SymSensus 에 대하여

1. 레슬리 램버트는 비잔틴 장군문제는 참가자의 수가 배반자의 수보다 3배 이상되어야 배반을 극복할 수 있다고 하였다. 이러한 결과가 응용된 것이 BFT 계열이라고 부르는 PAXOS 알고리즘이다. 현재 PoW나 PoS이외의 거래속도를 해결했다고 주장하는 대부분의 메인넷 합의과정은 주로 PAXOS알고리즘의 변형으로 BFT계열이라고 불러야 한다.

3. 그러면 BFT 계열의 합의과정이 기존의 알고리즘을 어떻게 개선할 수 있는가를 살펴보면 참가자 N개의 노드를 임의의 집단으로 나누는 방법과 동시투표방식을 개선하는 방법으로 구분해볼 수 있다.

4. 사회선택이론은 전략적 투표이론으로도 부르며 게임이론의 한 분야이다. 이 분야의 학자들은 대부분 수학자들이다. 후생경제학(Welfare Economics)에서 가장 유명한 정리가 Arrow불가능성 정리(Arrow Impossibility Theorem) 이다. 그 내용은 다음과 같다.

   <모든 개인의 선호를 만족시키는 하나의 사회후생함수는 존재하지 않는다.>

   이 불가능성의 정리를 두 명의 수학자 Gibbard와 Satterswaite가 독립적으로 연구하여 사회선택이론에서 가장 유명한 정리로 바꾸어 놓았다. 바로 Gibbard - Satterswaite 정리이며 다음과 같다.

   <시민주권사회에서 3개 이상의 투표결과가 있을 때, Voting(투표방식)이 독재적이라면 어느 누구도 투표결과를 조작하여 이득을 얻을 수 없다>

   <조작하여 이득을 얻을 수 없다>는 <not manipulable> 또는 <Strategy Proof>라고 표현한다. 여기서 투표이론에서 독재적이라는 것은 Veto(거부권)을 의미한다. 이러한 거부권은 Golden share 등에 응용되고 있고 사회선택이론의 중요한 연구분야이기도 하다.

4. Gibbard - Satterswaite 정리의 문제점은 투표결과가 대상의 순서(Ordinality)라서 합의과정에 그대로 적용하기 힘들다. 그런데 Hylland라는 노르웨이의 수학자가 이 문제를 확률적 독재자 (Random Dictatorship)라는 방식으로 재해석하였다. 확률적 독재자라는 것은 Veto권을 가진 투표자를 확률적으로 선택하는 것을 말하며 이때 투표결과를 숫자(Cardinality)로 표현할 수 있다는 점이다. Hylland의 정리는 다음과 같다.

   <시민주권사회에서 확률적인 독재자(비토권)의 투표방식은 어느 누구도 투표결과를 조작하여 이득을 얻을 수 없다>

5. Hylland의 결과를 BFT에 적용하면 다음과 같은 정리(SymSensus Theorem)를 도출힐 수 있다.

<Veto권이 존재하는 BFT 합의과정에서 Primary 노드(확률적 독재자)가 블록을 생성할 때 투표참가자들은 합의과정을 조작하여 이득을 얻을 수 없다>

이 정리를 이용하면 SymVerse 합의알고리즘은 합의과정에 걸리는 시간을 기존의 알고리즘의 50% 이상 줄일 수 있다. 그 방법은 합의 알고리즘에 거부권그룹을 만들어 다음과 같이 투표를 진행하면 된다. 첫째, 합의과정에 참가하는 집단을 두 개로 분류하고. A집단은 정수[N/3] +1 개의 노드로 구성된다. A집단은 투표권만 있으며 모두 동일한 투표결과를 보여준다. 나머지 노드들은 B집단으로 부르고 블록을 생성하는 Primary 노드가 될 수 있으며 투표권을 가게 만든다. 두 집단이 동시에 합의를 시작하면 A집단은 과반수만 넘으면 투표권의 결과가 결정되고, B집단의 절반이 투표를 진행하면 자동적으로 투표결과가 나타나기 때문이다. 기존의 BFT에서 합의정족수가 정수[2N/3] +1 되어야 했지만 B그룹의 정족수가 정수[N/3]이 되면 전체적인 합의가 이루어진다. A그룹은 과반수만 넘으면 전체가 합의하기 때문에 A그룹의 합의 종료시간이 B그룹보다 항상 짧기 때문에 합의는 신속하게 이루어진다.

[참고문헌]

- Lambert, L., "Generalized Consensus and Paxos" Microsoft Research Technical Report MSR-TR-2005-33 , 15 March 2005.
- Lambert, L., "Fast Paxos", Distributed Computing 19, 2 , October 2006. pp.79-103.
- Lambert, L, Danny Dolev, Marshall Pease, and Robert Shostak "The Byzantine Generals" in *Concurrency Control and Reliability in Distributed Systems,* Bharat K. Bhargava, editor, Van Nostrand Reinhold (1987) pp. 348-369.
- Moulin, H. *The Strategy of Social Choice.* Series: Advanced textbooks in economics, 18. North-Holland: Amsterdam, The Netherlands. 1983.
- Peleg, B. Game Theoretic Analysis of Voting in Committees, Cambridge University Press, Cambridge, 1984.
- Hylland, A. "Strategy proofness of voting procedures with lotteries as outcomes and infinite sets of strategies," mimeo. 1980
- Sen, A. "The Gibbard random dictatorship theorem: a generalization and a new proof," SERIEs 2, 515-527, 2011.