}{\left(1+\frac{1}{2}\alpha\right)} + \frac{\frac{1}{2}(1-\mu)}{\left(1+\frac{1}{2}\alpha\right)} = \frac{\frac{1}{2}(1-\alpha)}{\left(1+\frac{1}{2}\alpha\right)}$$

가 되고, 이를 GF와 α에 대한 그래프로 나타내면 다음과 같다.



[도표10] 공격자의 지분 비율(α)에 따른 Always justification 시의 GF

즉, GF는 α에 따라 $\frac{2}{7}$에서 $\frac{1}{2}$까지 변하며, 이는 공격자의 공격비용이 피해자의 손실비용의 2배에서 3.5배까지 증가함을 의미한다.

항상 1차 검증(Justification)이 일어나지 않는 상황에서의 GF는 투표자, 미투표자 모두에서 0이므로 이 경우 공격자의 공격비용은 공격자의 기회비용에 따라 무한대로 증가할 수 있다.

하지만, 이 해석 모델 역시 GF 산정에 공격자의 기회비용을 고려하여, 절대 손실을 정확히 반영하지 못했다는 문제점이 있다. 따라서 우리는 공격을 위해 네트워크에 참여한 Attacker V1을 참여자로 설정하여, Attacker V1가 투표하지 않음으로 발생하는 절대적 손실에 의한 Greifing factor 를 다시 구해보기로 한다.

Attacker V1 은 이번 Epoch에 투표기권 공격을 하기 위하여 네트워크에 참여하였으며, 이 경우의 Attacker V1의 투표기권 공격에 대한 절대적 손실은 다음과 같이 산정

하기로 한다.

절대적 손실 (Absolute loss) = Attacker V1의 Epoch i 전의 보증금 크기 – Attacker V1의 Epoch i 후의 보증금 크기

따라서, 이를 반영한 Absolute loss per validator type 은 [표26]과 같다.

		Absolute loss per validator type		
Scenario		Voters	Non-voters	Attacker ν
Always Justification		$\mathrm{D\,vot}, 0 \times \frac{1}{2}\alpha\rho$	$\mathrm{Dvnot}, 0 \times \frac{1}{2}\alpha\rho\left(\frac{1}{1+\rho}\right)$	$\mathrm{D}\nu, 0 \times \left(\frac{\rho}{1+\rho}\right)\left\{1-\frac{1}{2}(\mu-\alpha)\right\}$
Never Justification		0	0	$\mathrm{D}\nu, 0 \times \frac{\rho}{1+\rho}$
ν is a swing voter		$\mathrm{D\,vot}, 0 \times \frac{1}{2}\mu\rho$	$\mathrm{Dvnot}, 0 \times \frac{1}{2}\mu\rho \times \frac{1}{1+\rho}$	$\mathrm{D}\nu, 0 \times \frac{\rho}{1+\rho}$

[표26] 절대적 손실

이를 반영한 GF per validator type 은 [표 27]과 같다.

	Griefing factor (GFs) per Validator-type		
Scenario	Voters	Non-voters	Total
Always justification	$\frac{\frac{1}{2}(1+\rho)(\mu-\alpha)}{1-\frac{1}{2}(\mu-\alpha)}$	$\frac{\frac{1}{2}(1-\mu+\alpha)}{1-\frac{1}{2}(\mu-\alpha)}$	$\sum GFs$
Never Justification	0	0	0
ν is a swing voter	$\frac{\frac{1}{2}(1+\rho)(\mu-\alpha)}{\alpha}$	$\frac{\frac{1}{2}\mu(1-\mu+\alpha)(1+\rho)}{\alpha}$	$\sum GFs$

[표27] 절대적 손실을 반영한 GF

이를 통해 계산한 Total GF 는 다음과 같다.

Always justification 상황의 $\sum GFs$

$$\sum GFs \;=\; GF_v + GF_{nv} = \frac{\frac{1}{2}(\mu-\alpha)}{\left(1+\frac{1}{2}\alpha\right)} + \frac{\frac{1}{2}(1-\mu)}{\left(1+\frac{1}{2}\alpha\right)} = \frac{\frac{1}{2}(1-\alpha)}{\left(1+\frac{1}{2}\alpha\right)} = \frac{1}{2-(\mu-\alpha)}$$

Never justification 상황의 $\sum GFs$

$$\sum GFn = \frac{\frac{1}{2}(\mu-\alpha)}{\alpha} + \frac{\frac{1}{2}\mu(1-\mu+\alpha)}{\alpha} = \frac{\left(\mu-\frac{1}{2}\alpha-\frac{1}{2}\mu^2+\frac{1}{2}\mu\alpha\right)}{\alpha} = \frac{\mu+(1-\mu)(\mu-\alpha)}{2\alpha}$$

이렇게 공격자의 공격비용을 계산하여 공격에 필요한 비용을 예측 할 수 있고 **이는 Rule 8. Attacker의 공격 비용, Victim의 피해 비용을 정량화, Attack에 필요한 비용을 Simulation한다. Griefing factor** 에 부합하는 내용이다.

4.3.4.1 Long term stability and robustness

우리는 앞서 다수 검열시의 보증금 규모의 변화를 통해 다수 검열이 일어나는

것이 모든 검증인에게 손해를 가져오며, 이로 인해 공격자가 반드시 공격에 대한 일정 비용을 지불해야만 해당 공격이 가능하게 한 보상 설계(Reward scheme)에 대해 살펴본 바 있다.

그렇다면 의욕 저하 공격(Discouragement attack)이 긴 기간동안 일어나는 경우의 보증금(Deposit)의 양이 어떻게 변하는지 살펴보고, 이를 통해 해당 공격의 실제 발생 가능성에 대한 논의를 이어 나가고자 한다.

이를 위해 모든 참여자가 투표를 한다고 가정하기로 한다.

우리는 앞서 Interest factor ρ 를 다음과 같이 정의한 바 있다.

$$\rho = \frac{\gamma}{(\sum_{v \in V} Si - 1D * v, i)^p} + \beta \times (ESFi - 2)$$

편의를 위해 $\mathrm{Dn} = \sum_{v \in V} Dv, n$으로 정의하고, $\frac{1}{2}\gamma = \mathrm{y}$ 로 대체하기로 한다.

앞서 구했던 Reward formula에 $\mathrm{Ci} = \frac{1}{2}\rho i$ 를 대입하면 (모두가 투표하므로 $\mathrm{mi} = 1$ 이다.)

$$\frac{Dv, n}{Dv, n-1} \equiv (1 + \mathrm{Cn} - 1) = 1 + \frac{1}{2}\rho$$

이 되고, 위의 ρi에 관한 식을 상기 식에 대입하면 (정의에 의해 $Si - 1D * v, i = \mathrm{Dv, n}$, 모두가 투표하므로 ESF = 2, 따라서 $\frac{1}{2}\rho\mathrm{i} = \frac{y}{D_{n-1}^p}$)

$$1 + \frac{1}{2}\rho = 1 + \frac{y}{D_{n-1}^p}$$

가 된다.

위 식을 다시 정리하면

$$\mathrm{Dn} = \left(1 + \frac{y}{D_{n-1}^p}\right) \times \mathrm{Dn} - 1 = \mathrm{Dn} - 1 + \mathrm{yD}_{n-1}^{1-p}$$

$$\mathrm{Dn} = \prod_{j=1}^{n}\left(1 + \frac{y}{D_{j-1}^{p}}\right) Do$$

로 표현할 수 있다.

이 식에서 p 가 0인 경우 (Interest가 deposit에 비례), $\frac{1}{2}$ 인 경우 (Interest가 deposit의 Square root에 비례), 1 인 경우(Interest 와 deposit의 크기 상관없음) 에 대해 해당 식을 다시 써보면

$$\mathrm{p} = 0 : \mathrm{Dn} = \mathrm{D0}\sum_{j=0}^{n}\binom{n}{j} y^{j} \approx D0e^{ny}$$

$$\mathrm{p} = \frac{1}{2} : Dn \approx \left(1 + \frac{\frac{1}{2}ny}{\sqrt{D0}}\right)^{2} D0$$

$$\mathrm{p} = 1 : \mathrm{Dn} \approx \left(1 + \frac{ny}{D0}\right) D0$$

이를 일반화하면,

$$\mathrm{Dn} \approx \left(1 + \frac{pny}{D_0^{p}}\right)^{\frac{1}{p}} D0$$

가 되고, 이 식에 앞서 구했던 (10) 식을 대입하면,

$$\left(1 + \frac{pny}{D_0^{p}}\right)^{\frac{1}{p}} D0 + y\left(\left(1 + \frac{pny}{D_0^{p}}\right)^{\frac{1}{p}} D0\right)^{1-p}$$

$$= D0\left(\left(1 + \frac{pny}{D_0^{p}}\right)\left(1 + \frac{y}{D_0^{p}\left(1 + \frac{npy}{D_0^{p}}\right)}\right)^{p}\right)^{1-p}$$

$$\approx D0\left(\left(1+\frac{pny}{D_0^p}\right)\left(1+\frac{py}{D_0^p\left(1+\frac{npy}{D_0^p}\right)}\right)\right)^{1/p}$$

$$=\left(1+\frac{p(n+1)y}{D_0^p}\right)^{1/p} Do$$

$$\left(1+\frac{pny}{D_0^p}\right)^{1/p}\mathrm{Do}+\mathrm{y}\left(\left(1+\frac{pny}{D_0^p}\right)^{1/p} D_0\right)^{1-p}$$

$$=D_0\left(\left(1+\frac{pny}{D_0^p}\right)\left(1+\frac{y}{D_0^p\left(1+\frac{npy}{D_0^p}\right)}\right)^{p}\right)^{1/p}$$

$$\approx D_0\left(\left(1+\frac{pny}{D_0^p}\right)\left(1+\frac{py}{D_0^p\left(1+\frac{npy}{D_0^p}\right)}\right)\right)^{1/p}$$

$$=\left(1+\frac{p(n+1)y}{D_0^p}\right)^{1/p} D_0$$

$D_{\alpha,n}$을 attack을 하지 않는 경우의 attacker의 deposit , $Ð_{\alpha,n}$을 attack을 하는 경우의 attacker의 deposit 이라고 가정하면

$$D_{\alpha,\tau'}\approx\left(1+\frac{p\tau' y}{D_0^p}\right)^{1/p} D_{\alpha,0}$$

$$Ð_{\alpha,\tau}\approx\left(1+\frac{(1-h)p\tau' y}{D_0^p}\right)^{1/p} D_{\alpha,0}$$

$$Ð_{\alpha,\tau'} \approx \left(1 + \frac{p(\tau' - \tau)y}{D_0^p}\right)^{1/p} D_{\alpha,\tau}$$

$$Ð_{\tau} \approx \left(1 + \frac{(1-3h)p\tau y}{D_0^p}\right)^{1/p} D_0$$

$$\left(1 + \frac{p\tau' y}{D_0^p}\right)^{1/p} D_{\alpha,0} = \left(1 + \frac{(1-h)p\tau y}{D_0^p}\right)^{1/p} \left(1 + \frac{p(\tau' - \tau)y}{Ð_\tau^p}\right)^{1/p} D_{\alpha,0}$$

$$\frac{p\tau' y}{D_0^p} = \frac{(1-h)p\tau y}{D_0^p} + \frac{p(\tau' - \tau)y}{D_\tau^p} + \frac{(1-h)p\tau y}{D_0^p}\frac{p(\tau' - \tau)y}{D_\tau^p}$$

$$\tau' = (1-\mathrm{h})\tau + \frac{\tau' - \tau}{1 + \frac{(1-3h)p\tau y}{D_0^p}}\left(1 + \frac{(\tau' - \tau) + \tau p(\tau' - \tau)y}{D_0^p}\right)$$

$$\tau' = \frac{D_0^p + 3p\tau y - 3hp\tau y}{2py}$$

위 식을 통해 계산한 τ'는 $\mathrm{p} = \frac{1}{2}$, $\gamma = 0.007$, $\sum_v DD_{v,0} = 10000000$ 일 때, $\tau' = 903500$이 되어 대략 20년이 된다. 즉 Dos attack 등으로 censorship 공격을 시행하는 경우, 공격자가 이득을 얻기 위한 시점은 약 20년이 된다.

4.3.6. Persistence (Minority fork)

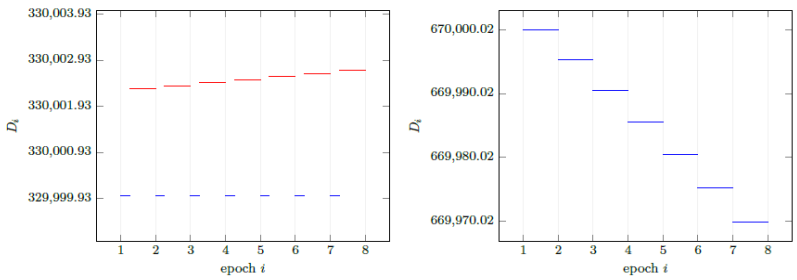
게임이론적 해석(Game theoretic interpretation)

연합(Coalition)에 의한 다수 검열(Majority censorship)이 지속적으로 일어나는 공격을 가정하고, 네트워크가 얼마나 이 공격에 대해 버틸 수 있는지에 대해 지속성(Persistence) 측면에서 알아보고자 한다. Casper FFG는 다수 검열(Majority Censorship)이 계속 일어나게 되는 경우, 마이너리티가 이에 대항할 수 있는 방법으로 마이너리티 포크(Minority fork)를 제시한다. 마이너리티는 카르텔에 의해 1차 검증(Justified)된 에폭(Epoch) 의 에폭 번호 + 해시 값을 체인상에 신고(Blacklisting)

할 권리를 가지고 있다. 마이너리티는 시스템에 검열을 신고(Blacklisting)한 후, 새로운 체인을 만들어간다. 이를 마이너리티 포크(Minority fork)라고 한다. 이 경우, 검증인은 다수 검열(Majority Censorship)로 신고된 체인 (Black-listed chain)과 마이너리티에 의해 새로 생긴 마이너리티 체인(Minority chain)에 투표하는 두 가지의 전략을 각각 갖게 되며, 두 가지의 전략 중 최선반응을 선택하게 된다. (두 체인에 모두 투표하는 행위는 몰수 조건에 해당하므로, 이 경우 보증금이 삭감된다.)

여기에서 앞서 살펴본 카르텔의 구조적 불안정성(Instability)이 큰 역할을 하게 된다. 일단 다수 검열 체인(Black-listed chain)으로 등록된 체인에 계속 투표를 하는 경우, 새로운 체인에는 투표할 수 없다. 물론 연합에 가담한 모든 참여자가 계속 다수 검열 체인(Black-listed chain)에 투표하기로 동맹을 맺는 경우, 마이너리티 포크(Minority fork)는 실패 할 것이다. 하지만 우리는 앞서 카르텔의 형성시의 우월전략과 유지시의 우월전략에 대해 알아본 바 있으며, 카르텔이 유지되는 경우의 우월전략은 카르텔의 붕괴임을 확인하였다. 이에 따르면, 연합에 의한 카르텔은 붕괴될 것이며, 이를 인지하고 있는 검증인의 최선반응은 카르텔을 떠나는 것이다.

다음은 상기 상황에 대해 앞서 살펴본 보상 메커니즘(Reward mechanism)을 바탕으로 시뮬레이션을 한 결과이다.



(a) Voting validator. (b) Non-voting validator.

Fig. 8. Evolution of the scaled deposits of voting and non-voting validators shortly after a minority fork. In the figure on the left, the red line represents the deposits after voting, and the blue line the deposits after the deposit scale factor update. The non-voting validators do not get rewards and their deposits shrink at the start of each epoch. In this graph, $\sum D = 10^6$.

[도표11] 마이너리티 포크 후의 보증금의 변화율 (a)투표자 (b)미투표자

실제 보상 공식 (Reward formula)을 적용하여, 마이너리티 포크(Minority fork) 가 일어난 이후의 검증인의 보증금을 시간에 따라 나타낸 그래프가 [도표11]이다. 에폭(Epoch) 번호가 증가함에 따라 마이너리티 체인(Minority chain)에 투표한 투표자의 보증금 규모가 점진적으로 증가([도표11]의 Red line)하는 것에 비해 미투표자의 보증금 규모는 빠른 속도로 감소하는 것을 알 수 있다. [도표11]은 이를 더 오랜 기간 시뮬레이션 한 결과이며, 시뮬레이션 상 3,706 에폭(Epoch) 후에 (Block producing time 15초 가정 시, 32일 후) 에폭(Epoch)의 확정(Finalization)이 일어났음을 알 수 있다. 우리는 이를 통해 다수의 검열 공격에 대해 네트워크의 지속성을 확보할 수 있음을 알 수 있다. 이는 우리가 앞서 살펴보았던 **Rule 7. 다수의 검열 공격에 대해 카르텔의 붕괴 요인을 적용하여, 카르텔의 공고화를 막는다. 마이너리티 포크와 신고 제도(Minority fork, Blacklisting)**에 해당하는 내용이다.

행동 경제학적 해석(Behavioral Economic interpretation) [15][16][17]

이더리움연구회 4기 토큰 이코노미 분과에서는 게임 이론과 더불어 행동경제학을 연구의 프레임워크로 상정하고 고찰하였다. Casper FFG는 암호 경제학 관점에서 모든 검증인이 경제적 인간(Econ)이라는 가정 하에 설계되었다. 그러나 행동 경제학에서 바라보는 사람(human)은 여러 가지 상황에 따라서 합리적이지 못하거나 때로는 모순된 행동까지 한다. 행동 경제학에서 경제적 인간은 '이론의 토대에 발을 딛고 사는 허구'로, human은 '실제 세계에서 행동하는 사람'으로 정의한다.

Casper FFG의 지속성(Persistence)이 성립되기 위해서는 다수 검열로 신고된 체인(Black-listed chain)에 투표 중인 검증인이 소수에 의해 새로 생긴 체인(Minority fork)에 투표하기 시작하면서 카르텔이 붕괴된다는 논리가 전제되어야 한다. 이는 검증인이 경제적 인간이라는 가정 하에 성립하는 논리이다. 여기에서는 행동경제학 관점에서 보는 비합리적 인간에 의한 마이너리티 포크에 대해 논의해보기로

한다.

다수 검열 공격의 불확실성

다수 검열 공격은 카르텔을 형성한 검증인 집단이 다른 검증인의 메시지를 배제하는 것이다. 메시지를 배제하기 시작할 때, 해당 검증인은 이를 바로 알아차리고 신고(Blacklisting)해야 한다. 하지만 메시지의 배제가 네트워크의 불안정으로 인해 발생한 것인지, 실제 카르텔이 형성된 것인지는 해당 검증인이 정보를 수집하여 판단해야 한다. 하지만 이는 매우 불확실한 정보를 바탕으로 하기 때문에, 검증인은 어림짐작(Heuristics)의 원리에 기대어 판단을 내릴 것이며, 여러 가지 외부 변수에 의해 명확한 판단을 내리기 어려울 것이다. 몇 가지 예를 들어보자.

첫째, 메시지를 배제당한 검증인은 과연 몇 개의 메시지가 배제되었을 때, 다수 검열 공격이 시작되었다고 판단하고 신고할 것인가.

둘째, 신고받기 시작한 체인(Black-listed chain)에 투표하고 있던 검증인은, 과연 몇 번의 신고가 누적되면 소수에 의해 새로 생긴 체인(Minority fork)에 투표하기 시작할 것인가.

이 숫자에 영향을 미칠 것은 기준점 효과(Anchoring effect)이다. 기준점 효과란, 모르는 수량을 추정하기 전에 특정 값이 머릿속에 떠오를 때 나타난다. 머릿속에 떠오른 값을 기준점 삼아 그와 가까운 숫자를 추정치로 내놓는 것이다. 간디가 114세가 넘어 사망했느냐고 질문하면, 35세가 넘어 사망했느냐고 질문할 때보다 사망 나이를 훨씬 높게 예측하여 대답하는 것이 그 예이다.

단 한 번의 메시지 누락으로 신고할 것인가? 그렇다면 마이너리티 포크는 여러 개가 계속해서 만들어질 것인가? 새로운 마이너리티 포크에서 메시지가 누락된다면 또다시 신고가 시작될 것인가? 모든 체인이 서로 신고한 체인이라면 어떻게 올바른 체인을 가려낼 수 있을 것인가? 완벽하지 못하더라도 이러한 의문에 대한 보강이 필요하다.

신고(Black-listing)의 무한 반복

여러 의문점이 존재하지만, 명확한 예를 들기 위해 다시 논의를 좁혀보자. 신고받은 체인(black-listed chain)과 소수에 의해 새로 생긴 체인(Minority fork), 단 두 개의 체인만 존재하며 더이상 새로운 마이너리티 포크가 일어나지 않는 상황이라고 가정해보자. Rule 7.처럼 해결된다면 약 30일 이후에는 모든 검증인이 하나의 체인에 투표할 것이다. 하지만 행동경제학 관점에서는 다른 해석이 가능하다.

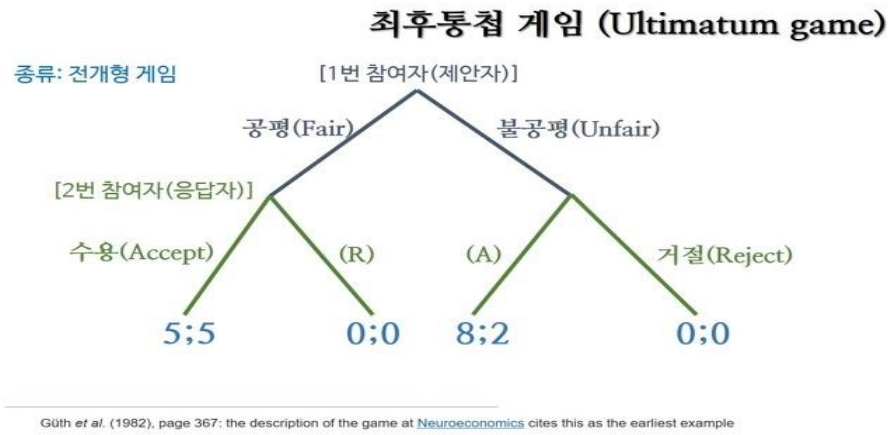
첫째, 하나의 체인으로 합쳐지는 순간, 곧바로 카르텔을 다시 형성하여 다수 검열 공격을 시작하는 경우다. 카르텔이 전체 체인을 장악하기 위해 약 30일 간의 이득을 포기하다가 하나의 체인으로 합쳐질 때 보상을 받은 후, 다시 이득을 포기하고 공격을 감행하는 것이다.

둘째, 다수 검열 공격을 당한 소수의 검증인도 계속해서 마이너리티 포크를 유지하는 경우다. 언젠가는 보상을 받을 수 있을 것이라고 생각한다면, 해당 체인을 신고하고 소수 체인에 남아있을 것이다.

이때 행동 경제학의 두 가지 관점이 적용될 수 있다.

첫째, 손실회피 성향이다. 인간(human)은 손실회피 성향을 기본적으로 갖고 있다. 하지만 일정 기준점 이상의 손실이 발생할 경우, 확률이 낮더라도 이득을 볼 수 있는 전략에 배팅한다. 손실회피 성향을 갖고 있기에 이성적으로 행동해야 할 검증인이, 기준점 이상의 손실을 보게 된다면, '판을 엎어버리는' 전략을 선택해버리는 것이다.

둘째, 최후통첩 게임에서 확인할 수 있는 역겨움의 정서이다.



[도표12] 최후통첩 게임[18]

최후통첩 게임의 예시는 다음과 같다. A에게 10,000원을 B와 나누어 가질 수 있도록 한다. A가 제안한 금액을 B는 갖거나 거부할 수 있다. B가 거부할 경우, A와 B 모두 아무것도 가질 수 없다. A와 B 모두 '합리적(이기적)인 인간'일 경우, A는 9,990원을 제안하고 B는 어떤 금액을 제시받던 거부하지 않는다. 누구와 어떤 금액을 나누는 것이 아니라, 그냥 금액을 제시했다면 가졌을 것이다. 그러나 대부분의 인간은 '합리적'이지 않기 때문에, 전체 금액의 30~50%의 금액을 제시한다. 제시받은 금액에 대해서 불공정한 분배라고 느낄 경우, 판 자체를 깨트릴 것으로 생각하기 때문이다. 이는 생물학적으로 인간의 뇌섬엽(insula, 인슐라)과 관련이 있다. 뇌섬엽은 역겨움과 부정적인 정서를 느낄 때 활성화된다. 제안받은 금액에서 이 정서를 느낄 때, '비합리적'인 의사결정을 하게 된다는 것이다.

최후통첩 게임에서 볼 수 있듯이, Casper FFG에서 설계한 보상 메커니즘 대로 보상을 수령하기 위해 이성적으로 행동해야 할 검증인이 외려 판을 깨뜨리는 형국으로 얼마든지 치달을 수 있다.

4.4. 한계점

본 논문은 Casper FFG의 보상-인센티브 체계를 PRESTO (Persistency, Robustness, Efficiency, Stability, Optimality) Tool을 이용해서 효과를 분석한 논문으로 Casper FFG를 경제 효과성 측면에서 처음으로 분석하여 시사점을 제시하였다는 점에서 그 의의가 있다.

하지만 본 논문에는 다음과 같은 한계점 역시 존재한다.

1. 내쉬 균형 분석 시 투표자, 미투표자, 공격자의 전략을 지나치게 단순화하였다. 즉, 투표자와 미투표자의 전략을 각각 투표와 비투표의 단일전략 보유로 고정, 공격자에게만 선택권을 부여하여 공격자의 손실을 선택에 따른 기회비용으로 가정함으로 어느 경우에도 공격자의 손실이 가장 커지는 상황을 설정하였다. (투표자와 미투표자의 손실에는 선택에 따른 기회비용이 포함되어 있지 않기 때문이다.)

2. 이렇게 설정된 상황에서는 공격자는 언제나 선택에 따른 기회비용을 치러야만 공격이 가능하다. (이러한 설정으로 공격자의 공격비용을 크게 산정할 수 있으나, 실제 공격을 위한 공격자의 절대적 손실을 반영하지는 못한다.)

3. Griefing factor 계산 시 공격자의 손실은 공격자의 선택에 따른 기회비용(상대적 비용, 상대적 손실)으로 산정하였으나, 투표자와 미투표자의 손실은 공격자의 공격에 따른 보증금 크기의 절대적 손실로 산정하였다. 같은 기준을 적용하지 않았으므로, 이를 적용하여 GF 를 계산할 수 없다.

4. 효과 분석을 위해 사용된 PRESTO Tool에 대한 신뢰도(Reliability)와 타당도(Validity)가 확보되어 있지 않아 본 논문의 결론을 그대로 해석 및 적용하기에는 무리가 있다.

따라서, 후속 연구에서는 이러한 한계점을 보완한 효과평가 모델 및 결과가 제시되기를 기대하는 바이다.

5. 맺음말

이상으로 이더리움 연구회 4기 토큰이코노미 분과에서는 암호경제학적 관점에서의 Casper FFG를 고찰하였다. 본 보고서가 많은 이들에게 아직은 생소한 암호경제학이라는 분야를 조금 더 친숙하게 접할 수 있도록 하는데 작은 도움이나마 되기를 바라면서 본 글을 마치고자 한다.

해당 문서는 비영리목적으로 누구나 공정 이용 및 공유하실 수 있으나 이용 시 반드시 출처를 표기해 주시기 바랍니다. 해당 문서를 비영리목적이 아닌 영리목적으로 무분별하게 이용할 경우 저작권법 제 37조에 의거하여 법적인 제재를 받을 수 있습니다.

6. Acknowledgement

홍종화 hjh93411@gmail.com

여기저기 영어로 흩어져있는 이더리움 자료를 모두 보는 것은 어려운 일이었다. 이번 리서치를 통해 이더리움이 어떤 경제적인 모델들을 바탕으로 설계를 하고자 하는지 알게 되었고, 이더리움에 대해 잘 알게 된 시간이었다. 좋은 팀원과의 협업을 통해 통합된 한글화 문서를 내놓게 되어 매우 기쁜 마음이다.

임호태 hottae0805@gmail.com

이더리움의 팬으로써 이런 도전적인 일에 동참할 수 있었다는 것이 너무나도 기쁩니다. 함께 밤새워 노력하신 이연 이코노미 분과 분들께 감사하다는 말씀드립니다. 이더리움 캐스퍼에 조금이나마 도움이 될 수 있는, 좀 더 나아간다면 암호경제학이라는 분야에 도움이 될 수 있는 문서가 되었으면 좋겠습니다.

이기호 kiho.e.lee@gmail.com

세 달만에 압축하여 성장할 수 있는 계기였습니다. 저보다 더 뜨거운 열정을 가진 분들과 함께했기에 가능했습니다. 다음 연구가 기다려집니다.

박시은 sieun0714@gmail.com

힘들었지만 재미있었던 한 달이었습니다. 결과물을 내놓아 평가받는 일은 언제나 떨리는 일이지만 부족한 부분은 부족한대로 다음을 위한 주춧돌이 될 것이라 믿습니다. 캐스퍼에 대해 밤을 새워 토론할 줄 아는 멋진 이연 4 기 토큰이코노미 분과장님 이하 팀원분들께 진심으로 깊은 감사를 전합니다.

강보영 bykang2015@gmail.com

서로 신뢰하지 않는 복수의 참여자간의 분산 네트워크 합의방식은 효율성을 희생하는 대신 효과성의 극대화를 추구한다. 이는 우리 스터디 팀 운영의 딜레마이기도 했다. 큰 배움이 있었다. 토큰 이코노미 도반들한테 감사하다

전창석 (분과장) jcs191072@gmail.com

분과원의 열정, 헌신, 노력이 이 캐스퍼 자료에 녹아있다. 근 한달을 하루 서너 시간도 못 잘 만큼 헌신해준 것을 잘 알고 있기에 분과장으로서 감사와 미안한 마음이 크다. 조금 더 완성도 있는 자료를 만들고자 최선 그 이상의 노력을 해주신 모든 분과원들에게 진심으로 감사의 마음을 전한다.

References

1. Roger A McCain, Game Theory: A Nontechnical Introduction to the Analysis of Strategy, World Scientific, 2014

2. 팃포탯 게임, 웹페이지
https://namu.wiki/w/%ED%8C%83%ED%8F%AC%ED%83%AF

3. 반복적 죄수의 딜레마, WILL KENTON, 웹페이지
https://www.investopedia.com/terms/i/iterated-prisoners-dilemma.asp

4. Chong et al., Iterated Prisoner's Dilemma and Evolutionary Game Theory, Advances in Natural Computation, 2007, 23-62

5. Pareto Optimality, Kevin Leyton-Brown, 웹페이지
https://www.coursera.org/learn/game-theory-1/lecture/5VlAm/1-10-pareto-optimality

6. Fischer at al., Impossibility of Distributed Consensus with One Faulty Process, Journal of the Asscctkion for Computing Machinery, 32(2), 1985, 374-382

7. Buchman, Tendermint: Byzantine Fault Tolerance in the Age of Blockchains, The University of Guelph, 2016

8. Castro et al., Practical Byzantine Fault Tolerance, Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999, 173-186

9. Nothing-at-stake, 웹페이지
https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-the-nothing-at-stake-problem-and-how-can-it-be-fixed

10. Buterin, Casper the Friendly Finality Gadget, Cornell University Library, on 3rd revision, 2018

11. Loss aversion, 웹페이지
https://en.wikipedia.org/wiki/Loss_aversion

12. Zamfir, History of Casper 4, 웹페이지

https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-4-3855638b5f0e

13. Daniel et al., Incentive Analysis of Casper the Friendly Finality Gadget as a POW/POS Hybrid Using PRESTO, draft, 2018
https://github.com/daniel-sutd/casper-paper/blob/103521ba005c6816204d4ce9e3c2134477897f70/casper_economics_basic.pdf

14. Chia et al., Rethinking Blockchain Security: Position Paper, draft, 2018
https://arxiv.org/pdf/1806.04358.pdf

15. Judgment under Uncertainty: Heuristics and Biases, Amos Tversky; Daniel Kahneman
http://psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf

16. Prospect Theory: An Analysis of Decision under Risk, Amos Tversky; Daniel Kahneman
https://www.uzh.ch/cmsssl/suz/dam/jcr:00000000-64a0-5b1c-0000-00003b7ec704/10.05-kahneman-tversky-79.pdf

17. Choices, Values, and Frames, Amos Tversky; Daniel Kahneman
http://web.missouri.edu/~segerti/capstone/choicesvalues.pdf

18. 최후통첩 게임, 웹페이지, http://ko.experiments.wikidok.net/wp-d/5973f1ffd4b02c822577133c/View