고려대학교 정보기술경영학회 ITS

블록체인 (Blockchain)

2022-2 학기 기술세션

목차

I. 블록체인

1. 블록체인의 기반과 탄생

블록체인은 분산 컴퓨팅 기술을 활용한 **데이터 위조, 변조 방지 기술**입니다. 이러한 아이디어를 처음으로 제시한 것은 스튜어트 하버(Stuart Haber)와 스캇 스토네타(Scott Stornetta)로, 1991 년에 'How to Time-Stamp a Digital Document'라는 논문에서 최초로 블록체인 아이디어를 제시합니다. 해당 논문에서, 하버와 스토네타는 암호 블록체인과 머클 트리(Merkle Tree)를 활용해, 타임 스탬핑을 통해 디지털 문서의 날짜가 변경되거나 위조되는 것을 막는 기술을 선보였습니다. 그러나 당시에는 이러한 기술이 실제 사용되지 못하고, 2004 년을 기준으로 특허권이 만료되었습니다.

1996 년, 닉 재보(Nick Szabo)는 **'스마트 컨트랙트'**라는 개념을 만들어냅니다. 스마트 계약은 제 3 의 중개기관 없이 개인과 개인 간의 P2P 방식을 통하여 원하는 계약 체결이 가능하도록 하는 계약 기능입니다. 단순히 이런 개념을 만들어 내는 것을 넘어서, 1998 년에 **분산형 디지털 통화를 이용하고 사용자의 컴퓨팅 파워를 가치로 변환할 수 있는 방법**을 고안해내고, 이를 비트골드(Bit Gold)라고 명명합니다. 비록, 비트골드 시스템은 실제로 실행되지 못하고 이론으로 남게 되었지만 컴퓨팅 파워를 저장할 수 있는 가치로 변환하는 이러한 방식은 향후 많은 암호화폐의 증명 작업의 근간이 되었고, 닉 재보는 '비트코인 구조의 선구자(A direct precursor to the Bitcoin Architecture)'로 불리게 됩니다.

비트골드와 유사한 시기에 웨이다이 (Wei Dai)는 분산 저장 방식을 활용한 암호화폐인 비머니(B-Money)를 고안해냅니다. 비머니는 각 참여자가 가지고 있는 비머니의 양에 대한 정보를 연결된 블록으로 저장하게 한다는 점에서 현대의 블록체인 기술과 상당히 유사한 개념을 가지고 있습니다. 또한, 현재 비트코인 네트워크가 사용하고 있는 **작업 증명** (POW: Proof of Work) 방식과 상당히 유사한 방식을 제시함으로써 비트코인의 탄생에 많은 영향을 끼쳤습니다.

웨이다이와 닉 재보가 어렴풋이 선보인 작업 증명의 개념이 명확해지는 것은 1997 년입니다. 아담 백(Adam Back)이 스팸메일과 서비스 거부 공격(Dos)을 막기 위해 해시캐시(HashCash)를 개발한 것입니다. 해시캐시는 이메일을 보낼 때, 실제 우편에서 사용하는 우표처럼 일정 양의 해시캐시를 지불하게 하여 대량 스팸메일을 막게 하려는 목적으로 만들어졌습니다. 이 해시캐시를 얻기 위해서는 컴퓨터 연산을 통해 일정한 해시를 찾도록 하는 **작업 증명 과정**을 거치도록 한 것입니다.

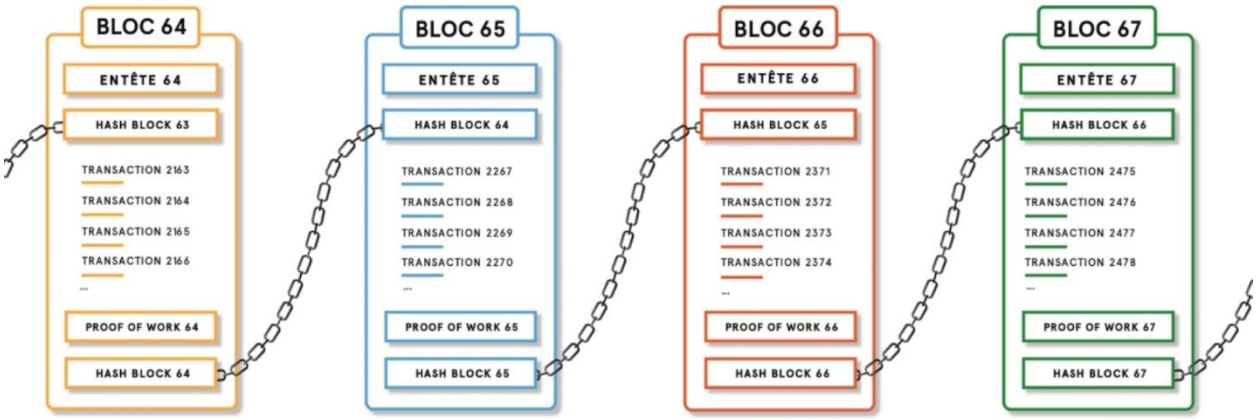
그러나 이 때의 작업 증명 방식은 다시 한번 큰 변화를 겪게 됩니다. 2004 년 할 핀니 (Hal Finney)가 **재사용 가능한 작업 증명 방식 (RPoW: Reusable Proof of Work) 시스템**을 제시한 것입니다. 기존의 해시캐시는 다른 사용자 간의 교환이 불가능했는데, 할 핀니는 해시캐시를 RSA 서명(RSA-sign)을 통하여 재사용 가능한 토큰으로 반환하고, 이를 개인 간 교환할 수 있도록 했습니다. 이 때, 이러한 토큰의 소유권을 모든 유저들이 실시간으로 확인할 수 있도록 설계된 서버에 기록하였는데, 이를 통하여 이중 지불 문제를 해결했습니다.

이렇듯 비트코인 탄생 이전에도 암호화폐를 실현하고자 하는 수많은 시스템과 실제로 암호화폐의 근간이 된 수많은 기술이 고안되었습니다. 이러한 시도는 현재, 암호화폐와 블록체인 기술이 구분되고 있는 시점에서도 암호화폐와 블록체인의 근간을 이루고 있습니다.

2. 블록체인의 구조

1) 블록과 체인

블록체인은, 당연하게도 '블록'과 '체인'으로 구성됩니다.

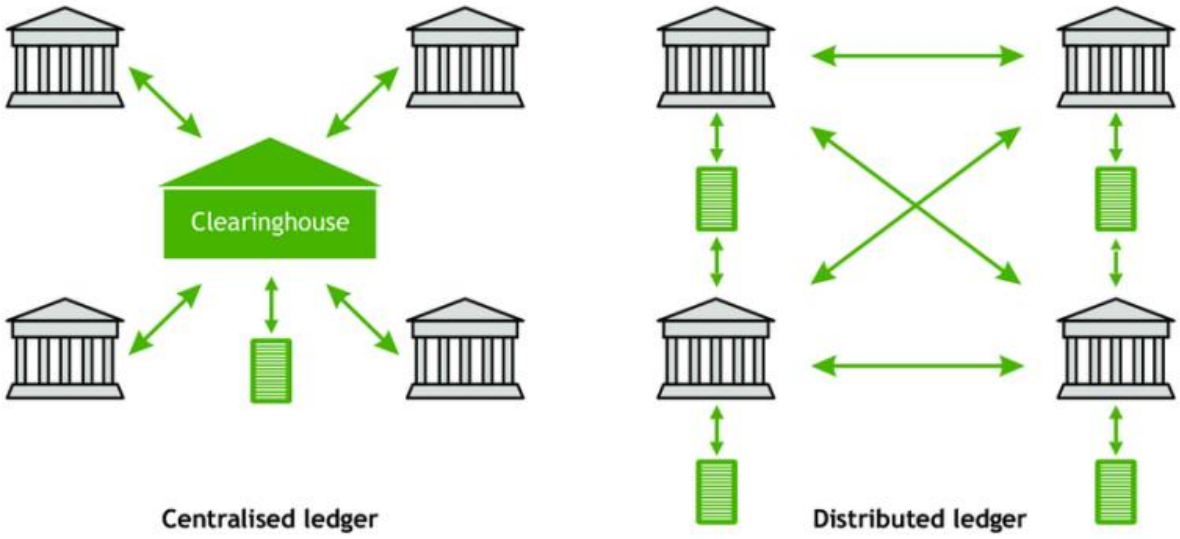


<그림 1-1. 연속된 데이터 체인 구조>

'블록'은 데이터의 저장 단위이자 방식입니다. 블록체인 구조에서 블록은 다수의 데이터를 포함하고 있습니다. 이러한 블록들이 체인, 말 그대로 사슬의 형태를 가지고, 시간 순서를 가지며 **연속적으로 연결**됩니다. 그러나 단순히 블록들이 시간 순서대로 놓여 있다면, 특정 블록에 있는 데이터를 위조, 변조하는 데에는 아무런 문제가 없을 것입니다. 따라서 이를 막기 위해 특별한 연결 방식이 필요한데, 이를 위해 해시 함수(Hash Function)가 사용됩니다.

해시 함수는 간단하게, 입력 값을 통해 출력 값을 얻기 쉽지만 출력 값을 통해 입력 값을 찾기가 어려운 함수입니다. (해시 함수의 자세한 구조는 Appendix 에서 찾아볼 수 있습니다.) 따라서 그림에서 볼 수 있는 블록 64 의 출력을 통해 다음 블록 65 의 입력을 찾아내기는 쉽지만 블록 65 의 입력을 통해 블록 64 의 출력 값을 찾아내기가 어렵게 됩니다. 이러한 성질로 인해, 블록 67, 66, 65 가 존재하는 상황에서 다른 블록을 블록 64 의 자리에 넣는 데이터 변조를 하기가 어려워지며, 데이터 변조의 난이도는 블록 64 이후에 블록이 더 많이 존재할수록 더욱 어려워집니다.

2) 분산원장 구조



<그림 1-2. 분산원장 구조>

블록체인이라는 기술이 고안된 배경에는 중앙 기관이 데이터를 관리하는 기존의 정보 체계에서 벗어나고자 하는 목표가 존재했습니다. 주로 트랜잭션, 화폐의 거래 내역을 이러한 방식으로 관리하고자 했기 때문에 이러한 방식을 분산 원장(Distributed Ledger)이라고 합니다. 여기서 '분산'이라는 의미는 분할 압축처럼 자료를 나눈 후 각 부분을 따로따로 저장하는 방식을 의미하는 것이 아니라, 모두가 자료 전체를 전부 중복해서 저장하는 것을 의미합니다. 이런 특징으로 인해, 블록체인 시스템은 해당 네트워크에 단 한 명의 참가자가 남게 되더라도 데이터를 보존할 수 있게 됩니다. 따라서 데이터의 영구성, 투명성을 얻을 수 있으며, 어떤 사용자가 어떤 거래를 남겼는지 모두가 공유하게 되므로 데이터의 추적 가능성과 신뢰성이라는 특징을 가지게 됩니다.

3. 합의 알고리즘과 비잔티움 장군 문제

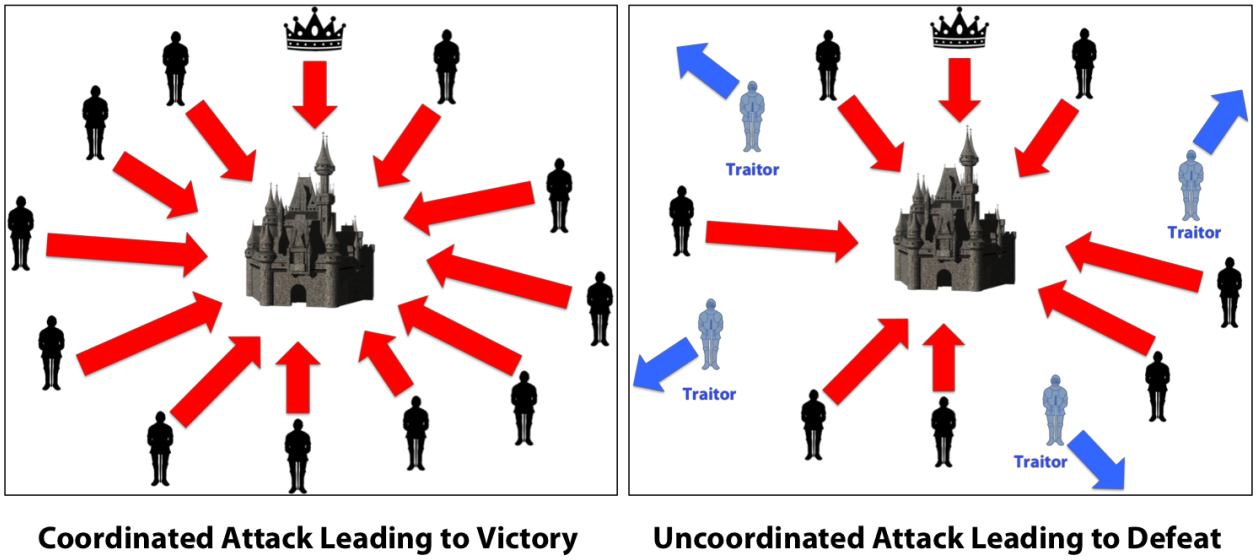
1) 합의 알고리즘의 필요성

분산형 시스템 기반의 블록체인 구조가 실제로 기능하기 위해서는 시스템 내부의 참여자들이 각각의 다른 참여자들의 정보가 올바른지 검증할 수 있어야 할 것입니다. 예를 들어, 새로운 블록이 생성될 때 누가 어떤 내용을 담은 블록을 네트워크에 추가할지에 대한 합의가 이루어져야 합니다. 이때 블록체인에서 사용되는 것이 다수의 참여자들이 통일된 의사결정을 할 수 있도록 돕는 합의 알고리즘입니다. 합의 알고리즘이 어떻게 등장했는지는 비잔티움 장군 문제를 통해 알아보겠습니다.

2) 비잔티움 장군 문제

앞서 중앙 집중형 시스템이 아닌 분산형 시스템을 통해 데이터를 보존하게 될 경우, 얻을 수 있는 이점에 대하여 살펴보았습니다. 그렇다면 왜, 블록체인 이전에는 분산형 시스템이 사용되지 않았던 것일까요? 혹시 분산된 시스템이 가지는 구조적인 문제가 있는 것은 아닐까요?

비잔티움 장군 문제(Byzantine Generals Problem)를 처음으로 제시한 것은 레슬리 램포트(Leslie Lamport)와 로버트 쇼스탁(Robert Shostak), 그리고 마샬 피스(Marshall Pease)였습니다.



<그림 1-3. 비잔티움 장군 문제의 성공과 실패>

1982 년에 발표한 논문에서, 세 명의 과학자는 비잔티움 제국의 여러 부대가 서로 교신하면서 공격 계획을 세우는 상황을 가정합니다. 모든 부대가 단 하나의 지휘체계에 맞추어 일사불란한 움직임을 보이는 경우에는 지휘관의 역량에 따라 작전의 성패가 결정될 것입니다. 하지만, 여러 명의 장군이 있고 장군 중 일부가 배신자일 수 있다고 가정하면 문제는 달라집니다. 일부 배신자가 공격을 중지하거나, 충직한 장군에게 잘못된 정보를 흘리기만 해도 작전은 실패하게 될 것입니다. 그렇다면 이러한 상황에서, '모든 장군이 동일한 공격 계획을 세우기 위해서 **얼마나 많은 충직한 장군**이 필요하고, **어떤 규칙을 통해 서로 교신**해야 하는지'가 비잔티움 장군 문제의 핵심입니다.

예시를 통해 이 문제가 생각보다 쉽지 않다는 점을 확인해보겠습니다. 충직한 브리엔니오스 장군은 다른 두 장군과 함께 페르시아의 거대한 도시, 크테시폰을 점령하고자 합니다. 역량이 출중한 브리엔니오스 장군은 다음날 오전 9 시가 성을 공격하기에 최적의 시기라고 판단하고, '20 일 오전 9 시에 공격한다'는 정보를 전령 테오도로스를 통해 다른 두 장군에게 전달하려고 합니다. 다음 세 가지 시나리오를 통해 발생할 수 있는 문제를 살펴보겠습니다.