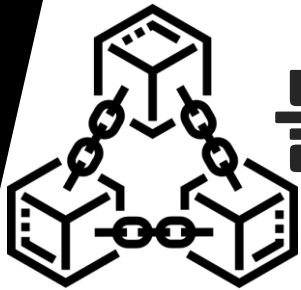




<https://github.com/Owen-Hwang/Newwave>



WEEK 1

블록체인의 개념과 이해

CONTENTS

01 블록체인이란 무엇인가?

02 블록체인의 기원

03 블록체인의 종류

04 블록체인 이해를 위한 핵심 개념 용어

05 블록체인의 활용

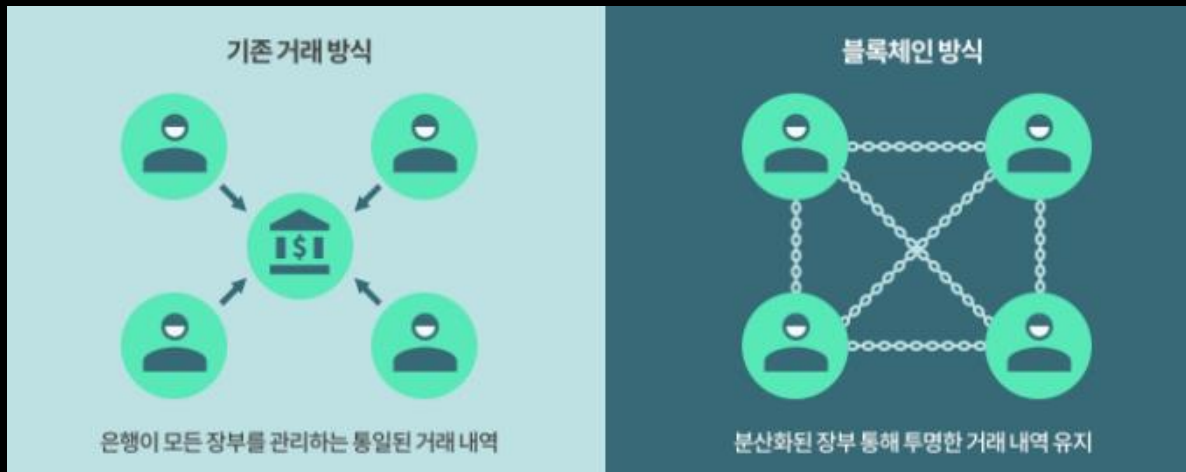
What is Blockchain

“Block + Chain”, ‘분산’원장

Blockchain [블록체인]

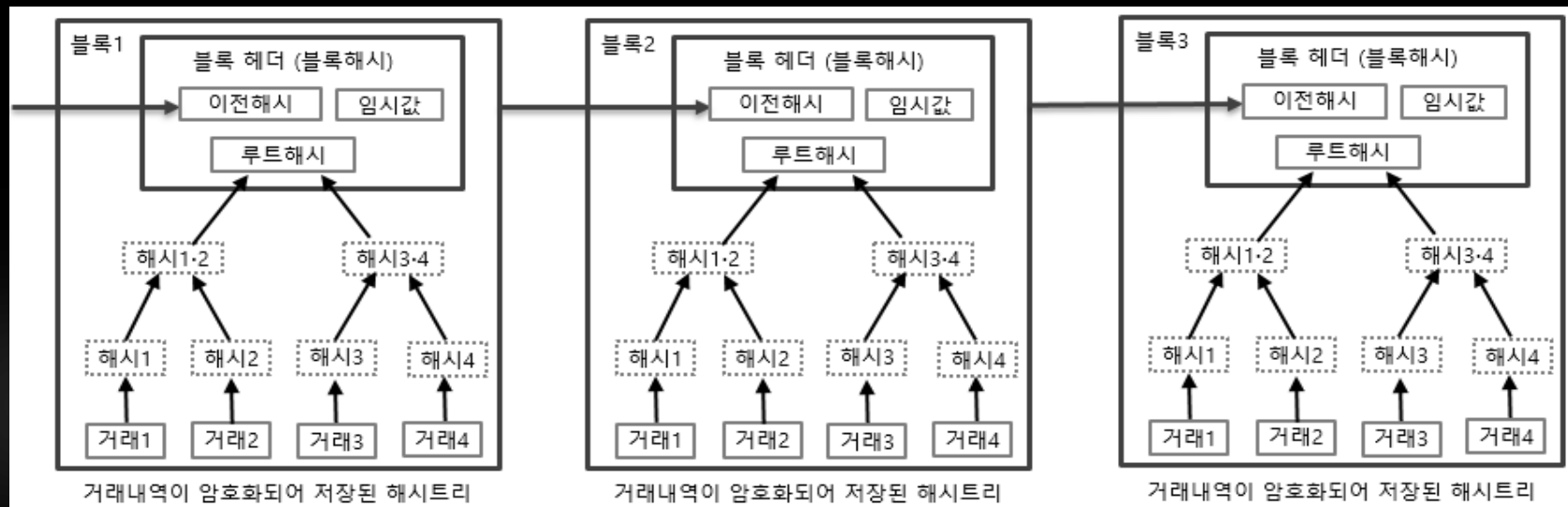
- 관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 원장 관리 기술의 일종

기본 원리



- 블록 구성
- 암호화
- 체인 연결
- 분산 저장

<https://youtu.be/uDm1BMdHg4>



Origin of Blockchain

Cypherpunk Movement

The Origin of Blockchain [블록체인의 기원]

사이퍼펑크 운동(Cypherpunk)

- 컴퓨터와 인터넷의 발달로 정부와 거대 기업이 개인의 사생활과 관련된 모든 정보를 수집할 수 있게 되자, 사이버펑크는 프라이버시(privacy) 보호를 강조하면서 이를 실현해 줄 암호기술에 관심을 가지게 되었다. 정부나 거대 기업들이 개인정보를 알 수 없도록 암호기술을 사용함으로써 프라이버시를 보호하고자 한 사회운동
- [참고 자료](http://www.news-paper.co.kr/news/articleView.html?idxno=35239) [http://www.news-paper.co.kr/news/articleView.html?idxno=35239]

사이퍼펑크 선언 (요약)

- 프라이버시는 전자 시대에서 열린 사회^[5]를 위해 필수적이다. 프라이버시는 비밀과 다르다. 프라이버시는 세상의 모든 사람들이 알게 되는 것을 원하지 않는 것이고, 비밀은 어느 누구도 알지 못하게 하는 것이다. 프라이버시는 자신에 대해 선택적으로 세상에 드러낼 수 있는 힘이다.
- 프라이버시를 보호하려면, 거래 당사자는 오직 해당 거래에 직접적으로 필요한 정보만 알아야 한다. 만약 가게에서 잡지를 구매하고 점원에게 현금을 건네준다면, 내가 누구인지에 대해 알려 줄 필요가 없다. 만약 그걸 알려줘야 한다면, 프라이버시가 보호되지 않는 것이다.
- 열린 사회에서 프라이버시를 보호하려면 익명의 거래 시스템이 필요하다. 지금까지는 현금이 그런 역할을 했다. 익명의 거래 시스템은 비밀 거래 시스템이 아니다. 익명의 거래 시스템에서 개인들은 자신이 원하는 만큼 자신에 대한 정보를 공개할 수 있다.
- 열린 사회에서 프라이버시를 보호하려면 암호기술이 필요하다. 내가 한 말은 내가 공개하고 싶은 사람들에게만 공개되어야 한다. 만약 내가 한 말이 전 세계 누구에게나 알려질 수 있다면, 프라이버시가 보호되지 않는 것이다.
- 정부나 기업 또는 다른 거대 조직들이 우리의 프라이버시를 지켜줄 것이라고 기대할 수 없다. 프라이버시 보호를 원한다면, 우리 스스로 지켜야 한다. 우리는 익명의 거래가 이루어질 수 있는 시스템을 만들기 위해 힘을 합쳐야 한다.
- 사이퍼펑크는 익명의 시스템을 만들기 위해 노력한다. 우리는 암호기술과 익명의 메일링 리스트 시스템, 디지털 서명, 그리고 전자화폐를 사용하여 우리의 프라이버시를 보호한다.
- 사이퍼펑크는 코드를 개발한다. 프라이버시를 보호하기 위한 소프트웨어를 개발해야 하는데, 우리 모두가 하지 않으면 프라이버시를 지킬 수 없기 때문에, 우리가 직접 개발할 것이다. 우리가 짠 코드는 동료 사이퍼펑크 개발자들이 이용할 수 있도록 전 세계에 무료로 배포될 것이다. 이 소프트웨어는 결코 파괴되지 않을 것이고, 광범위하게 분산된 시스템은 절대 정지되지 않을 것이다.
- 사이퍼펑크는 암호기술에 대한 규제를 반대한다. 암호기술을 규제하는 법률은 국가의 경계선을 벗어날 수 없다. 암호기술은 글로벌하게 퍼질 것이며, 그와 함께 익명의 거래 시스템도 전 세계로 확산될 것이다.
- 사이퍼펑크는 프라이버시를 안전하게 지켜주는 네트워크를 만들기 위해 적극 참여한다. 우리 함께 앞으로 힘차게 전진하자!

에릭 휴즈(Eric Hughes), hughes@soda.berkeley.edu, 1993년 3월 9일



이 선언문 중에서 특히 "사이퍼펑크는 코드를 개발한다." (Cypherpunks write code.)라는 문장은 사이퍼펑크 운동을 상징하는 유명한 문구가 되었다. 실제로 사이퍼펑크 운동가들은 자신의 사상을 현실에서 구현하기 위해 코드를 작성했고, 그 결과 2009년 1월 블록체인 기반의 암호화폐인 비트코인이 탄생했다.

『비트코인 제네시스 블록의 메세지』 #Block0

'Chancellor on brink of second bailout for banks, The Times, 03/Jan/2009' / '2009년 1월 3일, 은행을 위한 두 번째 긴급 구제 방안 발표 임박'



Type of Blockchain

Cryptocurrency is not universal

Type of Blockchain [블록체인의 종류]

	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	<ul style="list-style-type: none">● Anyone	<ul style="list-style-type: none">● Single organization	<ul style="list-style-type: none">● Multiple selected organizations
Participants	<ul style="list-style-type: none">● Permissionless● Anonymous	<ul style="list-style-type: none">● Permissioned● Known identities	<ul style="list-style-type: none">● Permissioned● Known identities
Security	<ul style="list-style-type: none">● Consensus mechanism● Proof of Work / Proof of Stake	<ul style="list-style-type: none">● Pre-approved participants● Voting/multi-party consensus	<ul style="list-style-type: none">● Pre-approved participants● Voting/multi-party consensus
Transaction Speed	<ul style="list-style-type: none">● Slow	<ul style="list-style-type: none">● Lighter and faster	<ul style="list-style-type: none">● Lighter and faster

- [참고자료](https://dragonchain.com/blog/differences-between-public-private-blockchains) [https://dragonchain.com/blog/differences-between-public-private-blockchains]

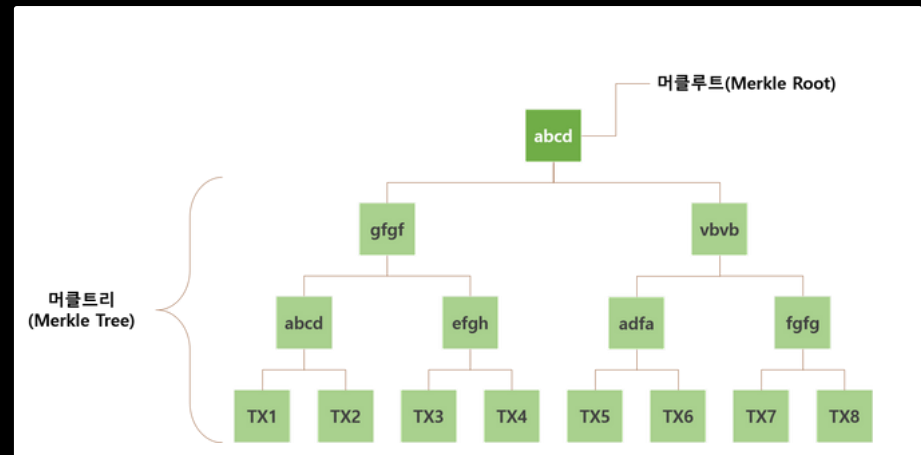
Keywords of Blockchain

Node? Hash?



Blockchain Keywords

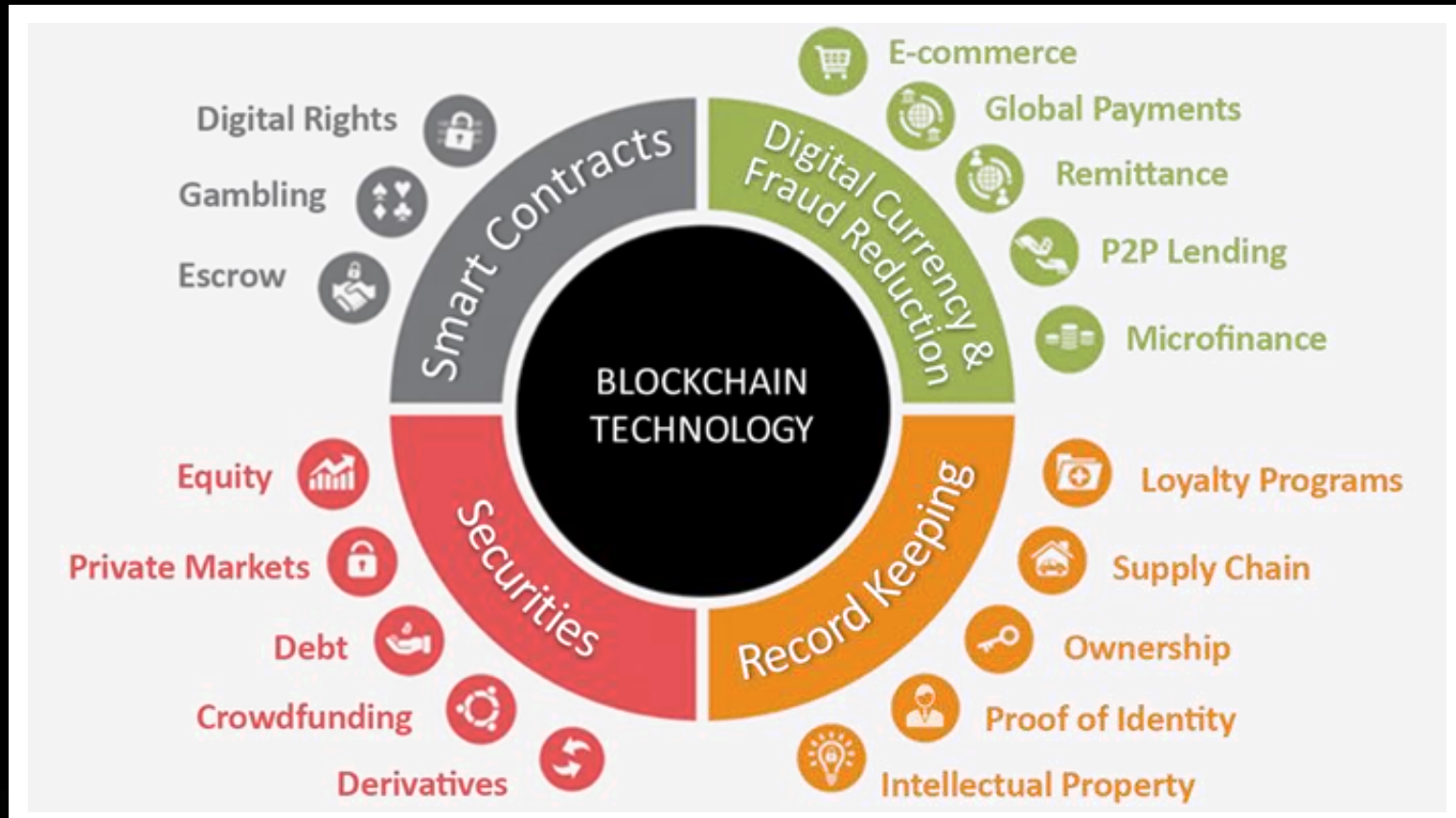
- Block
- Body
- Header
- Nounce
- SHA(256)
- Merkle Tree, Root
- Genesis
- Smart Contract
- Consensus Algorithm



Contents Title

For further details,
please contact us by e-mail

Application of Blockchain [블록체인의 활용]



- 블록체인 기술은 암호화폐, 스마트 계약, 물류관리, 문서관리, 의료정보관리, 저작권관리, 소셜미디어관리, 게임 아이템관리, 전자투표, 신원확인 등 다양한 분야에서 활용될 수 있다.
- [참고자료](http://wiki.hash.kr/index.php/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8#cite_note-50) [http://wiki.hash.kr/index.php/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8#cite_note-50]