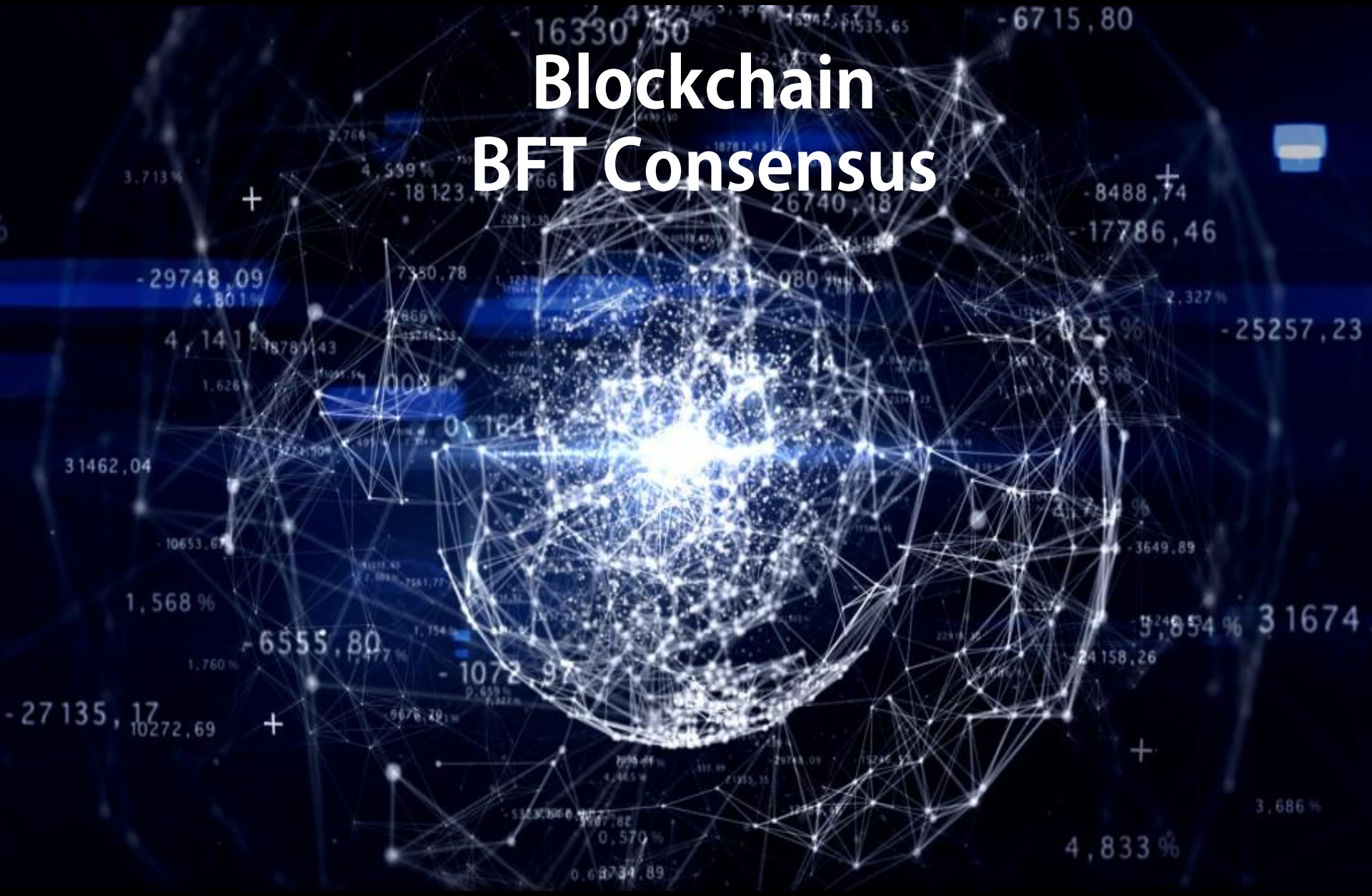

Blockchain
BFT Consensus

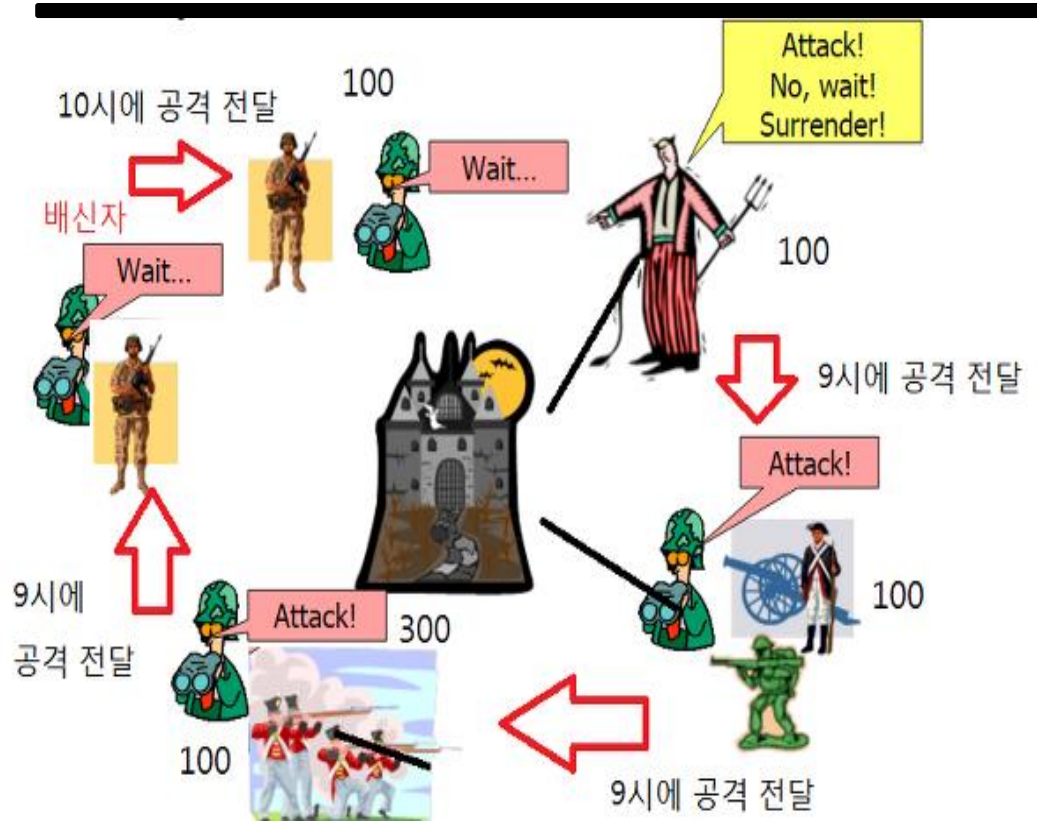
BFT(The Byzantine Generals Problem)

비잔티움 장군 문제(비잔티움 장애 허용)이란, 레슬리 램포트와 쇼스탁, 피스가 공저한 1982년 논문에서 최초로 사용된 표현이다.

가정 상황은 아래와 같다.
- 300 명의 병력이 있는 비잔티움 성을 100명씩의 병력을 가진 장군 5명이 치려고 한다.
- 이때 장군 5명은 모두 지리적으로 떨어져 있어, 연락병을 통해 소통이 가능하다.
- 이기려면 적 병력보다 많은 병력이 공격해야 한다.
- 장군들 중에는 배신자가 있어서 서로 신뢰가 불가능하다.

문제 상황) 서로 신뢰할 수 없는데, 어떻게 공격 시간을 합의 할 것인가?

BFT



장군1 : 장군 2 에게 9시에 공격하자고 전달

장군2 : 장군 3 에게 9시에 공격하자고 전달

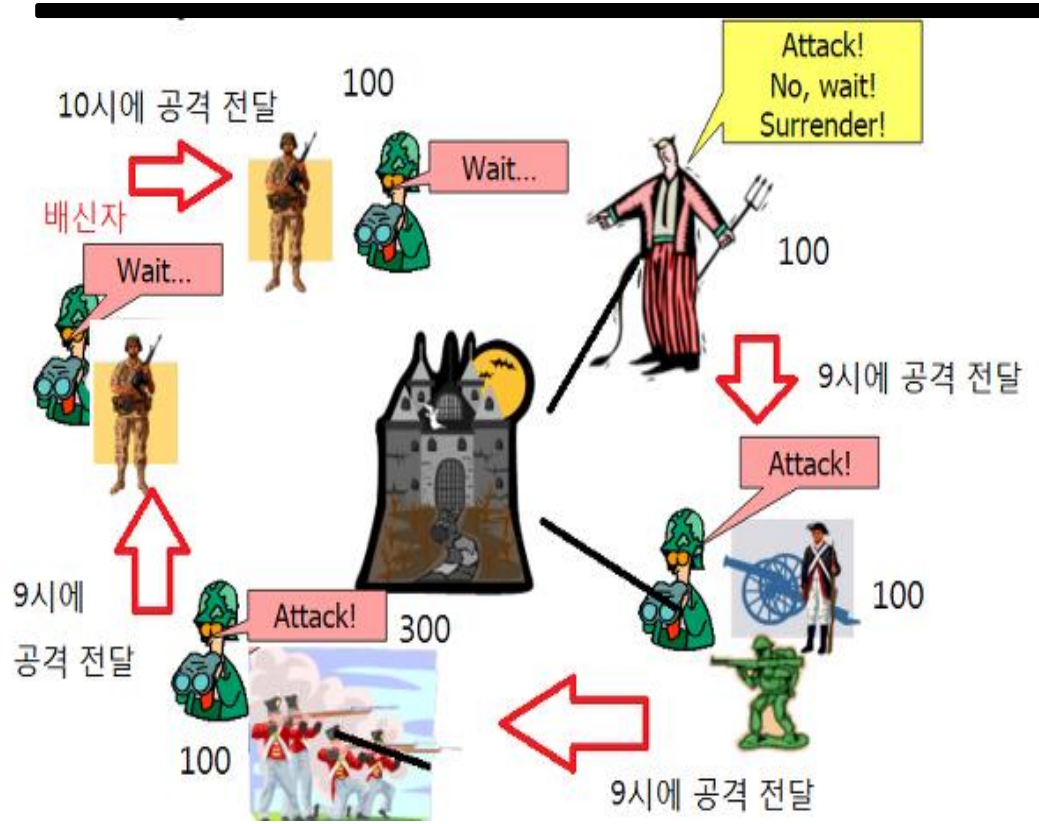
장군3 : 장군 4 에게 9시에 공격하자고 전달

장군4(배신자) : 장군 5 에게 10시에 공격하자고 거짓 전달

장군 5 : 10시 공격이라는 것 인식.

결과 : 9시에 장군 1 , 2, 3만 공격하게 되어 비잔티움 성 수복 실패.

BFT



즉 이러한 문제를 해결하기 위해서는 몇 명의 신뢰성 있는 장군이 필요한지, 통신 규약은 어떤식으로 해야하는지에 대한 문제가 바로 비잔티움 장군 문제 (비잔티움 장애 허용 : BFT) 이다.

Solving BFT Problem with POW Blockchain

블록체인은 여태까지 풀리지 않았던 문제인 BFT에 대한 해답으로 떠오르고 있다.
POW 블록체인을 이용한 해결법은 다음과 같다.
[새로운 규칙]

A. 장군들은 메시지를 보내기 위해 반드시 10분의 시간을 들여야 한다.
B. 메시지는 모든 이전 장군들의 메시지와 10분의 시간을 들였다는 증거를 포함하여 전송해야 한다.

BFT Scenario With New Rule

1. 장군1이 9AM 이라는 공격시간을 적어 10분간 작업하여 증거와 함께 장군2에게 보냄
2. 장군2는 9AM 이라는 메시지와 장군1의 10분 작업 증거를 보고 확신 후, 장군 3에게 9AM 메시지를 보냄(장군2도 10분간 작업하고, 장군1과 장군2의 메시지와 작업내용을 모두 포함하여 보냄)
3. 장군3은 배신자로 8AM 으로 메시지를 수정하여 보내고 싶으나, 그냥 보낼 수 없다. 아래과정을 해야한다.
   A) 10분보다 빠르게 10분간의 증거를 만들고 8AM의 메시지를 만들어내야 한다.
   B) 장군1, 장군2의 총 20분 작업에 해당하는 메시지 모두를 남은 시간내에 조작하여 다시 만든뒤 포함시켜 보냄
   이는 사실상 불가능하여, 들키기 싫으면 그냥 얌전히 9AM을 보내야 한다.
4. 장군 4, 장군 5 모두 동일