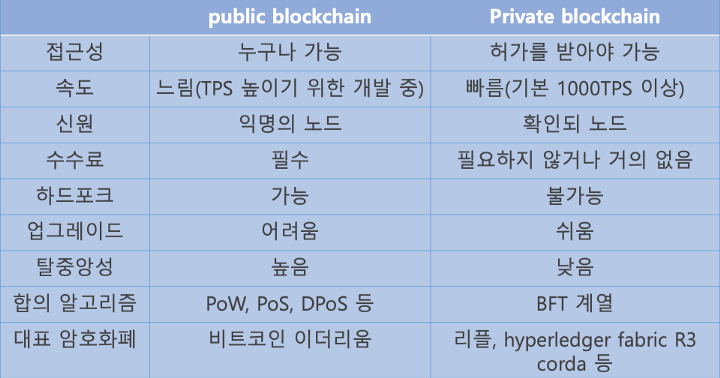
스마트 컨트랙트: 블록체인 위에 ‘약속’을 올려 놓는 것. 어떤 조건을 만족하면 어떤 행동을 하라는 코드를 추가한다.

Dapp(Decentralized application): 블록체인 위에서 구현되는 애플리케이션. 이더리움은 스마트 컨트랙트를 기반으로 개발자들이 자신이 원하는 애플리케이션을 만들 수 있도록 지원한다.

퍼블릭 블록체인: 비트코인 또는 이더리움과 같이 누구나 네크워크에 참여할 수 있는 블록체인

프라이빗 블록체인: 하나의 기관에서 독자적으로 사용하는 블록체인





컨소시엄 블록체인(Consortium Blockchain): 여러 기관들이 컨소시엄을 구성해 운영하는 블록체인, 즉 허가된 기관만 네트워크에 참여하는 블록체인

프라이빗 블록체인의 데이터가 변경되었을 때 탐지하기 위한 해결 방법: ‘앵커링Anchoring’이다. 프라이빗 블록체인의 거래 데이터 또는 블록 데이터의 해시값을 주기적으로 비트코인 등 퍼블릭 블록체인의 거래 안에 포함시키는 방식이다. 프라이빗 블록체인의 거래 데이터 해시값과 퍼블릭 블록체인의 해시값을 비교하여 데이터 위/변조 여부를 확인할 수 있다.

합의 알고리즘

PoW(Proof-of-Work): 비트코인을 비롯한 주요 퍼블릭 블록체인에서 채택하고 있는 합의 알고리즘이다. 블록을 만들어 배포한 후 많은 참가자가 사용하는 것을 올바른 블록으로 정의하기 때문에 참가자의 수에 영향을 받지 않고 얼마든지 참여자를 늘릴 수 있다. 반면 네크워크 상태에 따라 일부분에 불일치가 생긴 경우 ‘파이널리티 Finality’ 블록체인이 분기되었을 때 최종적으로 하나의 유효한 블록체인으로 확정되는 것’가 불확실하거나 확률에 의존할 수밖에 없다는 단점이 있다. 또한 PoW 방식은 속도가 느리다는 한계점이 있고 에너지 소모 역시 심각한 문제다.

PoS(Proof-of-Stake): 이더리움이 채택할 예정인 알고리즘이다. 화폐량을 더 많이 소유하고 있는 승인자가 우선적으로 블록을 생성할 수 있는 특징이 있다. 이것은 ‘대량 통화를 소유하고 있는 참가자는 그 통화 가치를 지키기 위해 시스템 신뢰성을 손상시키지 않을 것’이라는 전제를 바탕으로 한다. PoS 방식은 컴퓨팅 자원 소모가 아닌 자신이 가진 지분Stake을 통해 블록을 생성한다. 기본적인 구조는 poW와 다르지 않지만, 화폐량에 따란 해시 계산의 난도가 낮아지기 때문에 PoW와 비교해 자원 소모가 적다는 장점이 있다. 참여에 대한 보상은 이자와 같은 방식으로 코인이 지급되며, 일정 수 이상의 코인을 보관하고 있는 지갑을 블록체인 네트워크에 연결시켜놓기만 하면 보상을 받을 수 있습니다.

PBFT(Practical Byzantine Fault Tolerance): 네트워크의 모든 참가자를 미리 알고 있어야 한다. 참자가 중 한 명이 프라이머리가 되고 자신을 포함한 모든 참가자에게 요청을 보낸다. 그 요청에 대한 결과를 집계한 뒤 다수의 값을 사용해 블록을 확정한다. PBFT 방식은 언제나 참자가 전원과 커뮤니케이션애햐 하기 떄문에 참가자가 늘어나면 통신량이 증가하고 처리량이 저하된다. PoW나 PoS는 수천, 수만 개의 노드를 만들 수 있지만PBFT는 수십 개의 노드가 한계다.

DPos(Delegated Proof-of-Stake): 위임지분증명 이라 부르기도 하며 말그대로 위임된 POS입니다. PoS가 자산을 가진 사람들이 전부 참여할 수 있는 방식이라면 DPoS는 특정 인원에게만 POS를 할 수 있도록 권한을 위임하는 것입니다. 즉 특정인 몇 명만이 블록을 생성하여 증명할 수 있습니다.

HYPERLEDGER: 허가형 블록체인(권한을 얻어야 사용할 수 있는 블록체인). 프라이빗 블록체인 + 스마트계약

BaaSid.io 프로젝트: 한국, 일본, 싱가포르, 대만, 미국의 멤버들이 모여 전 세계 사용하지 않은 컴퓨터나 스마트폰의 저장 공간을 빌려 IDC 센터와 같은 서비스를 하려고 한다. 그러니까 각 가정에 쓰지 않는 컴퓨터나 스마트폰을 wifi에 연결하고 BaaSid 앱을 설치한 후에 사용하지 않던 컴퓨터의 저장 공간을 빌려주고 그 대가로 BAS토큰을 받는 것이다. 서비스 이용자는 BAS토큰을 구매해서 BaaSid에 지급해야 한다.

블록체인의 핵심은 해당 기술의 소스가 누구에게 종속되느냐에 있다. 일반적인 기술은 개발자, 개발사에게 100% 종속되기 마련이다. 하지만 블록체인은 다르다. 플레이어도 해당 소스에 대해 저작권을 행사할 수 있다. 이런 블록체인 기술을 게임에 적용할 때 얻는 이점에 대해선 게임 속 재화를 예로 들 수 있다. 예를 들어 기존 게임의 재화의 경우 게임 개발자, 개발사에 종속된다. 그러나 블록체인을 기반으로 한 재화의 경우 게임 속 재화에 대해서 플레이어가 재산권을 행사할 수 있을 뿐 아니라 현실 재화로까지 그 영역을 넓힐 수 있다.

이뿐만이 아니다. 디센트럴랜드가 적용한 ERC-721의 경우 대체 불가능하다는 장점을 가졌다. 이로 인해 게임 속 재화 역시 대체 불가능이라는 희소성을 가진다. 여기에 블록체인 기술을 도입한 게임끼리 재화를 교환할 수 있다는 점도 들 수 있다. '카운터 스트라이크'와 '배틀필드'의 두 게임의 재화는 각각 분리돼있는데 블록체인 기술을 도입한 게임이라면 이 같은 다른 게임끼리도 재화를 교환할 수 있다.

원문보기:

<http://www.inven.co.kr/webzine/news/?news=205446#csidxb1c6f52ef074d93802b4f881aeff8cc>