

Block Chain

중급 정규교육

블록체인과 산업

1주차

Contents

블록체인과 산업

- ① 4차 산업과 블록체인개념과 주요용어
- ② 블록체인 주요 적용분야
(블록체인이코노미, CBCD)
(DEFI, NFT)
- ③ 블록체인 시범사업 둘러보기
- ④ 퍼블릭블록체인과 프라이빗 블록체인

- ❏ **블록체인개념**
- ❏ **4차 산업혁명**
- ❏ **블록체인 주요용어**

블록체인이란

- ❖ 데이터를 저장하는 방식
- ❖ 데이터에 생명을 불어넣는 작업
- ❖ 중앙화된 서버에서 처리되고 데이터 저장의 효율성만 생각하던 흐름이
- ❖ 여러 참여주체가 나눠 가지고 처리하면서 데이터의 신뢰를 바탕으로 IT를 재편할 수 있도록 흐름이 바뀌어 가고 있음



적용분야

스타벅스

- ▣ 2018 년 블록 체인 이니셔티브로 시작하여 르완다, 콜롬비아 및 코스타리카를 돕는데 Azure 블록체인 클라우드 서비스 사용
- ▣ 블록체인 기반의 커피 추적 시스템 구축
- ▣ 커피 메이커, 드라이브 스루 주문 및 추적을 포함한 서빙 프로세스 부분에서 블록 체인 사용

Xbox

- ▣ 게임 퍼블리셔에게 로열티에 관한 정보를 제공하기 위해 블록 체인 사용
- ▣ Xbox 게임 파트너와 아티스트, 음악가, 작가 및 기타 비디오 게임 콘텐츠 제작자들 간의 로열티 계약 추적, 관리 및 결제 처리에 대한 가시성을 높일 수 있음

- ❖ 사용자가 블록체인을 통해 임대료 2배의 금액을 보증금으로 제출한 다음 스마트폰을 이용해서 현관 문을 열고 집안의 다양한 서비스를 이용
- ❖ 이용이 끝나면 블록체인의 계약 내용과 비교하여 남은 금액을 정산해주는 서비스 제공



• 활용분야



WHY?

블록체인 특징



비즈니스 네트워크(Business Network)

비즈니스 네트워크 참여자들에 의해 거래가 합의



자산 추적(Provenance)

어떤 참여자에 의해 언제 거래가 수행되었는지 투명하게 가시성 확보



합의(Consensus)

비즈니스 네트워크의 거래정보가 일관성있게 하나의 뷰(View)로 공유됨으로써 신뢰제공



불변성(Immutability)

참여자들간의 분쟁을 쉽게 빠르게 해결



최종성(Finality)

오류나 사기위조에 대해 탄력적으로 대응

블록체인 장점

1 시간절약

거래처리 시간이 일(days) 단위에서 준 실시간처리

2 비용절감

중개자의 오버헤드 및 비용 감소

3 위험감소

조작, 사기 및 사이버 범죄 감소

4 신뢰확산

프로세스 공유 및 위변조 불가능한 기록을 통해 신뢰 확보

HOW?

❖ 비즈니스의 기반이 될 데이터를 저장할 수 있는 네트워크 구성

▣ 메인넷기술

- 퍼블릭 네트워크 사용 (이더리움, eos...)
- Hyperledger fabri과 같은 프라이빗 네트워크 구성툴 이용

▣ 참여할 주체들 모집

- ICO
- 컨소시엄네트워크
- 독점 프라이빗 블록체인

❖ 비즈니스 프로세스를 스마트 컨트랙트 프로그램으로 작성

▣ 토큰이코노미

▣ 블록체인 프로세스

❖ 블록체인 연동 웹서비스, 앱 개발

배워야 할 .. 것.. 들..

- ❖ 비즈니스 기획
- ❖ 비즈니스 프로세스
- ❖ 프로젝트 기획 설계 운용
- ❖ 프로그래밍
 - ▣ 네트워크 구성
 - ▣ 스마트컨트랙트 구현 배포 운용
 - ▣ 웹서비스 (웹서버, 웹클라이언트, 앱, 웹디비)
 - ▣ dAPP

관련 직업군

비즈니스 프로세스
-> 스마트 컨트랙트 개발자
네트워크 구성
-> 메인넷 개발자, 네트워크 아키텍처
서비스 개발자
-> 서버 API 개발, 운영
클라이언트 개발자
dAPP, 스마트 컨트랙트 연동

- ❖ ETRI 블록체인 연구소
- ❖ 삼성전자 블록체인 연구소
- ❖ 카카오 그라운드엑스 클레이튼
- ❖ ICON루프
- ❖ IBM - 블록체인 플랫폼

❖ DID

- ❑ myid, did initial did alliance, mykeepin
- ❑ 주로 통신사, 대기업들, 블록체인 회사들

❖ 국외는?

- ❑ facebook (diem), google (deep mind), ibm,

1
1

대학? 취업?

❖ 대학 전공

- ❑ 컴퓨터공학
- ❑ 소프트웨어공학
- ❑ 사이버보안
- ❑ 블록체인, 인공지능, IOT..
- ❑ 복수전공?
 - 산업공학, 금융공학, 수학과, 기계과, 전자과, 경영학과.....



❖ 대학원 전공

- ❑ 아주대학교 사이버보안 전문과정

❖ 한국표준협회 교육들

- ❑ 서울 ict 이노베이션 스퀘어
- ❑ <https://ict.eksa.or.kr/interact/ict.user>

기술적 정의

 블록체인은

비즈니스 네트워크에서 **트랜잭션**을 기록하고

자산을 **추적**하는 **프로세스**를 용이하게하는

변경 불가능한 **공유 원장**이다

좀더 쉽게...

- ❖ 데이터를 저장하는 기술
- ❖ 한곳에 저장하는 것이 아니라 여러곳에 중복적으로
- ❖ 보안이 우수하게 ->
데이터의 신뢰, 투명성을 높이도록
- ❖ 특정 서버의 공격이나 일탈로 서비스가 왜곡되지 않도록

블록체인 데이터 기반 서비스

- ❖ 데이터를 트랜잭션이라는 단위로 규격화 후 서명
 - ❖ 블록에 담아 누구나 바꾸지 못하도록 해시값으로 지문생성
 - ❖ 일관성있게 순서대로 나열하여
 - ❖ 모두가 나눠가지게 되는 기술
-
- ❖ 데이터를 처리하는 기술
 - ▣ 중앙서버에서 처리하던 명령들을 <- 공격받고 왜곡하고
 - ▣ 데이터를 나눠가지는 모든 노드들이나 선출된 노드들에 의해 검증하고 합의하여!
-
- ❖ 모든 데이터가 블록에?
 - ▣ 이력 검증이 필요한 데이터
 - ▣ 비즈니스 프로세스에 상호작용의 토대로 사용할 데이터

블록체인 생태계

0. 높은 생산성 (창업, 기획)

1. 통합 템플릿 플랫폼

2. 손쉬운 개발

네트워크-스마트컨트랙트-앱

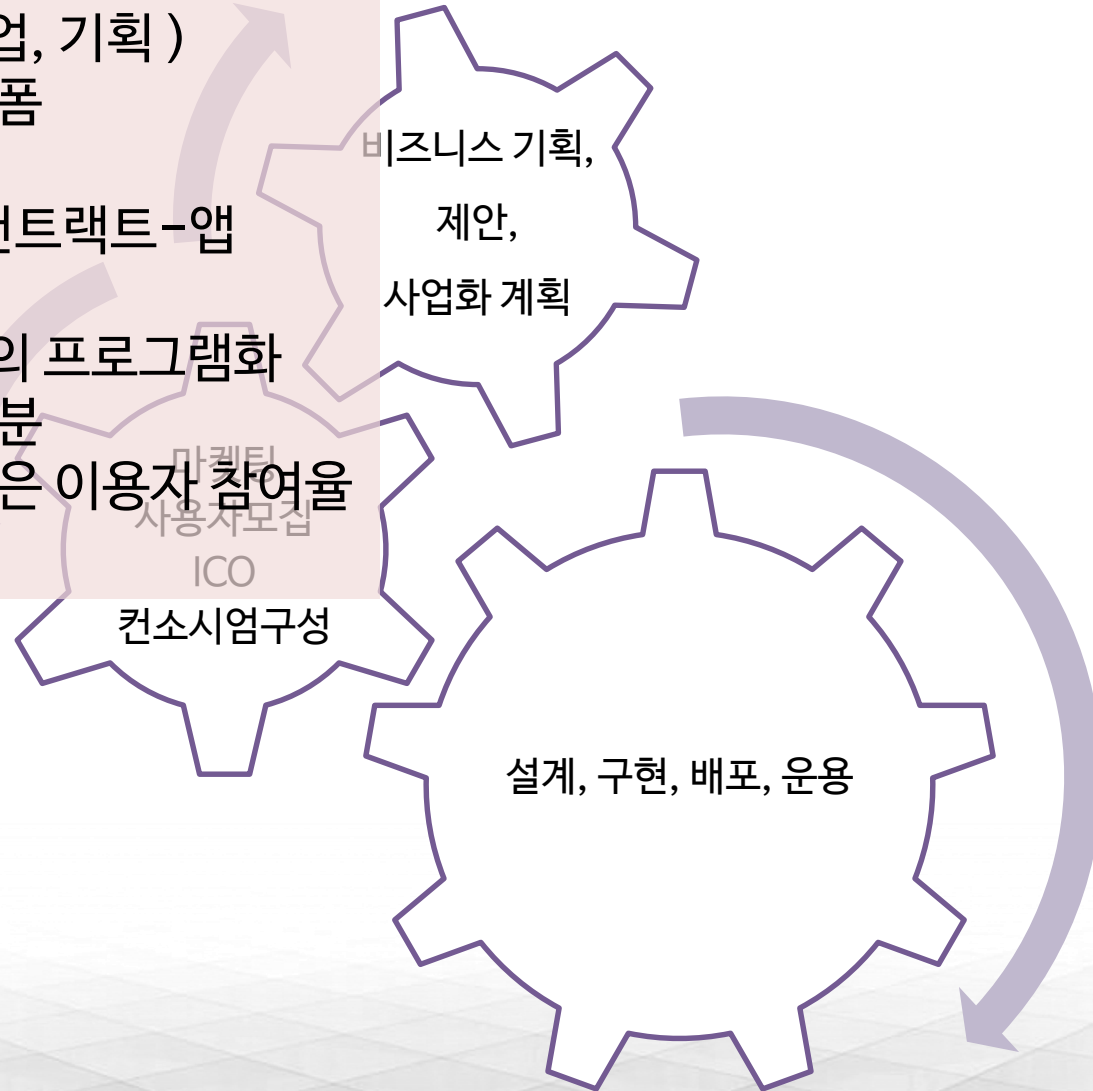
3. 운영자동화

비즈니스 프로세스의 프로그램화

4. 올바른 수익의 배분

5. 낮은 수수료와 높은 이용자 참여율

6. 자율 IT 생태계



탈 중앙화

커버넌스

- ▣ 일반적으로 ‘과거의 일방적인 정부 주도적 경향에서 벗어나
- ▣ 정부, 기업, 비정부기구 등 다양한 행위자가
- ▣ 공동의 관심사에 대한 네트워크를 구축하여
- ▣ 문제를 해결하는 새로운 국정운영의 방식

국가 중심의 화폐에서 서비스 중심의 화폐 개념으로...

블록체인에 암호화폐가 꼭 필요한가?

시초?

❖ 비트코인 (<http://bitcoin.org>)

- ❑ 암호화폐, 작업증명(POW)

❖ 데이비드 채움 David Chaum

- ❑ "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups" , first known proposal for a blockchain protocol, 1982
- ❑ DIGI CASH - 1989



David Chaum

4차 산업혁명

- ❖ **정보통신 기술(ICT)의 융합**으로 이루어지는 차세대 산업 혁명
- ❖ 핵심분야 기술혁신
 - ▣ 생물학
 - 생명공학, 헬스케어...
 - ▣ 물리학
 - 나노기술, 양자기술..
 - ▣ IT
 - 로봇공학, 빅데이터, AI, 데이터마이닝, IOT, 블록체인, 3D 프린팅...

추천도서

클라우스 슈밥의 제4차 산업혁명

클라우스 슈밥 지음 | 송경원 옮김



THE FOURTH INDUSTRIAL REVOLUTION



| 제4차 산업혁명 × 코로나19 |

클라우스 슈밥의 위대한 리셋

클라우스 슈밥 · 티베르티오 칼라초 지음 | 이진원 옮김

COVID-19: The Great Reset



클라우스 슈밥의 제4차 산업혁명

THE NEXT

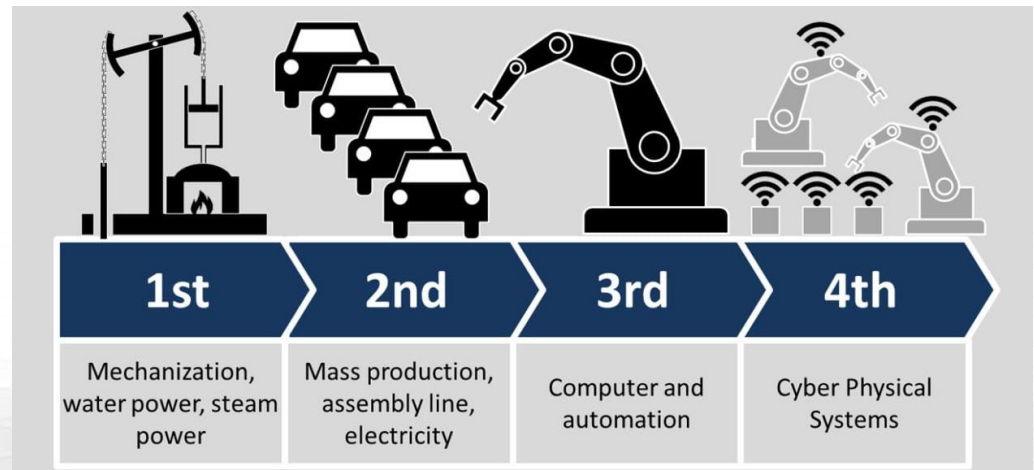
더 넥스트

클라우스 슈밥 지음 | 김민우·이영 옮김

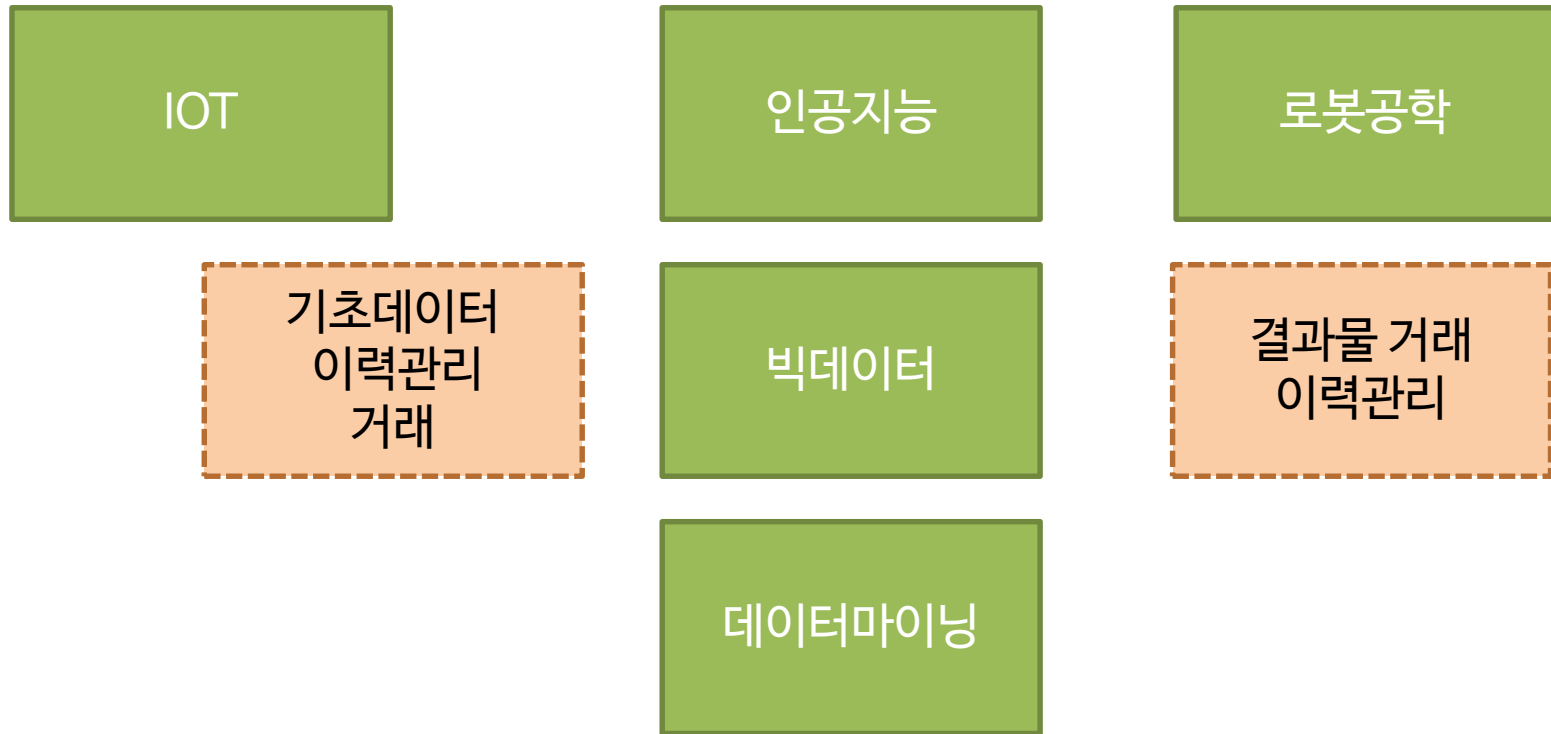


4차 산업혁명에서의 블록체인

- ❖ 통합 - 제2의 인터넷
- ❖ 손쉬운 개발
- ❖ 초연결
- ❖ 탈중앙화, 신뢰성 높은 데이터기반 서비스 프로세스
- ❖ 권력의 흐름
 - 국가 -> 기업 -> IT기업 -> 영리해진 개개인



IT 기술 속의 블록체인



데이터/시스템 보안, 거래 플랫폼, 결과물거래, 신뢰성 투명성,
비즈니스기획-개발-운용
블록체인 - 인터넷 2.0 - 초연결 - 탈중앙화

블록체인 핵심 기술

보안요소

- ▣ 키 기반 암호기술
- ▣ 해시 알고리즘
- ▣ 인증기술 - CA, PKI

네트워크 + 웹서비스 기술

합의 알고리즘 - 합의 알고리즘의 필요성과 분류

스마트 컨트랙트

블록체인 핵심 기술

보안요소

- ▣ 키 기반 암호기술
- ▣ 해시 알고리즘
- ▣ 인증기술 - CA, PKI

네트워크 + 웹서비스 기술

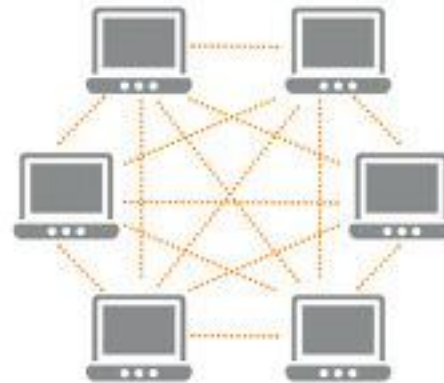
합의 알고리즘 - 합의 알고리즘의 필요성과 분류

스마트 컨트랙트

P2P 네트워크



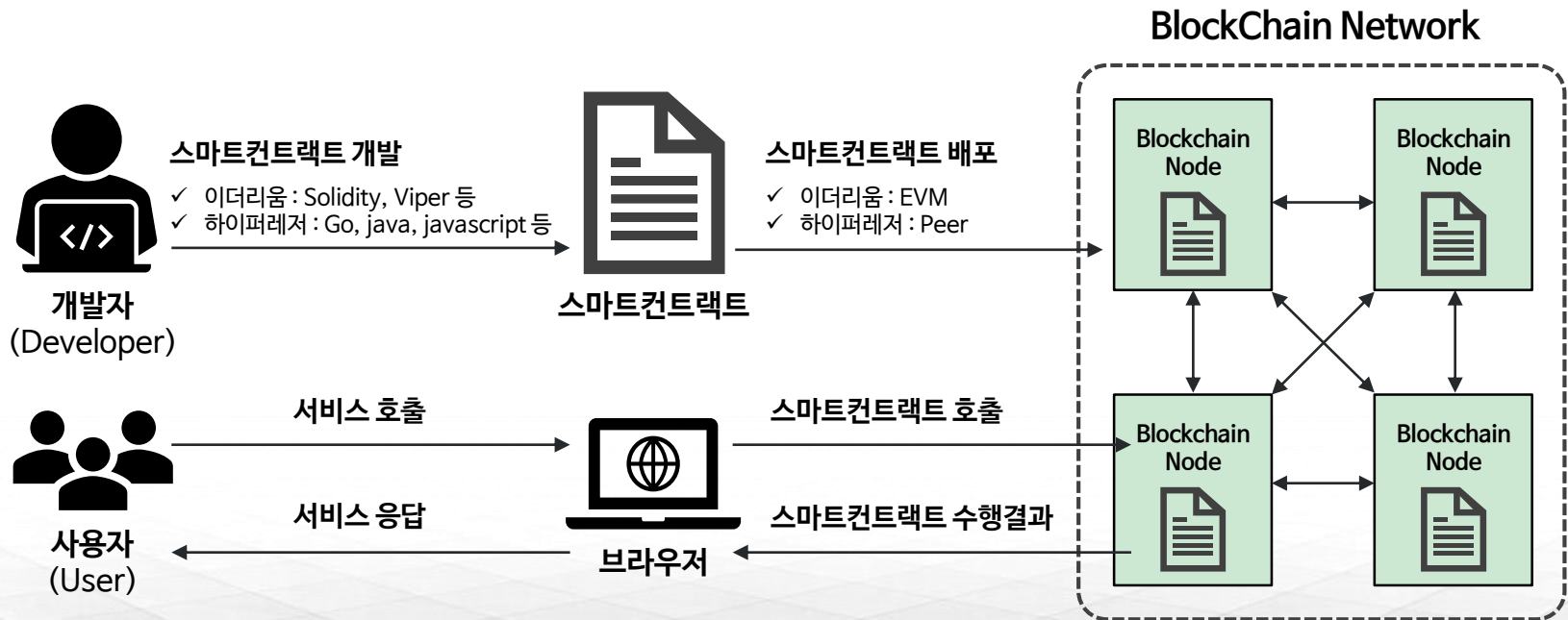
Server-Based



P2P

스마트 컨트랙트란

- 서면으로 이루어지던 계약을 코드로 구현하고 특정 조건이 충족되었을 때 해당 계약이 이행되도록 하는 개념
- 블록체인에서 동작하는 응용프로그램의 단위로 스마트 컨트랙트의 개발 흐름은 웹 응용프로그램 개발과 유사함



스마트 계약은 금융거래를 벗어나 블록체인 상에서 다양한 거래를 실현

- 중재자 없이 P2P로 계약을 체결하고 수정할 수 있는 기술
- 이해 당사자 간의 공유 네트워크를 통해 금융거래, 부동산 계약, 공증 등 다양한 형태의 계약에 대한 신뢰를 쌓아 나갈 수 있는 기반
- 중개자와 상호 거래 이력의 문서화 절차 없이 자동화된 계약처리가 가능



- 가구간 직접적인 P2P 전력거래 가능
- 신재생 에너지의 스마트 그리드 활용
(신재생 전자화폐, 전기차 충전 및 지불, 전력거래 결제 시스템)

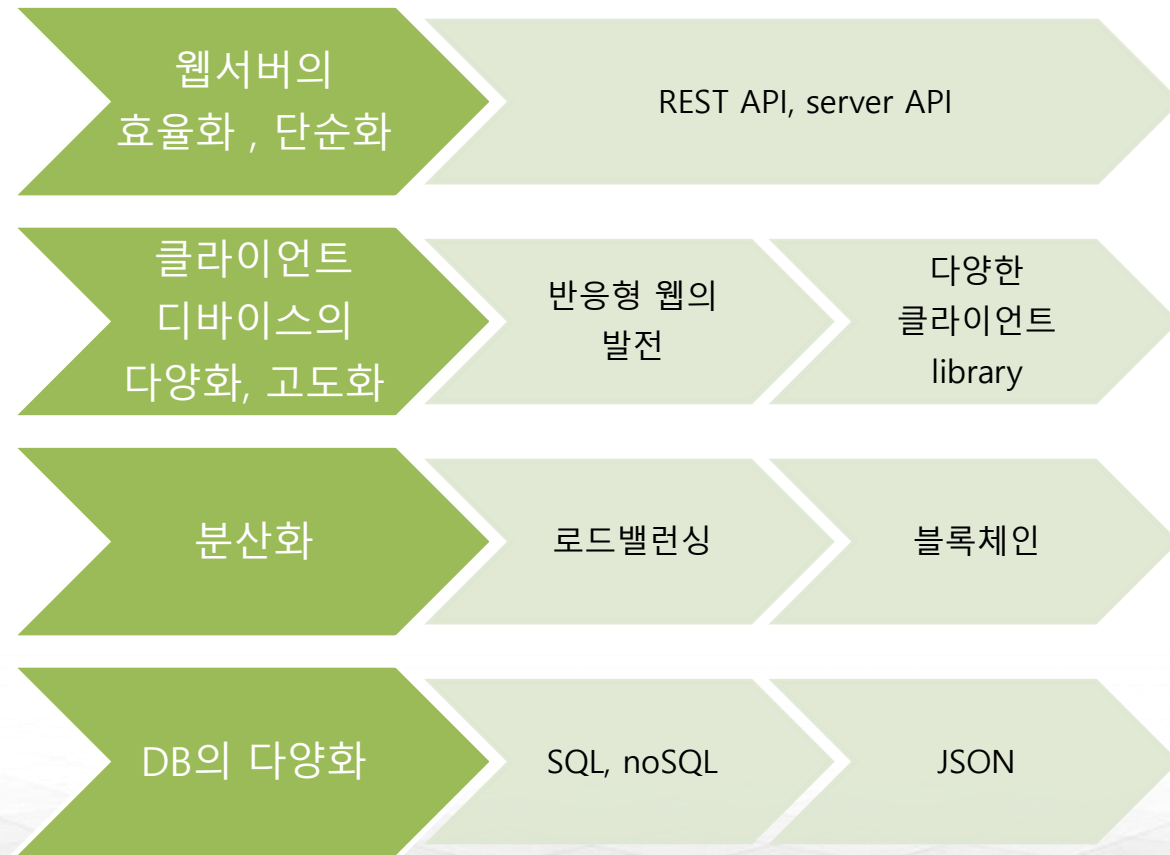
현재 금융업을 제외하면 블록체인 활용 형태가 각 개별기업에 국한되어 있어 거래 (계약) 중개, 공급망 구축 등의 시너지 효과는 발휘되지 않는 상황

개별기업의 도입단계를 거쳐 산업 내 블록체인 네트워크 형성이 현실화되기까지는 비용문제나 매뉴얼 수립 등이 필요해 다소 시간이 소요될 전망

현대의 웹서비스 기술

현대 웹서비스 기술의 특징

분업과 독립화



클라이언트 기술들

RESPONSIVE WEB DESIGN

- 미디어쿼리 [Media Queries]

- 유동적 레이아웃
레이아웃 크기를 상대단위로 지정

- HTML5 & CSS 3.0

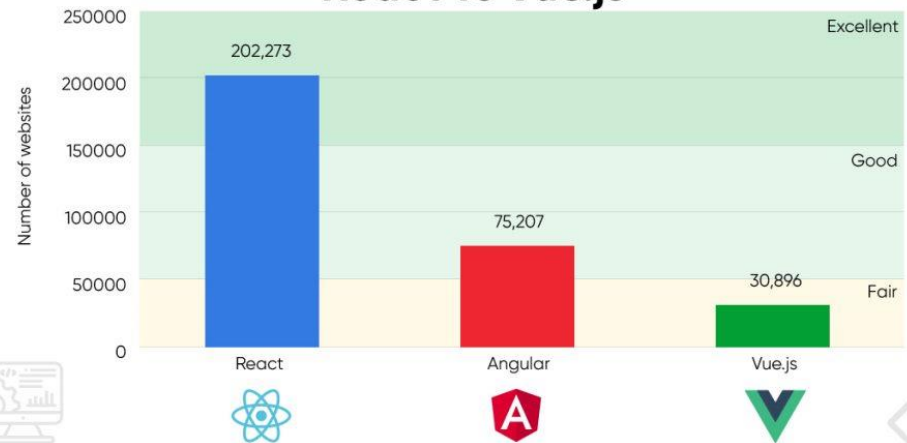
JavaScript, 미디어 객체들을 대체

- Adaptive Web Design(적응형 웹)

서버, 클라이언트 언어로 디바이스의 정보를 체크한 후
최적화된 마크업을 호출하는 기술

tms

Popularity: Angular vs React vs Vue.js



<https://www.tekkiwebsolutions.com/blog/comparison-of-angular-vs-react-vs-vue/>

웹서버 기술들



As an asynchronous event-driven JavaScript runtime, Node.js is designed to build scalable network applications. In the following "hello world" example, many connections can be handled concurrently. Upon each connection, the callback is fired, but if there is no work to be done, Node.js will sleep.

```
const http = require('http');

const hostname = '127.0.0.1';
const port = 3000;

const server = http.createServer((req, res) => {
  res.statusCode = 200;
  res.setHeader('Content-Type', 'text/plain');
  res.end('Hello World');
});

server.listen(port, hostname, () => {
  console.log(`Server running at http://${hostname}:${port}/`);
});
```

This is in contrast to today's more common concurrency model, in which OS threads are employed. Thread-based networking is relatively inefficient and very difficult to use. Furthermore, users of Node.js are free from worries of dead-locking the process, since there



Spring Boot 2.5.0



OVERVIEW LEARN SAMPLES

Documentation

Each **Spring project** has its own; it explains in great details how you can use **project features** and what you can achieve with them.

2.5.0 CURRENT GA	Reference Doc.	API Doc.
2.5.1-SNAPSHOT SNAPSHOT	Reference Doc.	API Doc.
2.4.7-SNAPSHOT SNAPSHOT	Reference Doc.	API Doc.
2.4.6 GA	Reference Doc.	API Doc.
2.3.12.BUILD-SNAPSHOT SNAPSHOT	Reference Doc.	API Doc.
2.3.11.RELEASE GA	Reference Doc.	API Doc.
2.2.13.RELEASE GA	Reference Doc.	API Doc.

Guides

Designed to be completed in **15-30 minutes**, a guide provides quick, hands-on instructions for **building a starter app** for any development task with **Spring**.

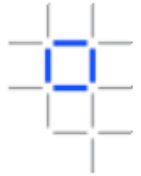
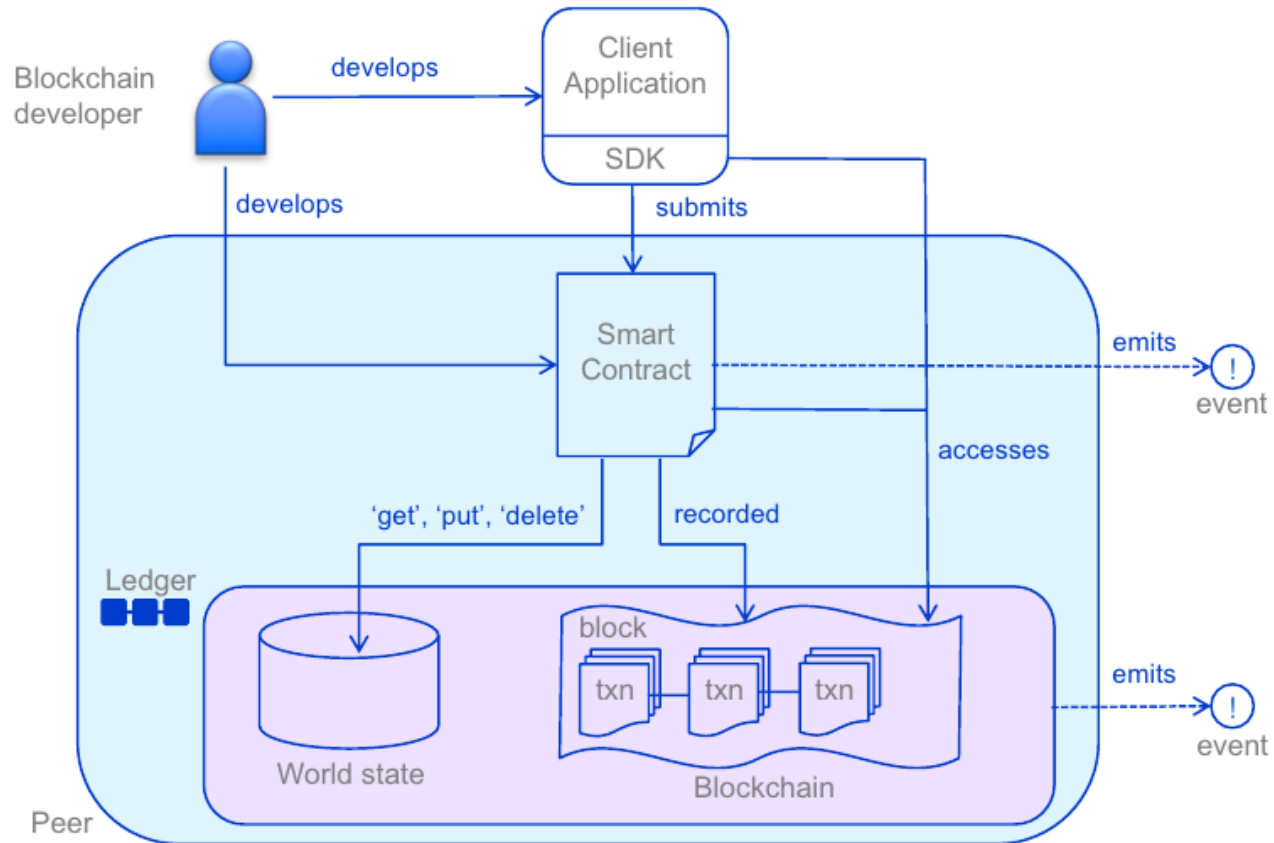


Building a RESTful Web Service

Learn how to create a RESTful web service with Spring.

어플리케이션

How applications interact with the ledger











IBM Blockchain

Peer

IBM

블록체인 컴포넌트

Ledger		Contains the current world state of the ledger and a Blockchain of transaction invocations
Smart Contract		Encapsulates business network transactions in code. Transaction invocations result in gets and sets of the ledger state
Consensus Network		A collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger
Membership		Manages identify and transaction certificates, as well as other aspects of permissioned access
Events		Creates notifications of significant operations on the Blockchain (e.g. a new block), as well as notifications related to smart contracts. Does not include event distribution
Systems management		Provides the ability to create, change and monitor Blockchain components
Wallet		Securely manages a user's security credentials
Systems integration		Responsible for integrating Blockchain bi-directionally with external systems. Not part of Blockchain, but used with it

2018 Key issues Study | 6

블록체인에서의 어플리케이션

블록체인 네트워크

geth
hyperledger fabric

...

블록체인 스마트컨트랙트

solidity
chaincode

...

웹서비스

웹서버
웹클라이언트
데이터베이스

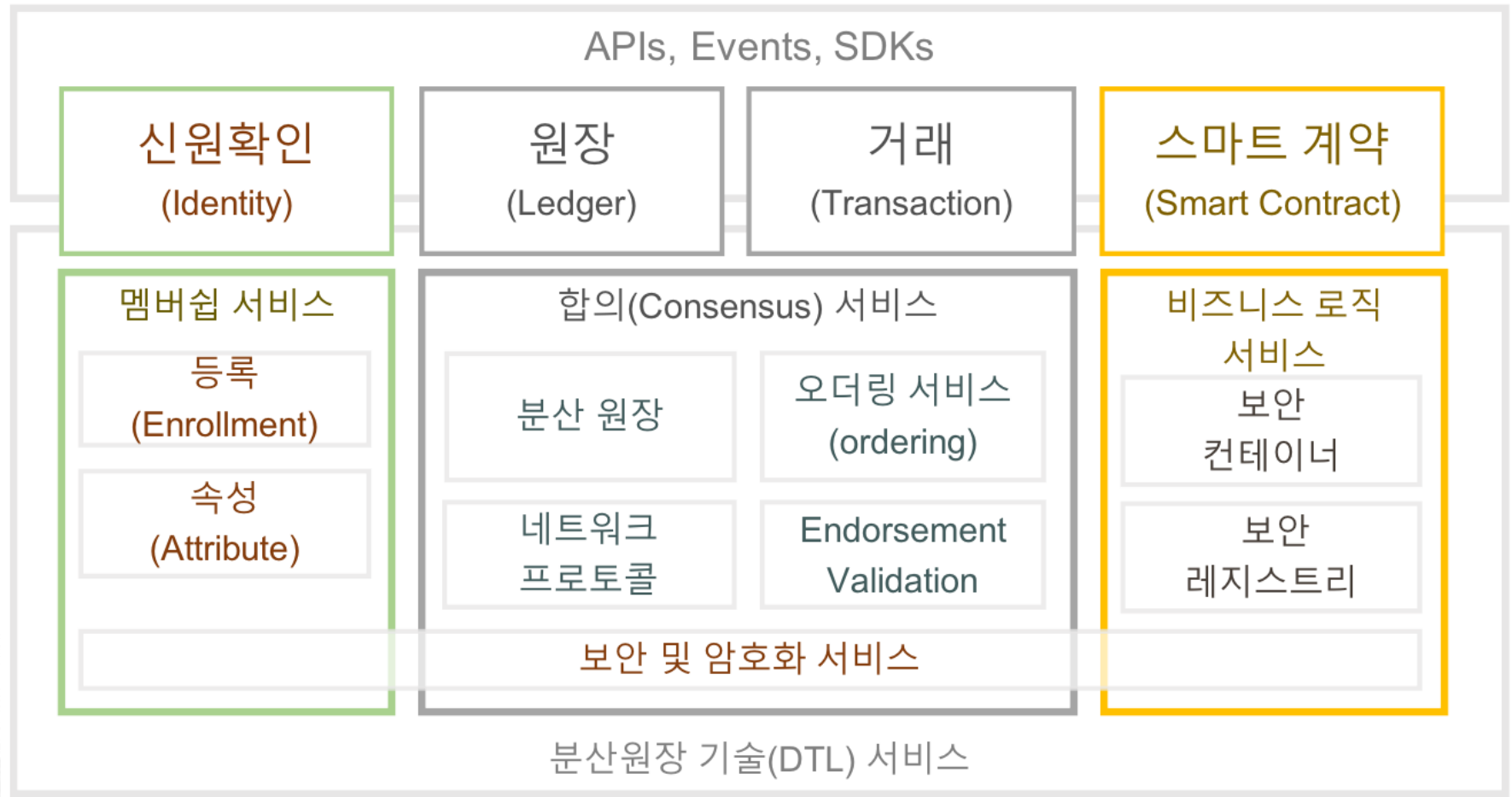
...

?

블록체인 기초 기술들

- ❏ 참조모델
- ❏ 블록체인 기본구조
- ❏ 합의

하이퍼레저 패브릭 참조모델

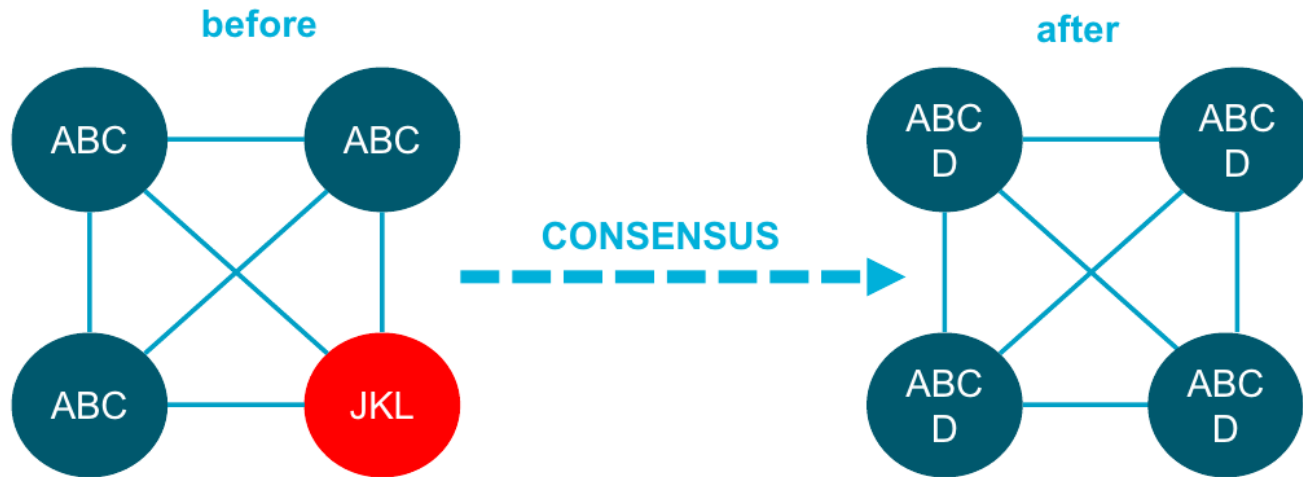


블록체인 원장구조



합의(Consensus)란 ...

- 블록체인 모든 참여자의 원장(블록 및 상태)에 일관성이 있는지 확인

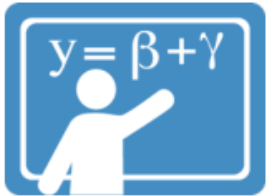


- 거래 및 거래 실행 순서에 대한 동의
- 동일한 원장을 유지하기 위하여 검증 참여자들의 상태를 동기화
- 거래원장이 일치하지 않는 참여자 노드의 상태 수정
- 악의적인 참여자 노드들은 격리

peer/node

Ledger
State

합의 알고리즘 예시



Proof of work



Proof of stake



Solo /
No-ops



Kafka /
Zookeeper



Proof of
Elapsed Time



PBFT
based

추가 블록체인가기술

📦 거래소기술

- 중앙화된 거래소 : 위임 -> pub/priv 키관리
- > p2p 거래소 : 개인의 지갑에 pub/priv 키를 블록체인기술 별로 저장
- 개인간의 1:1 거래를 만들어내는 기술
- Uniswap v3 -> Ethereum Token 을 사용해서 작성된 스마트 컨트랙트

📦 -> Defi (암호 자산의 거래)

- 암호화폐 -> 거래 -> 중간단계 암호화폐 -> 분산금융 (거래, 대출:암호화폐, 스테이킹-이자수익-암호화폐 동결 - POS작동, 파생상품)
- 토큰구현 : erc20...

📦 NFT (암호 자산의 생성과 활용)

- 암호화폐 vs 자산에 대한 블록체인화 (디지털 자산 : 디지털사진 - ID, 결과물, 생성-활용-거래=> app 으로 구현)
- 토큰구현 : erc721...

블록체인개념정리-용어

블록
블록체인
분산원장

거버넌스
컨소시엄

트랜잭션

암호화폐
gas
수수료 보상
마이닝-채굴

합의알고리즘
작업증명-**POW**
지분증명-**POS**

네트워크
P2P
서버-클라이언트

피어
노드

비대칭키
개인키 공유키
해쉬
머클트리

블록체인개념정리-용어

블록
블록체인
분산원장

거버넌스
컨소시엄

트랜잭션

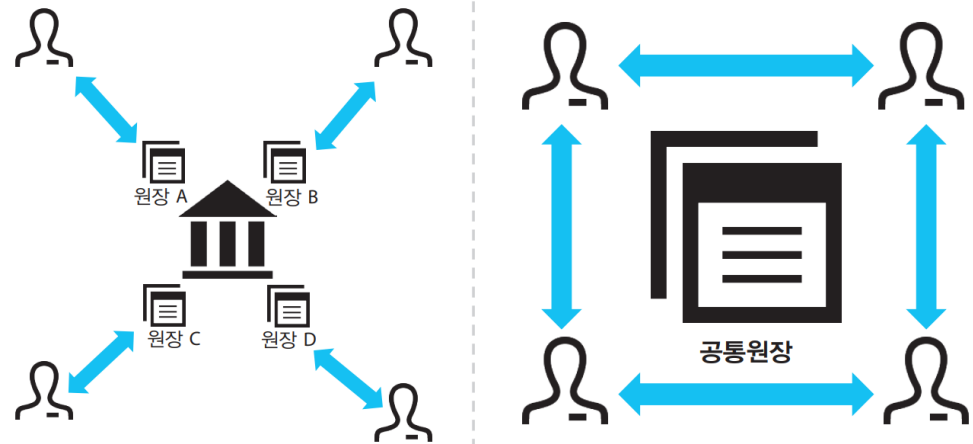
암호화폐
gas
수수료 보상
마이닝-채굴

합의알고리즘
작업증명-POW
지분증명-POS

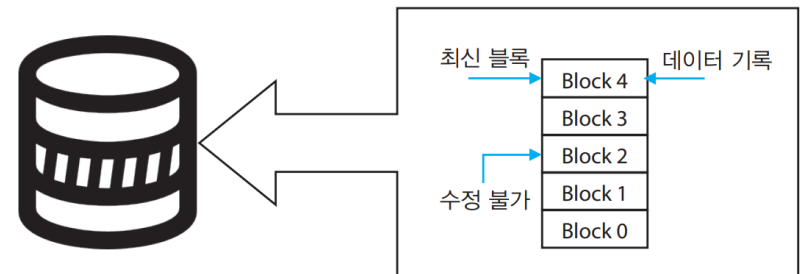
네트워크
P2P
서버-클라이언트

피어
노드

비대칭키
개인키 공유키
해쉬
머클트리



• 오늘날 비즈니스 네트워크 VS 블록체인 비즈니스 네트워크



• 블록체인의 Append-only 저장 방식

블록체인개념정리-용어

BFT
비잔틴장애극복

스마트컨트랙트
체인코드

플랫폼
SDK, API

멀티체인

하드포크
소프트포크

WEB3
JSON
JSON-RPC

VM
JVM EVM CCENV

ONCHAIN
OFFCHAIN
SIDECHAIN

블록체인개념정리-용어

BFT
비잔틴장애극복

스마트컨트랙트
체인코드

플랫폼
SDK, API

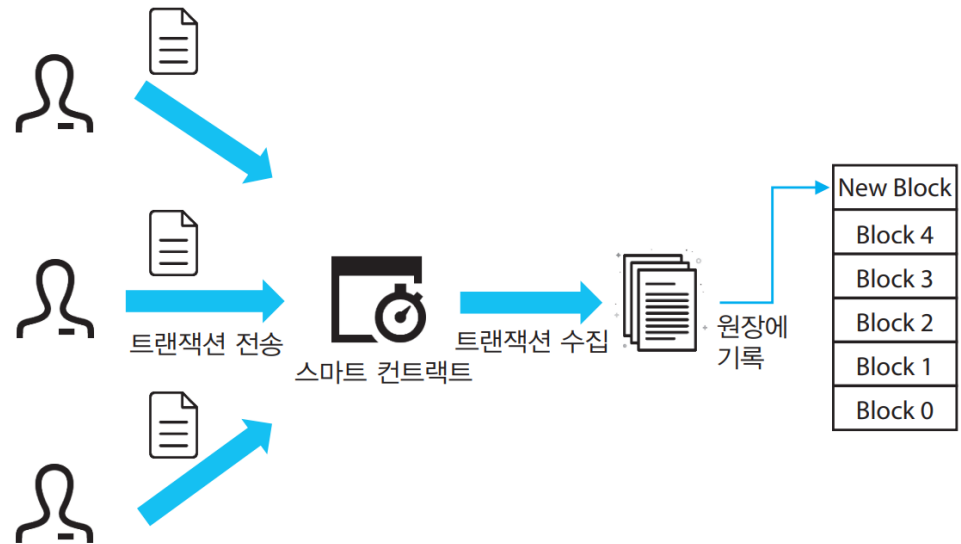
멀티체인

하드포크
소프트포크

WEB3
JSON
JSON-RPC

VM
JVM EVM CCENV

ONCHAIN
OFFCHAIN
SIDECHAIN



- 스마트 컨트랙트를 통한 분산원장 접근 예시

블록체인의 분류

프라이빗 블록체인 - 사전에 인증서발급

- 하이퍼레저 프로젝트
- R3 Corda
- 리플...

퍼블릭 블록체인 - 누구나 네트워크이 구성원

- 비트코인
- 이더리움
- 알트코인

하이브리드 블록체인

- 인터블록체인