

BLOCKCHAIN

Kumoh National Institute of Technology (kit)
School of Industrial Engineering
Tae Sung Kim, Ph.D.
tkim@kumoh.ac.kr



BLOCKCHAIN

CONTENTS

1

Introduction to Blockchain

2

Blockchain Technology

3

The Impact of the Blockchain

1. 블록체인 개론

(1) 블록체인 개념

Blockchain Concepts



Centralized



Decentralized

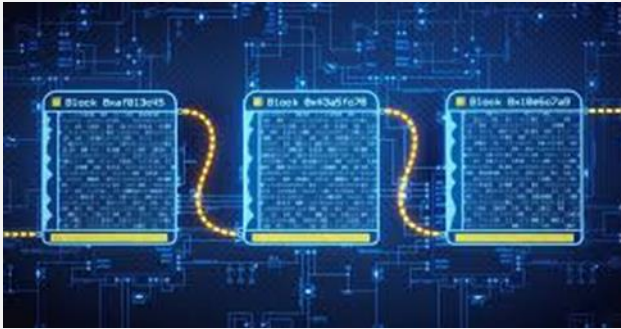


Distributed

Operation	Centralized	Decentralized	Distributed
Governance/ Business Model	Centrally Controlled	Community Controlled	Autonomous
Stability/Resilience	Unstable	Bounded Stability	Stable
Scalability	Large Throughput/ Small Number of Nodes	Small Throughput/Medium Number of Nodes	Infinite
Speed of Enterprise Development	Fast	Medium	Very Slow
Architecture Evolution/Diversity	Permissioned/Private	Hybrid	Permissionless/Public
Tokenization	No	Possibly	Yes
Trust Control	High Traditional/Low Algorithmic	Medium Traditional/ Medium Algorithmic	Low Traditional/High Algorithmic

1. 블록체인 개론

(2) 블록체인 정의



Blockchain is a type of distributed ledger in which value exchange transactions (in bitcoin or other token) are sequentially grouped into blocks. Each block is chained to the previous block and immutably recorded across a peer-to-peer network, using cryptographic trust and assurance mechanisms. Depending on the implementation, transactions can include programmable behavior.

블록 체인은 가치 교환 거래 (비트코인 또는 기타 토큰)가 순차적으로 블록으로 그룹화되는 일종의 분산 원장이다. 각 블록은 이전 블록에 연결되며 암호화 신뢰 및 보증 메커니즘을 사용하여 피어 투 피어 네트워크를 통해 영구적으로 기록된다. 구현에 따라 트랜잭션에는 프로그래밍 가능한 동작이 포함될 수 있다.

1. 블록체인 개론

(3) 블록체인 특성

블록체인이란, 거래 데이터를 단순히 기록만 하는 데이터베이스가 아니라
이용자 간 거래 정보를 주고받으며 정확성을 확인하고 위조하기 어려운 형태로
기록하는 기술

- 당사자 간의 거래 정보가 중앙 시스템을 경유하지 않고 정합성, 정확성을 가지고 직접 데이터베이스에 기입된다.
- 기입된 데이터는 위조 불능(완결성)의 성격을 가진다.(불가역성)
- 기입된 정보는 누구라도 어디에서라도 참조 가능하다.(고속 확인)
- 인터넷을 이용하면, 대규모 개발도 불필요하고 낮은 비용과 높은 보안성 그리고 지속적인 운용이 가능하다.
- 블록체인에는 어떤 정보라도 보낼 수 있다.
- 특정 조건을 충족시킨 경우 블록체인에 거래 정보를 기입하는 것도 가능하다.
(Smart Contract)

1. 블록체인 개론

(4) 4차 산업혁명 시대의 10가지 전략 기술들

Top 10 Strategic Technology Trends for 2018

Intelligent



AI Foundation

Intelligent Apps
and Analytics

Intelligent Things

Digital



Digital Twins

Cloud to the Edge

Conversational Platforms

Immersive Experience

Mesh



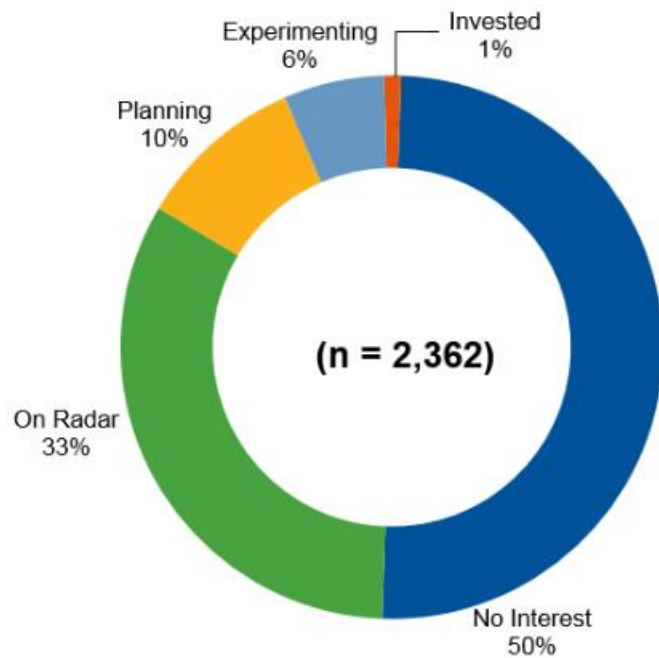
Blockchain

Event-Driven Model

Continuous Adaptive
Risk and Trust

1. 블록체인 개론

(5) Gartner's 2017 CIO Survey Focus on Blockchain



10% think of blockchain as a game changer

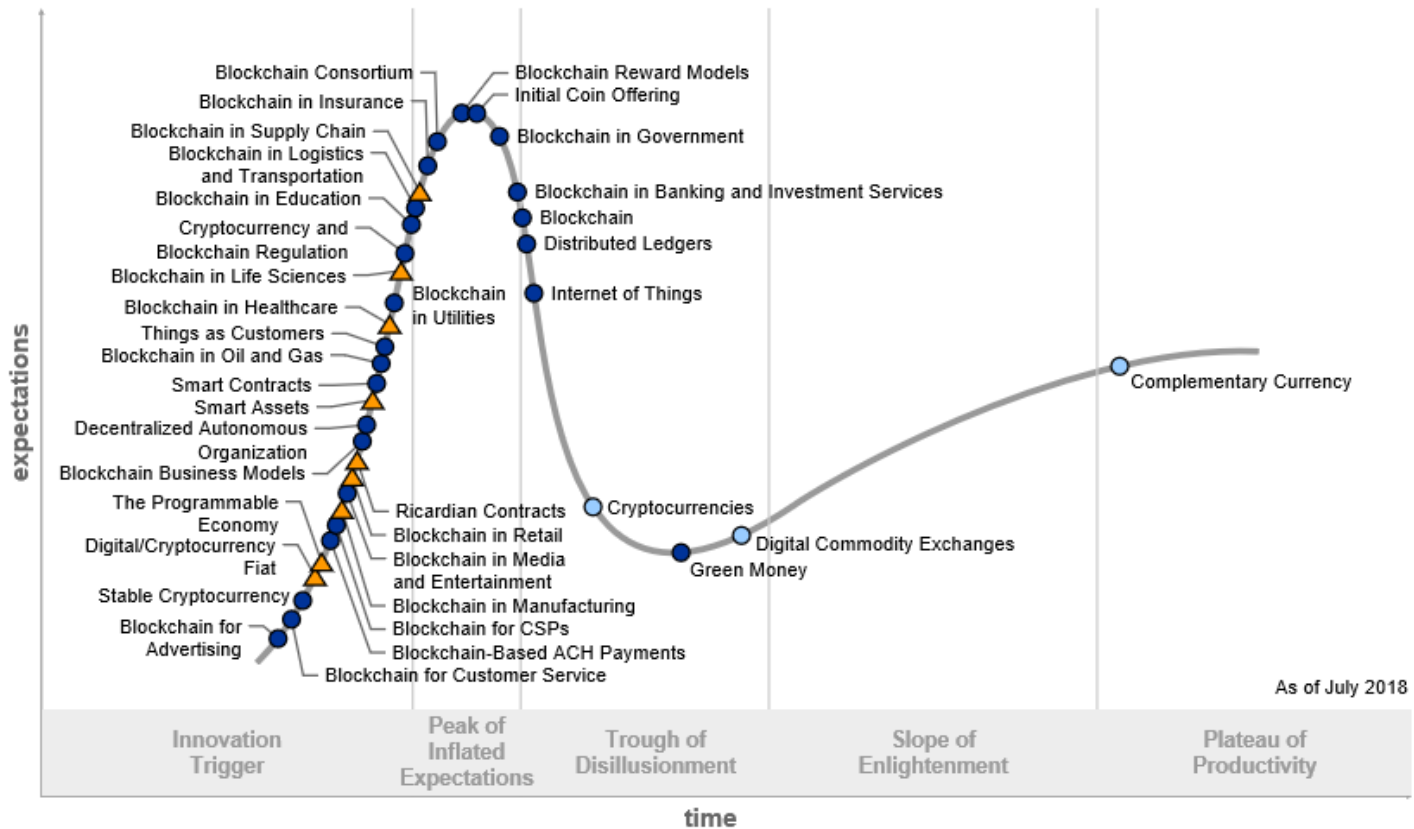
Question: In your opinion, which three of these technologies have the most potential to change your organization over the next five years?

Total Answers, Excludes don't know responses	2,331
Advanced Analytics	81%
Internet of Things (IoT)	48%
Digital Security	43%
Business Algorithms	40%
Machine Learning	22%
Virtual Customer Assistants	19%
Augmented Reality	13%
Blockchain	10%
Autonomous Vehicles	7%
Smart Robots	6%
Other	1%

1. 블록체인 개론

(6) 블록체인의 글로벌 동향

Interactive Hype Cycle



Plateau will be reached:

○ less than 2 years ● 2 to 5 years ● 5 to 10 years ▲ more than 10 years ⊗ obsolete before plateau

CONTENTS

1

Introduction to Blockchain

2

Blockchain Technology

3

The Impact of the Blockchain

2. 블록체인 기술

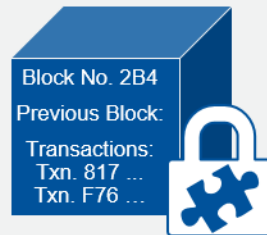
(1) How does blockchain work?

How Does Blockchain Work?

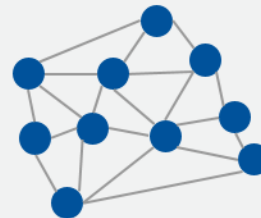
Network member
proposes new transaction



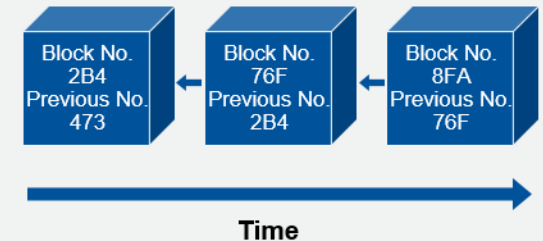
Nodes (computers) add the
proposed transaction
to other proposed
transactions into a block



Nodes use consensus
algorithms to confirm key
criteria and add the block
to the blockchain



Once the transaction is validated,
the confirmed block is appended
to the blockchain with the hash of
the previous blockchain



2. 블록체인 기술

(2) 블록체인 구분

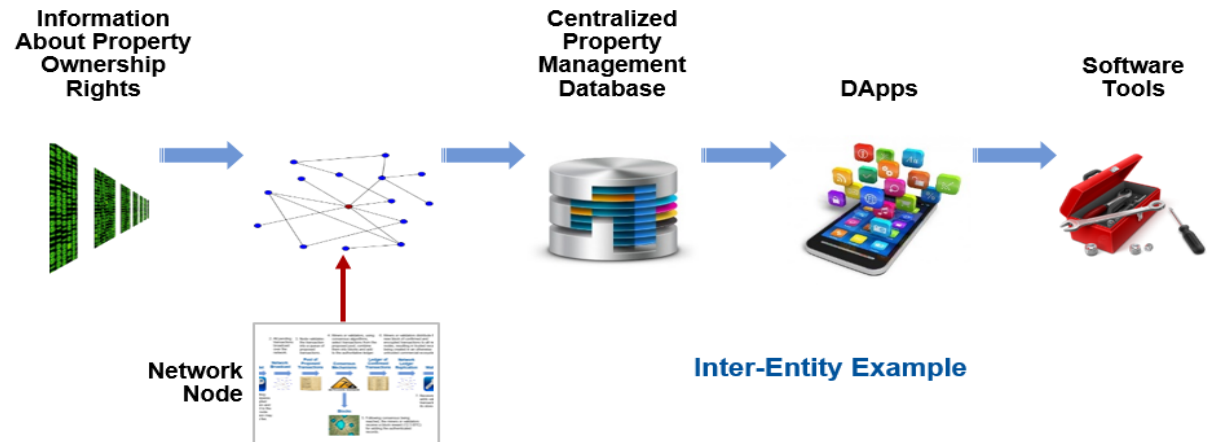
Private Blockchain

- 권한 관리의 유연성
- 다양한 프라이버시 확보
- 고도의 퍼포먼스 실현
- 경제적 리소스 공급이 중단되면 P2P Network 가동도 멈출 수 있음
- 특정 기업이나 단체에 의한 관리(금융기관 선호)

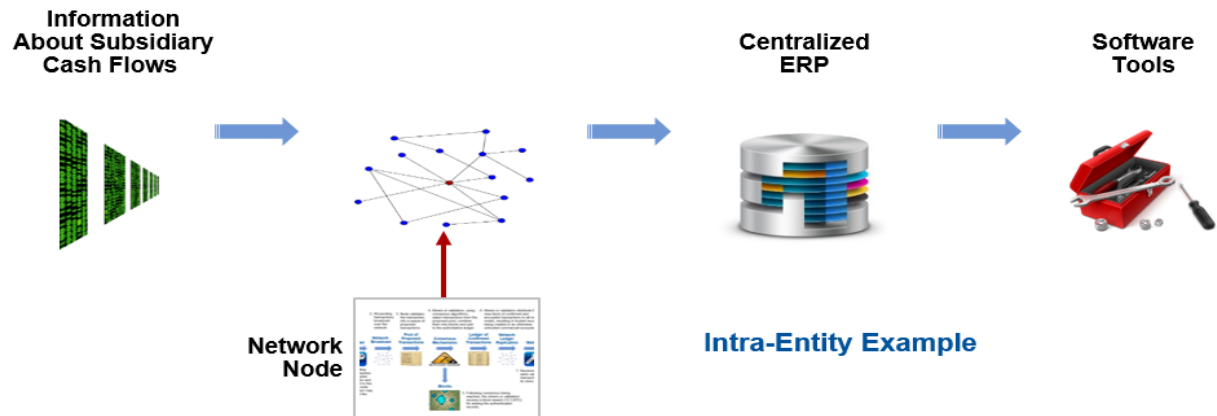
Public Blockchain

- 참가 노드의 50%이상 동의 없으면 기능 추가 불가
- 중단 없는 P2P Network
- 제3자에 대한 신용이 필요 없음(신용이 무수한 노드 운영자에게 분산, 익명화되어 보존된 가치에 대해 특정 제3자를 신용할 필요가 없음)

Private/Permissioned Solution Architectures



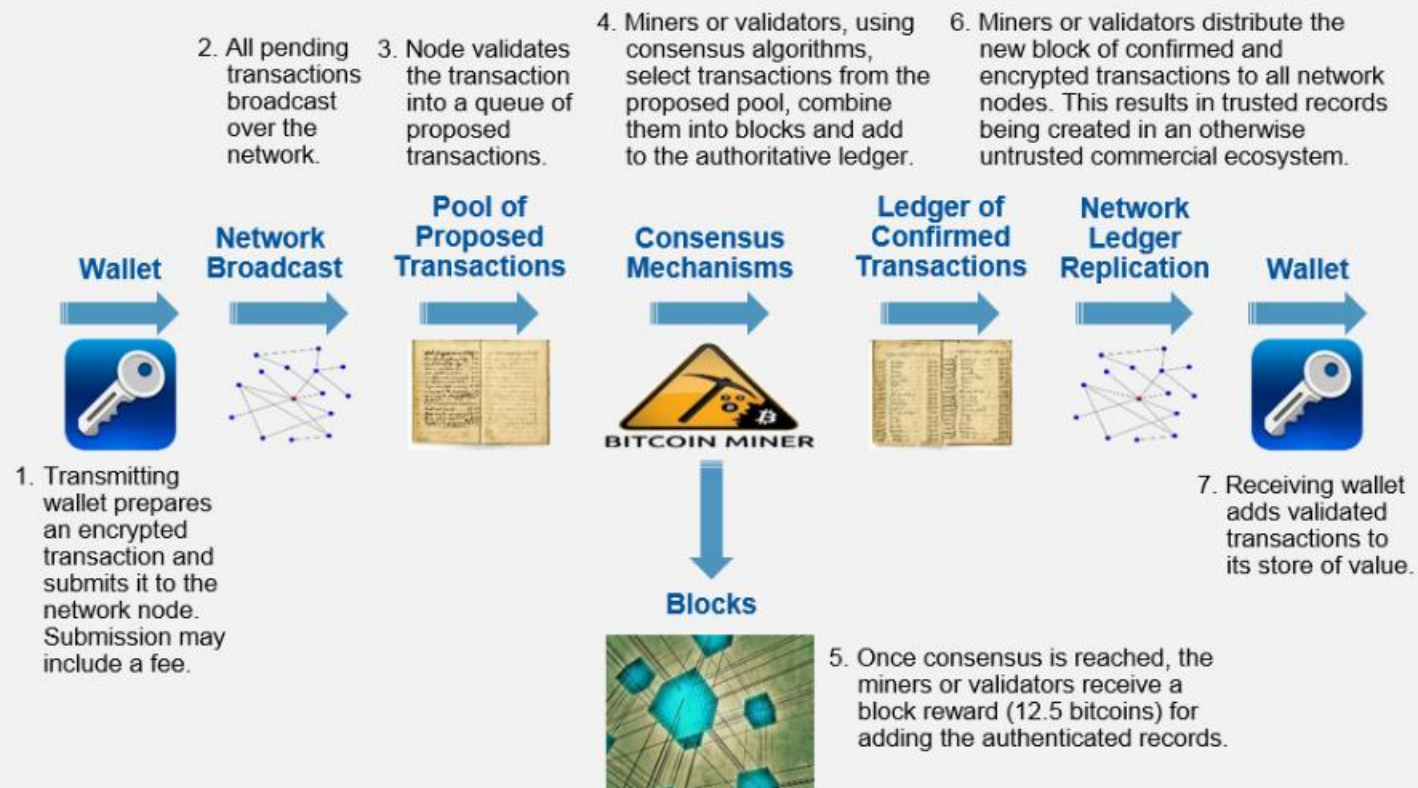
Public/Permissionless Solution Architectures



2. 블록체인 기술

(3) 블록체인 플랫폼 아키텍처

Blockchain Platform Architecture (Bitcoin Example)



2. 블록체인 기술

(4) Key Elements of Blockchain

The Blockchain Ledger

Shared and Distributed
Decentralized and Tokenized
Irrevocable Record
Algorithmic-Based Trust



Extended Characteristics













Dynamic Behavior
Controlled Updates
Controlled Access
Alternative Authentication
and Validation

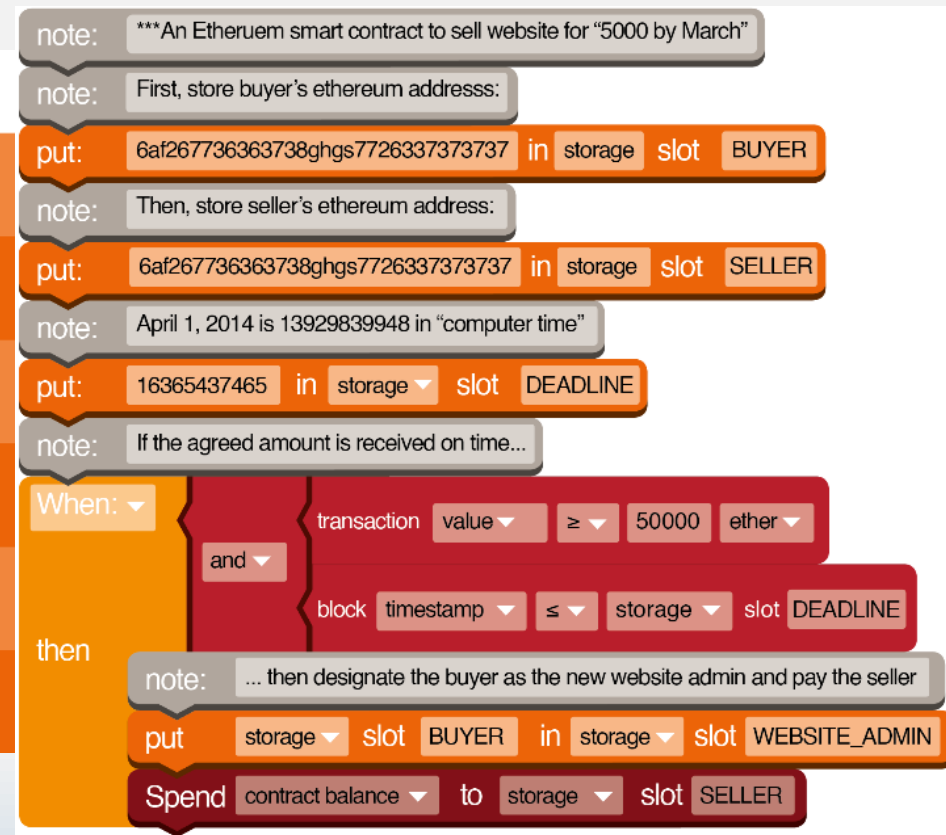
- Enterprise Ethereum Alliance
- Microsoft Coco Framework
- IBM Hyperledger Fabric
- Vertical Offerings: Banking, Healthcare, Supply Chain

2. 블록체인 기술

(5) Smart Contracts

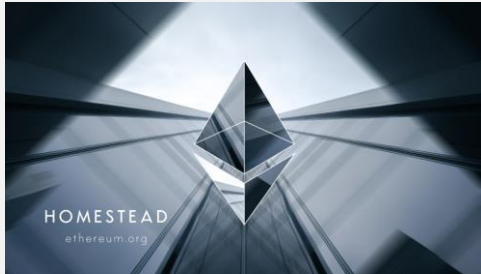
- 컨센서스 프로토콜은 계약 코드로 인해 발생하는 일련의 작업을 결정하는 데 중요함
- 신 재생 에너지부터 자동화 된 호텔 객실 예약에 이르기까지 모든 것을 P2P로 교환

Traditional contracts	Smart contracts
 1-3 Days	 Minutes
 Manual remittance	 Automatic remittance
 Escrow necessary	 Escrow may not be necessary
 Expensive	 Fraction of the cost
 Physical presence (wet signature)	 Virtual presence (digital signature)
 Lawyers necessary	 Lawyers may not be necessary



2. 블록체인 기술

(6) Ethereum Alliance



Ethereum은 다운타임, 검열, 사기 또는 제3자 간섭의 가능성없이 프로그램된대로 정확하게 실행되는 응용 프로그램인 스마트 계약(Smart Contracts)을 실행하는 분산 플랫폼이다.

- Ethereum은 임의의 계약을 쓸 수 있으며, 상태를 변경할 수 있는 튜링 완전한 프로그래밍 언어가 내장된 블록체인을 제공하는 것을 목적으로 하고 있다.
- 이용자는 몇줄의 코드 로직을 기입하는 것으로 우리가 상상할 수 없는 시스템을 만들 수 있다.

Solidity는 Smart Contract를 구현하기 위한 Contract 기반의 고급 프로그래밍 언어

```
pragma solidity ^0.4.0;

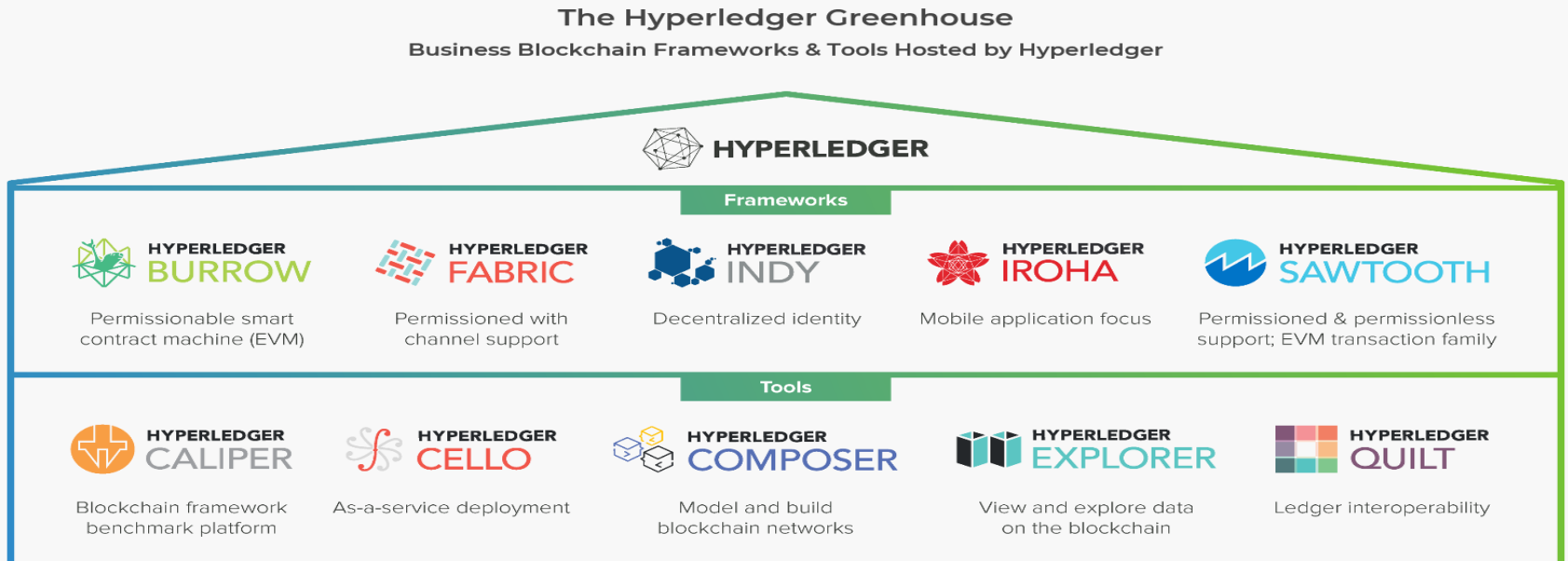
contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public constant returns (uint) {
        return storedData;
    }
}
```

2. 블록체인 기술

(7) Hyperledger - IBM



- Hyperledger는 산업 간 블록체인 기술을 발전시키기 위해 만들어진 오픈 소스
- 리눅스 파이낸싱, 금융, IoT, 공급망, 제조 및 기술 분야에 적용
- 비즈니스 블록체인 프레임 워크는 Hyperledger를 통해 호스팅
- Hyperledger는 분산 원장에 대한 산업 간 개방 표준의 중요한 기능을 제공

2. 블록체인 기술

(8) NEM(New Economy Movement)



- 다른 마이닝 기법 (Harvesting: 수확) : Proof of Importance(POI)
- 데이터베이스 서버가 포함된 어플리케이션 서버의 개념에 근거한 아키텍처 : 웹 기반의 아키텍처
- 거래의 비밀성, 신뢰성 그리고 부인 방지를 보장하기 위한 암호화 기술(타원 곡선 암호) 사용
- 짧은 블록(생성) 타임(기존 블록체인 블록 타임의 1/10분)
- 더 쉬운 트랜잭션 관리(하나의 마더 계정이 동시에 하나의 서브 계정으로서의 역할 수행)
- 노드의 자동 검증(Eigentrust++ 알고리즘이 도입되어 노드를 자동으로 관리하고 신뢰도의 관점에서 레이트를 붙인다. 그래서 신뢰 할 수 없는 노드는 거부되며 무시되는 사양으로 되어 있음: 평가 시스템 보유)

2. 블록체인 기술

(9) Benefits and Risks of Blockchain as a Data Management Platform

Blockchain as a Data Management Platform



CONTENTS

1

Introduction to Blockchain

2

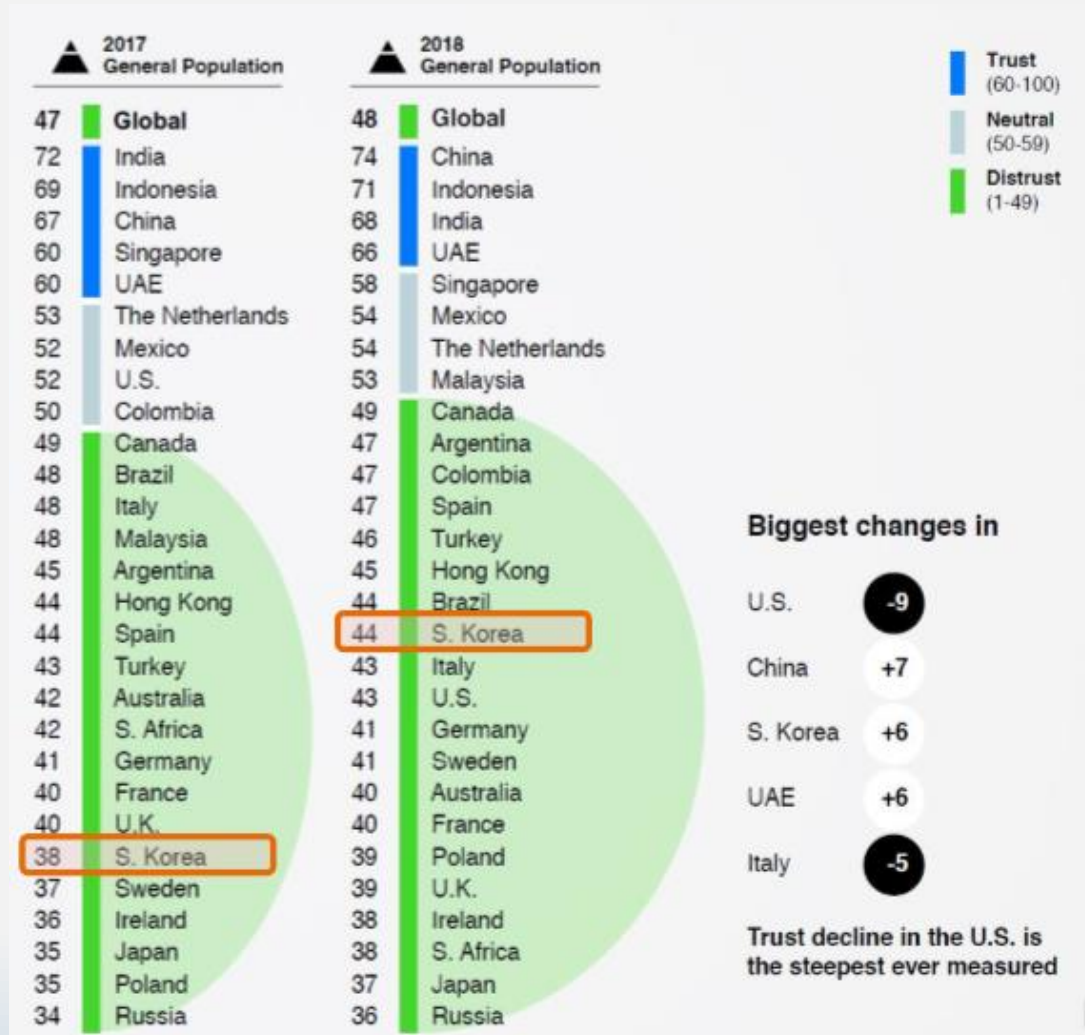
Blockchain Technology

3

The Impact of the Blockchain

3. 산업에 미치는 블록체인의 충격

(1) 대한민국의 신뢰도는?

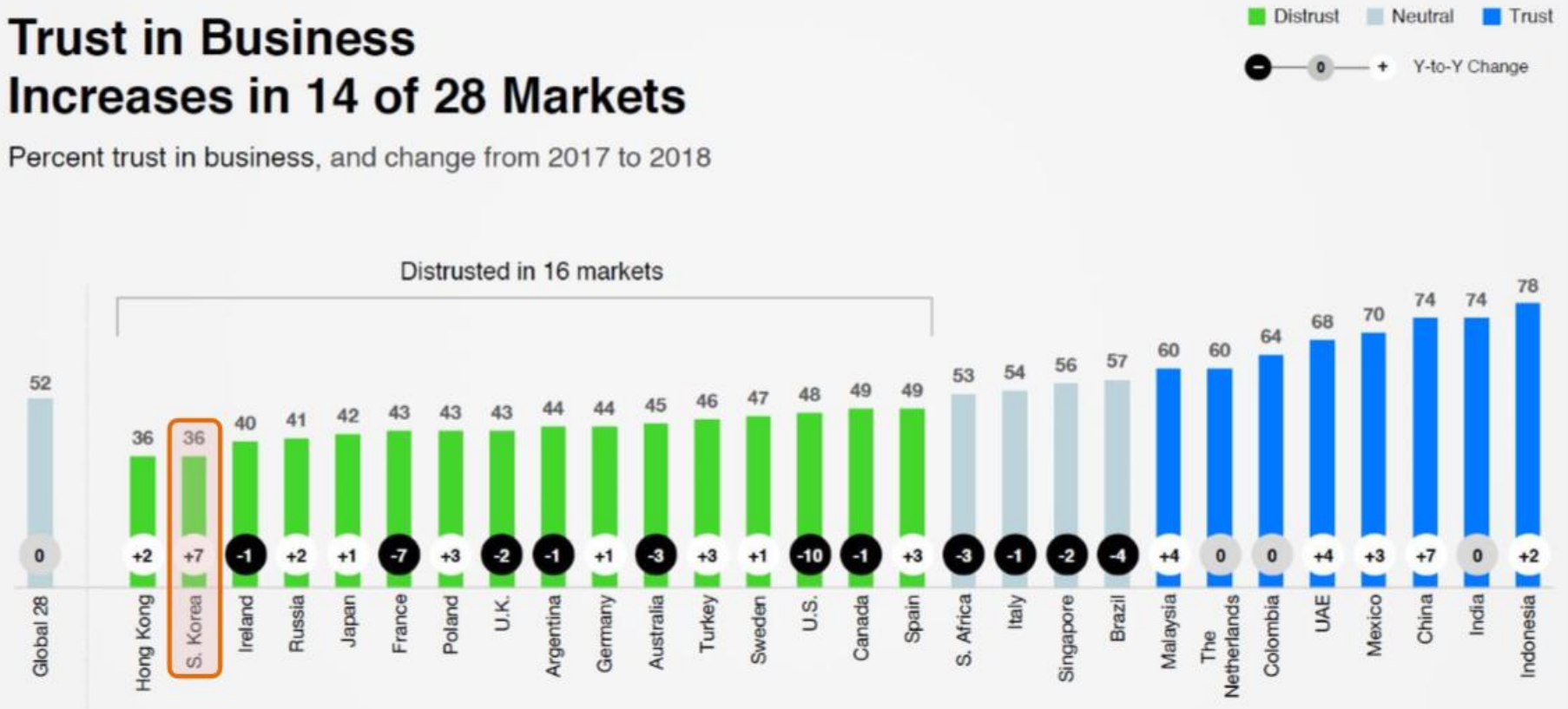


3. 산업에 미치는 블록체인의 충격

(2) 한국 기업의 신뢰도는?

Trust in Business Increases in 14 of 28 Markets

Percent trust in business, and change from 2017 to 2018



Source : www.edelman.com

3. 산업에 미치는 블록체인의 충격

(3) 신뢰 생태계(Trust-Ecosystem)의 중요성

신뢰를 전제하지 않은 생태계에서 많은 에너지와 비용이 낭비되고 있으며
신뢰 생태계가 구성 되었을 경우 해결 가능

1. 이해 당사자들간의 최적의 의사결정 가능

- 이해 당사자들의 최적의 의사결정을 가능케 하며 협력이 가능한 사회를 창출



구분	B 침묵	B 자백
A 침묵	A : 0.5년 B : 0.5년	A : 10년 B : 석방
A 자백	A : 석방 B : 10년	A : 5년 B : 5년



2. 검증 단계의 비용 절감

- 유통이력/문서검증 등 검증에 필요한 비용 절감



3. 국가 및 기업의 이미지 제고

- 소비자(국민)들의 기업(국가)에 대한 신뢰도 상승으로 매출(만족도) 상승



4. 4차 산업혁명시대의 신뢰생태계 인프라 제공

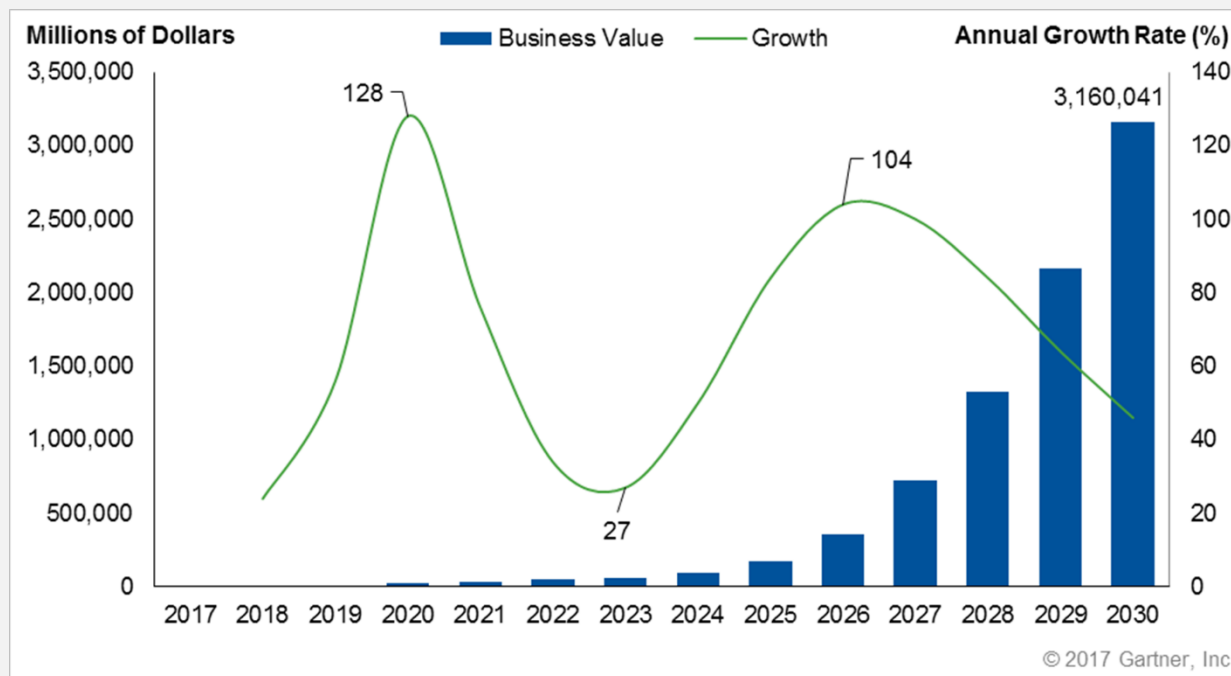
- 초연결/초지능화 시대에 새로운 가치를 창조하는 협업과 융합을 위한 신뢰의 인프라 제공



3. 산업에 미치는 블록체인의 충격

(4) Blockchain Business Value, Worldwide (2017~2030)

Blockchain의 사업적 부가가치는 2025년까지 \$176.6 billion(197조원)를 약간 넘게 될 것이며, 2030년에는 \$3.1 trillion(3,537조원)를 초과 할 것이다.



- 2022년까지 Blockchain 기술로 구축된 혁신적인 비즈니스 중 적어도 하나는 \$10 billion(11조원)의 가치가 있을 것임
- 2030년까지 전 세계 고객기반 비즈니스의 30%가 사물로 구성될 것이며, 이러한 비즈니스들은 Blockchain을 상업활동으로 수행하는 기초 기술로 사용될 것임

3. 산업에 미치는 블록체인의 충격

(5) 한국 정부의 대응

South Korea Budgets Nearly \$4.5B(5,000억원) for Blockchain, Emerging Tech

- 한국은 블록체인, 인공지능 및 기타 신기술 개발을 가속화하기 위해 2019년에 약 9억 달러(1조원)를 투자
- 플랫폼 경제를 개발하는 방법에 대한 부처 간 및 민간 부문 전문가 간의 논의가 있었으며, 장기적인 관점에서 투자를 계속할 4가지 프로젝트를 제시함
 - (1) 대용량 데이터 및 인공 지능을 위한 디지털 플랫폼 구축
 - (2) 블록체인 기술을 통한 데이터 트랜잭션 및 공유 경제 보호
 - (3) 수소 연료전지 공급망 설정
 - (4) 미래에 이러한 산업 분야의 자격을 갖춘 인력에 대한 수요를 충족시키기 위한 교육 프로그램 개발
- 정부는 민간 기업의 기술 경쟁력을 높이고 기업들이 블록체인 플랫폼 및 서비스를 테스트 할 수 있는 시설을 제공하기 위해 블록체인 기술 지원 센터를 설립하겠다는 의사를 발표함

3. 산업에 미치는 블록체인의 충격

(6) 블록체인의 활용을 기대할 수 있는 분야(1/2)

- 금융(은행, 자금이동, 유가증권 거래)
- 유통, 소매(물류, 디지털 콘텐츠 유통)
- 에스크로가 유효한 자금회수 위험의 회피 수단이 되는 거래(업무 위탁 거래, 무역, 부동산 매매, 중고품 매매)
- 예약을 동반한 각종 산업, 숙박시설, 교통기관, 의료기관, 학습시설 등
- 시간 이용, 사용료 등 사용량에 따라 요금을 부가하는 각종 산업이나 서비스(주차장, 렌터카, 임대 회의실, 대여 금고, 임대 창고, 디지털 콘텐츠, 노래방, 헬스클럽, 대중 목욕탕 등)
- 센서 네트워크, IoT 등을 활용한 자동 거래를 동반한 산업(가스, 수도, 전기, 통신, 교통, 농업, 축산업)
- 내용증명, 상업 등기, 부동산 등기(사실 사항 증명)

3. 산업에 미치는 블록체인의 충격

(6) 블록체인의 활용을 기대할 수 있는 분야(2/2)

신분증

(1) Bitnation



- 난민이나 국가로부터 공식 신분증을 받지 못한 개발도상국의 사람을 대상으로, 보통 국가가 제공하는 사회 보장 등의 기능을 블록체인에서 실현
- 가상화폐로 충전이 가능한 직불카드를 제공 할 수 있으며 신분증을 인증할 수 없어서 은행 계좌를 개설 할 수 없는 사람들을 위한 서비스 제공 가능

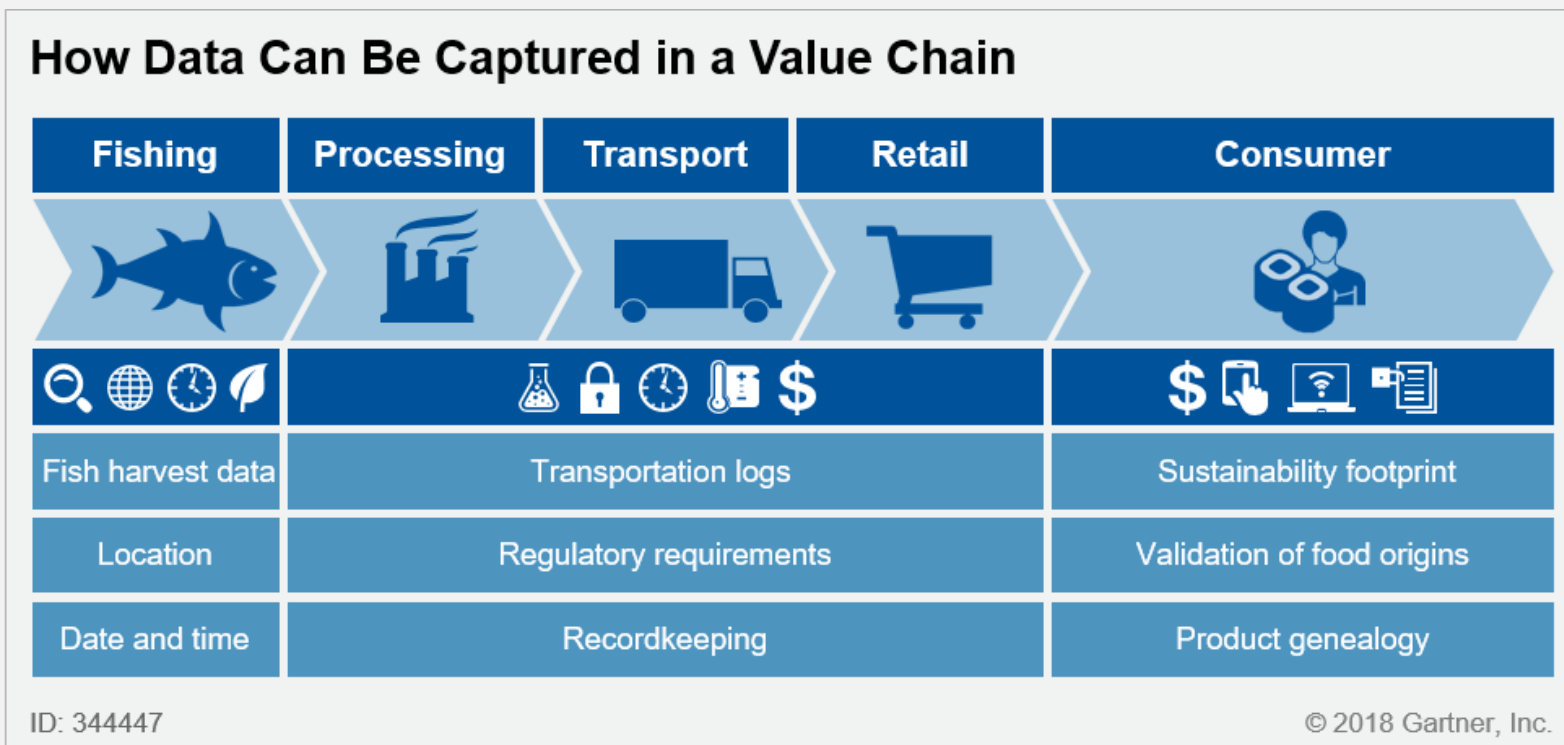
(2) Onename



- 블록체인상에 고유의 사용자 이름(ID)을 기록하여 온라인상의 아이덴티티 증명에 사용
- 각종 SNS 등과 자신의 블록체인 ID를 연결할 수 있으며, 정보 발신지의 증명이나 확인을 블록체인에서 실행 가능
- 블록체인의 ID를 이용하여 온라인상의 각종 서비스를 패스워드 없이 로그인할 수 있는 서비스 제공

3. 산업에 미치는 블록체인의 충격

(7) Information Captured by Blockchain in the Fish-to-Sushi Value Chain



3. 산업에 미치는 블록체인의 충격

(8) 블록체인 도입 사례(1/4)

‘후쿠시마 수산물’ 수입금지 패소… 한국식탁 오르나

WTO “협정 위반” 1심 판정

정부 “상소”… 방사능 검사는 계속
최종 패소해도 日과 수입분량 협상

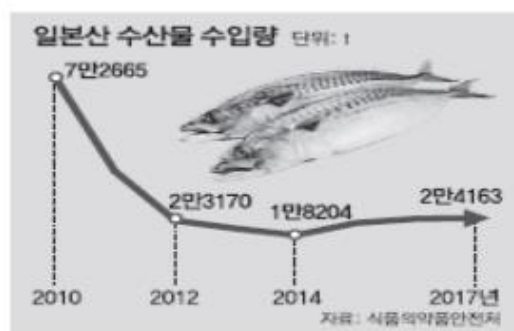
한국이 후쿠시마산 수산물 수입 금지 조치를 둘러싼 무역 분쟁 1심에서 일본에 패소했다. 한국 정부는 즉각 상소할 계획이지만 1심 판정이 번복될 가능성이 낮아 2011년 후쿠시마 원전 사고 이후 제한됐던 이 지역 수산물의 수입이 이르면 내년 말부터 재개될 것으로 전망된다.

다만 일본산 수산물 전체에 대한 정부의 방사능 검사는 계속돼 방사능에 오염된 수산물이 우리 식탁에 오를 가능성은 낮아 보인다.

23일 산업통상자원부와 해양수산부 등에 따르면 세계무역기구(WTO)는 22일(현지 시간) 한국 정부의 일본산 수산물 수입 규제 조치가 WTO 협정을 위반했다는 내용의 패널 판정 보고서를 공개했다.

보고서는 “일본산과 다른 나라 식품의 방사능 오염 위험이 모두 비슷하게 낮다. 일본산만 수입을 금지하고 ‘기타 방사성물질’(핵종)에 대한 추가 검사 조치를 하는 것은 차별이자 필요 이상의 무역 제한 조치”라고 밝혔다.

앞서 한국 정부는 2011년 3월 후쿠시마 원전 사고 직후 후쿠시마와 주변 8개 현의 일부 수산물 수입을 금지했다. 2013년에 8개 현 전체 수산물 금지로 확대했다. 이에 대해 일본 정부는



한일 수산물 무역 분쟁 현황

구분	내용
한국 수입 금지 조치	2011년 3월, 후쿠시마 등 일본 8개 현의 수산물 수입 금지
일본 제소 내용	2015년 5월, 한국의 전복 멸치 대구 고등어 등 28종 수산물 수입 금지 등에 대해 WTO 협정 위반 제소
1심 결과	한국 패소, 한국 정부 상소 예정

자료: 산업통상자원부 등

2015년 5월 “전복 멸치 대구 고등어 등 28종의 수산물 수입 금지와 기타 방사성물질 검사 증명서 요구는 WTO 협정 위반”이라며 제소했다.

정부는 이번 판정에 대해 즉각 상소할 방침이다. 상소는 1심 판정이 공개된 뒤 60일 안에 할 수 있으며 상소심(최종심) 판정은 상소 제기 후 3개월 내에 나온다.

하지만 그동안 WTO 1심 결과가 상소심에서 뒤집힌 전례가 거의 없어 한국이 최종 패소할 것이라는 전망이 조심스럽게 나온다. 9월경 상소심 결과가 나오면 한일 양국은 최대 15개월간 수입금지 해제 수준 등을 협의한다.

이런 절차를 고려하면 이르면 내년 말부터 후쿠시마산 수산물 수입이 재개될 가능성이 높다. 정부는 수입이 재개되더라도 당장 우리 식탁에 방사능 오염 수산물이 오를 가능성은 낮다고 보고 있다.

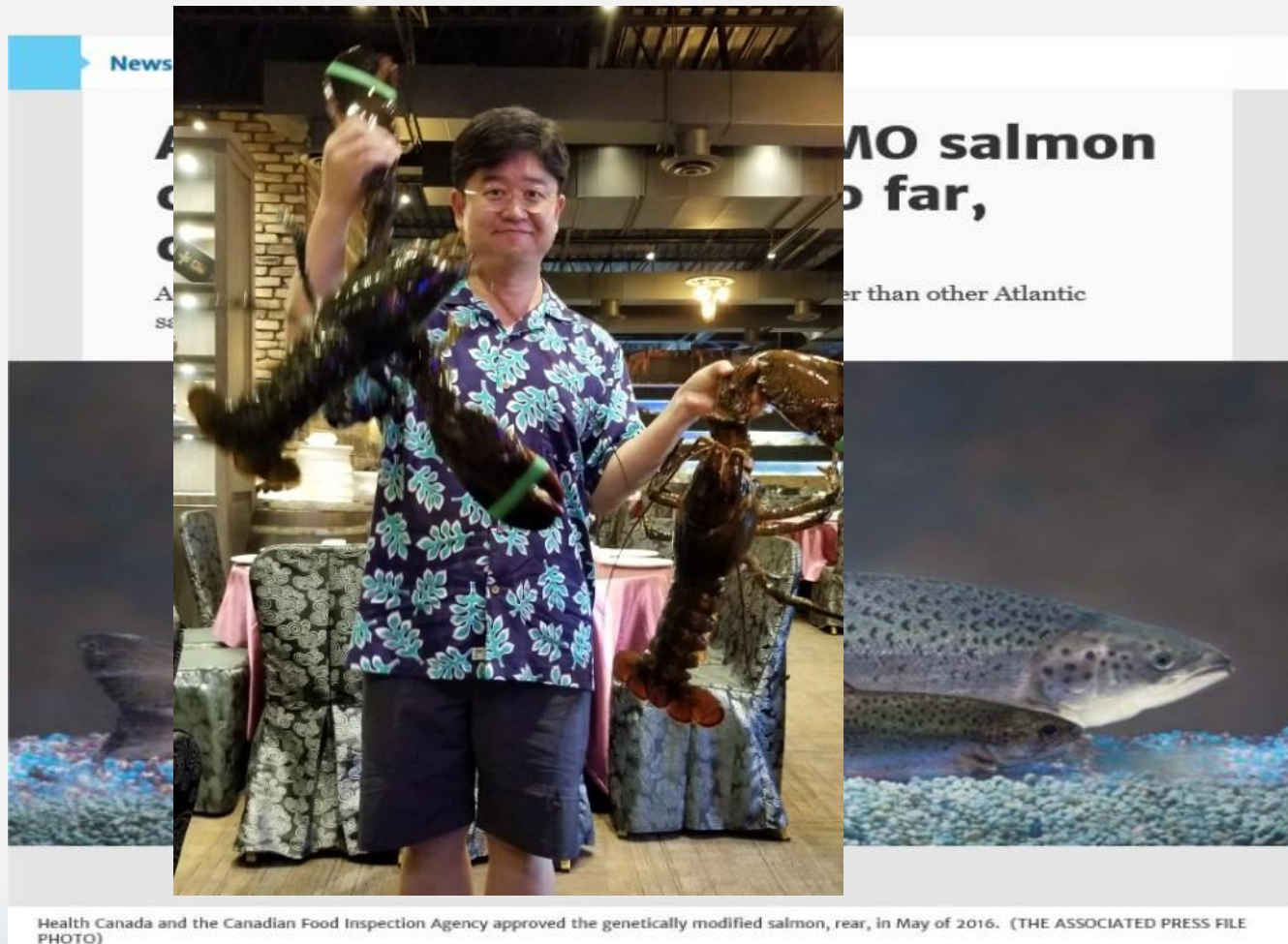
수입 금지 조치가 전면 해제되지는 않는 데다 일본산 수산물에 대한 방사능 전수조사는 계속 진행되기 때문이다. 현재 국내에 수입되는 일본산 수산물은 전량에 대해 1차적으로 식품의약품안전처의 방사능 검사를 거친다. 해수부 산하 국립수산물품질관리원의 원산지 확인 단속 때도 추가 방사능 검사가 실시된다. 식약처가 2013년 이후 수입된 일본산 수산물 총 10만 9300t에 대해 방사능 검사를 실시한 결과 방사능물질이 검출돼 반송된 물량은 총 5건, 20t이었다. 식약처 관계자는 “이번 분쟁에서 최종 패소한다고 해도 수입 단계의 방사능 전수조사는 계속 유지된다”며 “최악의 상황을 대비해 추가 대책도 마련할 예정”이라고 덧붙였다.

현재 한국 외에 중국이 후쿠시마 근처 10개 현, 대만이 5개 현의 모든 수산물 수입을 금지하고 있다. 하지만 기타 방사성물질 검사 증명서를 요구하는 국가는 한국이 유일하다. 미국은 일본이 지체적으로 출하를 제한한 품목만 수입을 금지하고 있다.

세종=최혜령 herstory@donga.com / 주애진 기자

3. 산업에 미치는 블록체인의 충격

(8) 블록체인 도입 사례(2/4)



3. 산업에 미치는 블록체인의 충격

(8) 블록체인 도입 사례(3/4)

부산시 소재 수산가공업 대상으로 원재료의 수입, 생산 및 유통에 이르는 과정을 4차 산업혁명 핵심 기술 중 하나인 블록체인을 기반으로 관리하여 선진화 및 투명화 가능성 검증 추진



[추진배경]

- 유통기한 변조 및 먹거리 사고 발생으로 불안감 고조
- 소비자가 직접 안전성을 확인할 수 있는 이력관리 필요

[추진목적]

- 제조일자 변조 가능성 차단 및 원재료에서 생산/가공/유통 전 과정에 대해 블록체인을 기반으로 이력 추적 검증

3. 산업에 미치는 블록체인의 충격

(8) 블록체인 도입 사례(4/4)

<div>이력조회</div> <div>Cello Blockchain</div>	<div>이력조회</div> <div>Cello Blockchain</div>
<div>어묵 제품의 원재료(연육) 수입부터 생산 및 유통과정에 대한 이력정보를 제공합니다.</div>	<div>어묵 제품의 원재료(연육) 수입부터 생산 및 유통과정에 대한 이력정보를 제공합니다.</div>
<div>기본정보</div> <div>이력정보</div>	<div>기본정보</div> <div>이력정보</div>
<div>2017-12-29</div> <div>UNI-PASS</div> <div>냉동연육 반입/수입신고</div> <div>수출국:VN (베트남) / 수입량:21000 KG</div> <div>2018-01-18</div> <div>UNI-PASS</div> <div>냉동연육 반입/수입신고</div> <div>수출국:VN (베트남) / 수입량:20500 KG</div> <div>2018-02-02 (국내반입 2017-12-29)</div> <div>냉동연육 입고</div> <div>수출국: VN(베트남) / 입고량:10000 KG</div> <div>2018-02-02 (국내반입 2018-01-18)</div> <div>냉동연육 입고</div> <div>수출국: VN(베트남) / 입고량:2000 KG</div> <div>2018-02-03</div> <div>200사각(특천) 가공/생산</div> <div>생산량:975 KG / 750 BOX</div>	<div>수출국:VN (베트남) / 수입량:20500 KG</div> <div>2018-02-02 (국내반입 2017-12-29)</div> <div>냉동연육 입고</div> <div>수출국: VN(베트남) / 입고량:10000 KG</div> <div>2018-02-02 (국내반입 2018-01-18)</div> <div>냉동연육 입고</div> <div>수출국: VN(베트남) / 입고량:2000 KG</div> <div>2018-02-03</div> <div>200사각(특천) 가공/생산</div> <div>생산량:975 KG / 750 BOX</div> <div>2018-02-05</div> <div>200사각(특천) 출고</div> <div>출고처:삼진어묵(부산역 광장점) / 12 BOX</div>

Source : Samsung SDS Cello Blockchain

3. 산업에 미치는 블록체인의 충격

(9) 블록체인 기반 가공식품 유통이력관리의 기대효과

블록체인의 불역성(Immutability)을 활용한 유통이력관리를 통해 소비자에게 안전한 먹거리를 제공하고 기업은 신뢰를 확보하며 산업 선진화를 통한 국가 경쟁력 향상을 기대할 수 있음



3. 산업에 미치는 블록체인의 충격

(10) Military applications of Blockchain(1/2)

American Defense Agency Eyes Blockchain for Secure Communications



해킹되지 않는 안전한
메시징 플랫폼으로
Hyperledger 도입 연구



- 거부된 통신 환경에서 지상에 있는 군대는 소속부대와 국방부에 안전하게 연락 할 수 있는 방법 확보에 주력



- "무기를 사용할 때마다 일반적으로 데이터 무결성이 매우 중요합니다 ..." "핵 명령 및 통제, 위성 명령 및 통제, 정보 무결성이 매우 중요합니다."- Timothy Booher , Blockchain 프로그램 관리자, DARPA

3. 산업에 미치는 블록체인의 충격

(10) Military applications of Blockchain(2/2)



- 나토 통신정보 기관은 현재 군사 물류, 조달 및 금융, 사물 인터넷(IoT) 및 군대에 관심있는 기타 응용과 관련된 Blockchain 기술 적용 분야의 제안을 평가중임.
- 이 제안은 NATO C4ISR 및 사이버 능력 요구사항을 지원하는 혁신적이고 최첨단 기술 솔루션을 가속화하기 위해 2016년 혁신과제의 일부로 제출되었음.



Q&A

Kumoh National Institute of Technology (kit)
School of Industrial Engineering
Tae Sung Kim, Ph.D.
tkim@kumoh.ac.kr



BLOCKCHAIN