

The background of the slide is a dark blue field filled with a complex, interconnected network of glowing white and light blue lines and dots, resembling a digital or blockchain network structure.

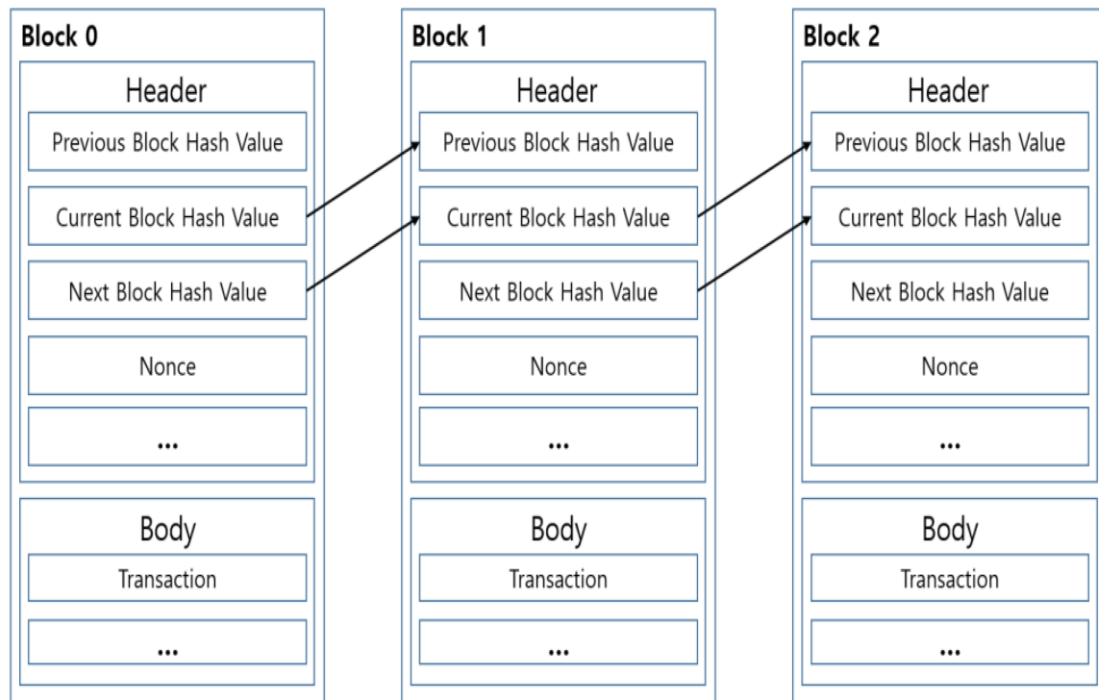
Blockchain Definition and Types

What is Blockchain?



블록이라는 데이터의 기본 단위를
사용하며 중앙서버 없는 풀어 P2P
네트워크를 기반으로 작동하는
분산 원장 기술이다.

Blockchain Structure - Block



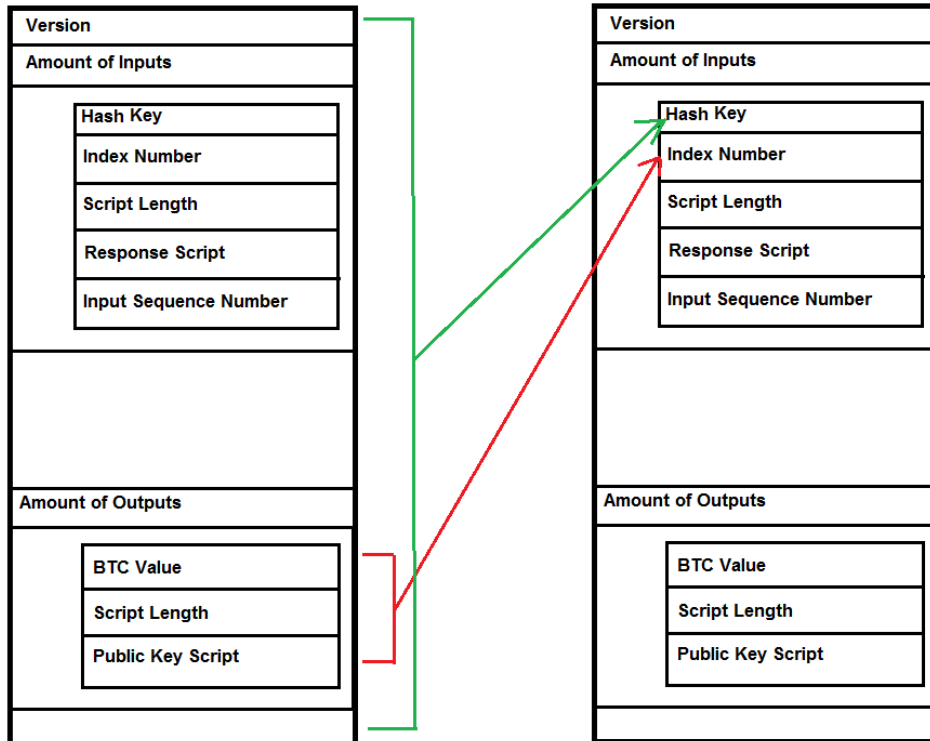
블록은 블록헤더와 Body로
나뉘어져 있다.

각각의 블록은 이전 블록과 현재
블록, 그리고 다음 블록의 해시
값이 들어간다.

링크드리스트와 유사한 구조지
만, 차이가 존재한다.

링크드리스트의 경우 접근을 위
해 앞뒤 노드의 주소값을 저장하
지만 블록체인의 경우에는 앞뒤
블록의 정보를 해싱하여 생성된
해싱값을 저장한다.

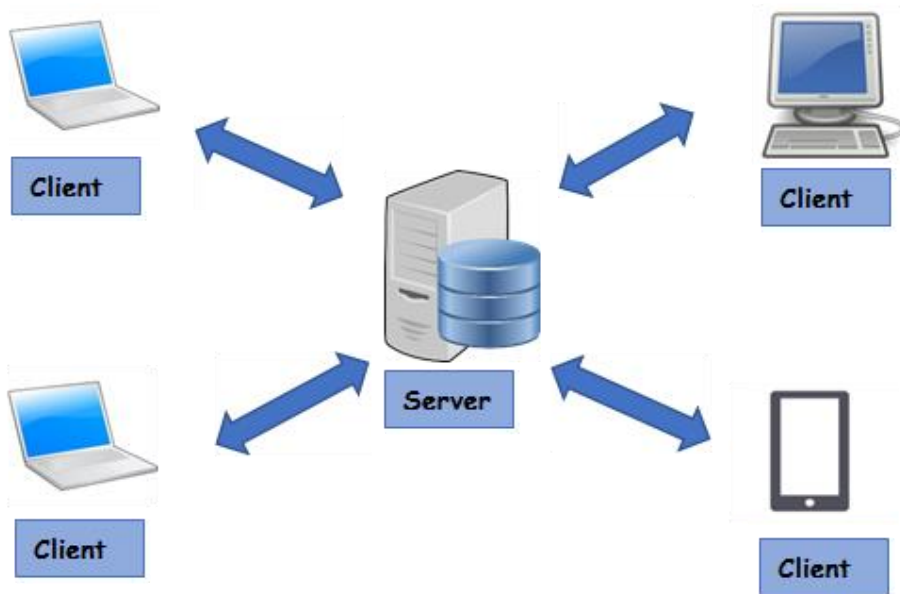
Blockchain Structure - Transaction



트랜잭션은 Version 정보와 Inputs, Output으로 구성된다. Input에는 블록 Index값과 순서에 대한 정보, Size등이 담기고,

Output에는 실제 전송할 암호화폐의 값과 Length, 공개키 서명이 들어간다.

Blockchain 적용의 이점 - Decentralized

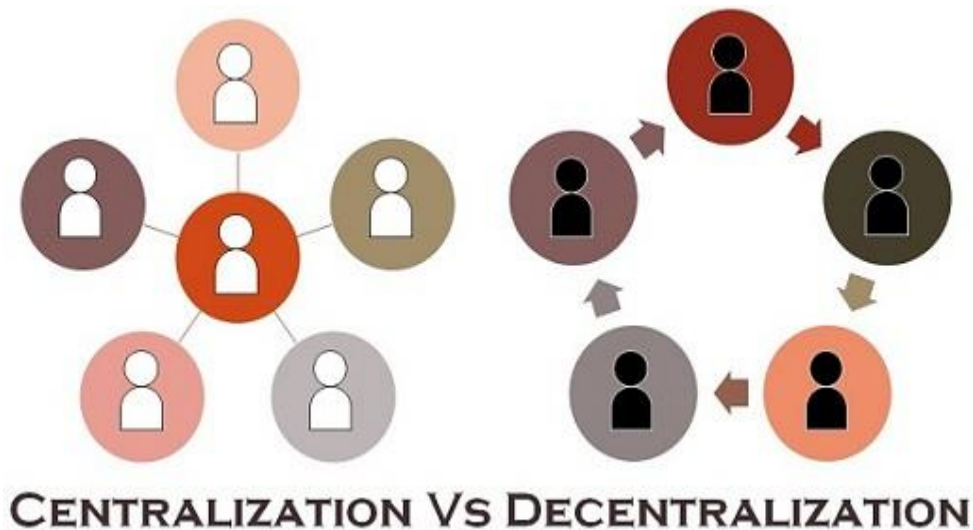


기존의 네트워크 방식은
Server-Client 구조가 대부분이었다.

하지만 Server-Client의 경우 중앙화 된 서버가 존재하게 되고, 만약 중앙화 된 서버에 문제가 발생하거나 해당 서비스 업체가 도산할 경우 우리는 서비스를 더 이상 이용할 수 없게 된다.

게다가, 중앙화 된 서버는 유저들의 정보를 멋대로 독점하여 기업 이윤을 창출하기도 한다. (Google, Amazon)

Blockchain 적용의 이점 - Decentralized

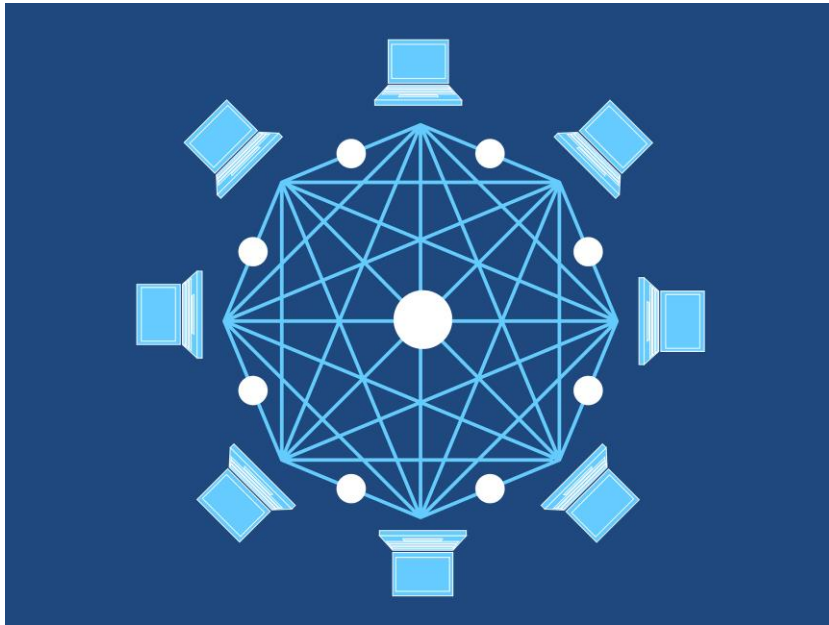


블록체인의 경우 기존의 중앙화 서버 방식에서 벗어나, 모든 노드가 Peer로 참여하는 Pure P2P 방식을 이용한다.

모든 노드가 서버와 클라이언트의 역할을 모두 수행하기 때문에, 적어도 하나 이상의 노드가 동작하고 있다면 서비스는 항상 동작할 수 있다.

또한, 모든 트랜잭션 정보가 투명하게 공개 되어 정보 불균형을 개선할 수 있다.

Blockchain 적용의 이점 – Trusted Network



블록체인은 모든 노드가 Peer로 참여하고 새로운 트랜잭션들을 담은 블록이 네트워크에 등록될 때, 항상 합의(컨센서스)를 거친다.

Consensus 알고리즘을 거치면서, 만약 블록이 조작되었을 경우 다른 피어 노드의 값과 대조하여 바로 알아차릴 수 있다.

블록체인에서 정보를 조작할 수 있는 유일한 방법은 51% 이상의 노드수를 확보하여 과반수의 동의를 받아 내는 것 뿐이다. 이는 현실적으로 불가능하다.

Blockchain 적용의 이점 – Token Economy



토큰 이코노미란, 원래 심리학에서 파생된 개념으로 아이들의 행동 발달에 사용되는 일종의 교육 방식이다.

보상이 존재하면 옳은 행동을 하게 된다는 이론이다.

현실 Economy와 같은 맥락이라고 보면 된다.

우리가 직장에 나가는 이유는 돈을 벌기 때문이다.

보상을 주게 된다면 Peer로 참여하는 모든 네트워크 참여자들이 생태계를 위해 봉사하게 되는 것이다.

Blockchain 적용의 이점 – Token Economy



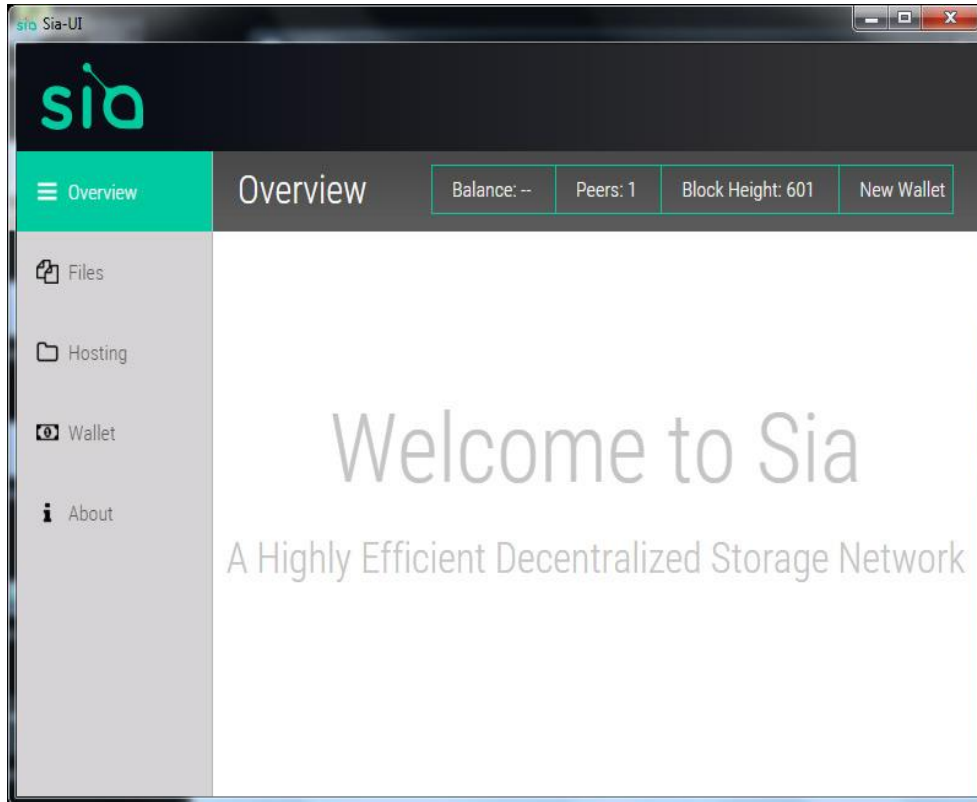
FaceBook, Google, Naver, Amazon이 가지고 있는 무기는 막대한 정보이다.

하지만 구글 검색엔진에 검색되는 답변, 네이버 블로그와 지식인의 답변, 페이스북의 소식과 피드, Amazon의 빅데이터는 사실 네트워크 참여자들이 만들어 낸 부가가치다.

그럼에도 불구하고 일반 유저들에게는 전혀 보상이 돌아가지 않는다.

블록체인의 Token Economy에서는 네트워크의 부가가치를 만든 참여자들에게 암호화폐를 통해서 보상을 제공한다. 이는 별도의 홍보 없이도 참여자가 네트워크에 참여하도록 하는 훌륭한 견인책이 될 수 있다.

Token Economy Case – Siacoin



Siacoin은 자체 블록체인 코어를 사용하고 있는 프로젝트로, 블록체인 기반의 클라우드 스토리지 서비스를 제공한다.

하지만 그 방식이 기존 클라우드와는 다른데, AWS나 Google등의 회사에서 제공하는 클라우드가 아니라, 네트워크 참여자들의 드라이브 공간을 이용할 수 있다.

하드 공간이 남아도는 사람들은 자신의 하드 용량을 제공하고, 클라우드 스토리지가 필요한 사람은 SiaCoin을 제공하는 대신 권한을 얻게 된다.

Token Economy Case – BAT (1/2)



BAT은 Firefox의 재단인 Mozilla의 대표였던 브렌던 아이크의 작품이다.

브렌던 아이크는 Mozilla 재단의 전대표이자, JavaScript의 창시자이기도 하다.

BAT은 블록체인 웹 광고 플랫폼으로, 광고주만 돈을 받을게 아니라, 광고를 보는 사용자들도 돈을 줘야한다는 발상에서 시작된 프로젝트이다. 자체 브라우저인 Brave Browser와 함께 사용된다.

구글이 매우 경계하는 프로젝트중 하나이다.

Token Economy Case – BAT (2/2)



Brave Browser는 BAT에서 만든 자체 브라우저로, 아직 Beta 버전이지만 실제 다운받아서 사용할 수 있다.

Brave Browser는 엄청난 Ad Block 기능을 가지고 있는데, 평소에는 Block상태였다가, 광고를 보겠다고 유저가 직접 선택하는 경우에만 광고가 표시되고 유저는 그 대가로BAT토큰을 받게 된다.

Brave Browser의 Ad block능력은 너무 강력해서, Google의 AdSense광고를 모두 없애 버리는데다가, 심지어 유튜브에서 처음 5초간의 광고마저 없애 버린다. 게다가 Block을 끌 경우에도 구글의 광고를 없애버리고 그 위치에 BAT 재단의 자체 광고를 넣는 패기까지 가지고 있다.

구글 광고 담당 수석 부사장의 인터뷰



구글에서 광고 담당 수석 부사장을 맡고 있는 쉬리더 라마스레미는 영국 런던에서 열린 세미나에서

“우리의 광고 시장을 위협하는 블록체인 프로젝트가 있다. 구글도 가만히 있을 수는 없어 자체 연구팀이 연구를 진행중이다.” 라고 답했다.

아마도 그 프로젝트가 BATI 아닐까 생각한다.

Public Blockchain Consensus Algorithm

P O W



**Consensus Algorithm
With Mining**

P O S



**Consensus Algorithm
With Stake**

D P O S



**Consensus Algorithm
With Delegated Stake**

Public Blockchain 개발 종류

Ethereum Dapp

가장 대중적인 블록체인 서비스 개발 방식으로
Ethereum Dapp형식으로 개발된 암호화폐의 종류는
수백~수천개에 이른다.
하지만 이더리움의 본질적인 한계점이 있고, 코딩 자체
는 간단하지만 그만큼 복잡한 프로그래밍은 불가능하다.

Eos Dapp

EOS는 기존의 Solidity방식과 달리 C++을 활용한
WASM 방식으로 코딩을 진행한다. 이로 인해 보다
빠르고 복잡한 프로그래밍이 가능하다.

Blockchain Core

EOS나 Ethereum, Qtum 기반으로 간단한 프로그래밍을 하는
것이 아니라 블록체인 코어 그 자체를 개발하는 것이다.
비트코인과 대다수의 블록체인은 C++로 개발되었지만,
이더리움이 Go로 개발되면서 최근에는 Go를 이용한 코어
개발이 떠오르고 있다. 어려워서 비 인기 분야이다.

다양한 블록체인 Case

	컨센서스 방식	블록체인 프로그래밍 지원	Smart Contract 지원	차별점
Bitcoin	POW	Yes (단순 스크립트)	No	블록체인 개념을 도입한 최초의 Cryptocurrency
Ethereum	POW+POS (Casper)	Yes (Solidity)	Yes	블록체인 프로그래밍 기능을 추가하여 블록체인 2.0시대를 열었다.
EOS	DPOS	Yes (WASM)	Yes	Ethereum의 문제점인 Gas 문제를 해결하였고 Dpos방식을 통해 속도를 끌어올렸으나, 아직 검증되지 않았다.
Quantum	POS	Yes (Solidity)	Yes	비트코인에 이더리움의 방식을 융합시켜 비트코인의 방식으로 트랜잭션을 처리하지만 Solidity로 Dapp개발이 가능하다.
Ripple	Ripple Protocol	No	No	은행권에서 사용한다고 해서 열기가 뜨거웠던 코인으로, 중앙화된 블록체인이라는게 특징이다.

Private Blockchain



HYPERLEDGER PROJECT

IBM과 Linux Foundation이 협력하여 개발한 HyperLedger Project는

암호화폐 없이 기업에서 사용할 수 있는 엔터프라이즈 형식의 블록체인 플랫폼을 지원한다.

이는 기업 내부에서의 효율적인 정보 처리를 위해서 사용되며, 컨센서스 방식이 간편하기 때문에 처리가능한 TPS(Transaction Per Second)가 Public 방식에 비해서 훨씬 높다.