

The background of the slide features a blurred image of a person in a dark suit holding a transparent blue globe. Surrounding the person and globe is a network of white lines connecting various circular icons. These icons include a globe with a cityscape, a globe with a bar chart, a globe with silhouettes of people, a globe with hands holding it, a globe with a laptop, a globe with a network of orange nodes, and a globe with a cityscape. The overall theme is global connectivity and technology.

블록체인의 현재와 미래

“블록체인 정보의 비대칭성을 극복하기 위한 강의”

장동인

AiBB Lab, 서울과학종합대학원 겸임교수

장 동 인(Don Chang)

010-5259-9509 / donchang0725@gmail.com



경력

- 현, AiBB Lab 대표(AI, Big Data, Blockchain)
- 현, 연세대 의료 블록체인 고위과정 주임교수
- 현, MediTrust CTO (의료블록체인)
- 현, Advisor of Edenchain, MyCreditChain, Linkchain, Funkey Pay, Tempo ICO, Futurepia
- 현, 서울과학종합대학원 빅데이터MBA 교수
- 현, 빅데이터 전문가 협의회 의장
- 국방과학연구소 빅데이터 PM
- 한국 테라데이타 부사장
- 미래읽기 컨설팅 대표
- Ernst & Young 컨설팅 본부장
- Deloitte consulting 전무(CRM부문 파트너)
- SAS Korea 부사장
- Siebel Korea 초대 이사장
- Oracle Korea 컨설팅 본부 이사
- Oracle HQ, Senior Principal Consultant
- Germany Amadeus, System Support Engineer
- American Airline Information Service, Consultant
- EDS, System Engineer
- VISA International, Programmer

학력

- 서울과학종합대학원, 경영학박사 졸업(Big Data)
- University of Southern California, 컴퓨터 공학 석사 졸업
- 서울 공대 원자핵 공학과 졸업
- 용산고등학교졸업

전문분야

- 블록체인과 reverse-ICO 전략
- 빅데이터 전략 및 활용
- AI (Deep Learning) 의 활용
- 영상빅데이터의 분석, 물체 인식, 추적
- 클라우드 컴퓨팅
- 고객 및 마케팅 전략

저서



AiBB Lab (Ai, Big Data, Blockchain)

- 블록체인 최고위 과정 세팅 및 강의
- AI, Big Data, Blockchain 기업 강의
- 블록체인 컨설팅 (기업의 Public blockchain, Private Blockchain 도입 전략)
- 블록체인 교육 (16시간 강의)
 - “블록체인 정보의 비대칭성을 극복하기 위한 강의”
- 블록체인 기업의 Advisor
- “블록체인” 인터넷 방송(Talk IT)
- 기업의 빅데이터 전략 컨설팅(내부 전문가 육성 방법론)
- 인재 영입

AiBB Lab 블록체인 16시간 강의 내용

1. 암호화폐와 블록체인

블록체인의 사상과 철학
탈중앙화
제2인터넷과 블록체인
블록체인과 암호화폐와의 관계
국내 ICO에 대한 규제 내용
국내 ICO의 성공사례
향후 ICO의 전망과 대응 방법

2. Blockchain 4.0을 향하여

분산원장과 블록체인
블록체인 기술(해시, 디지털서명, 머클트리, 헤더구조, 채굴
하드포크, 소프트포크, 세그윗
다양한 Consensus Algorithm
블록체인 1.0 (비트코인)의 기술과 문제점
블록체인 2.0 이더리움의 좋은 영향
이더리움의 퍼포먼스, 보안, 거버넌스, 개발환경, 채굴비용, 파이날리티
등 문제점
Blockchain 3.0이 이더리움의 문제점을 해결하는 접근 방법
분산원장의 개념을 구현하는 다양한 블록체인 소프트웨어
차세대 블록체인인 Blockchain 4.0을 향하여
블록체인 시대에 무엇을 할 것인가?

3. Blockchain Use Case 분석 및 주요 특징

블록체인을 도입해야 하는 분야
블록체인 use case 분석 템플릿(블록체인 플랫폼, 블록체인 서비스)
주요 암호화폐(코인/토큰) 해설
블록체인의 산업별 use case, 특징, 시사점
한국 정부의 블록체인 시범사업 현황

4. Startup을 위한 블록체인 ICO 전략

현재의 비즈니스 문제점을 해결하는 블록체인 철학
ICO 핵심 포인트
토큰 이코노미 설계방법
토큰 이코노미 사례 및 분석
ICO 단계 및 활동 내용
성공한 ICO 사례 및 시사점
퍼블릭 블록체인 성공 전략

5. 기업의 Reverse ICO 추진 전략 (퍼블릭 블록체인)

왜 Reverse ICO인가?
Reverse ICO의 성공 사례 및 시사점
Reverse ICO를 위한 준비할 내용
Reverse ICO의 법적인 이슈들
성공적인 Reverse ICO 추진 방법 및 전략

6. 기업의 프라이빗 블록체인 추진 전략

블록체인 도입 체크 리스트
블록체인을 도입해야 하는 경우와 도입 해서는 안되는 경우
기업에서 블록체인 서비스 도입 단계 및 의사결정 방안
블록체인 파일럿 프로젝트 주제 선택 및 추진 방안
기업간 업무 프로세스 설계 방법
블록체인 프로젝트 추진 방안

7. 주요 블록체인 플랫폼 및 소프트웨어 설명

Hyperledger Fabric,
R3 Corda
Ethereum

장 동 인(Don Chang)

Become a member

Medium

Sign in

Get started



Conston Taylor [Follow](#)

ICOs, ICO Evaluations, blockchain, cryptocurrency <https://www.linkedin.com/in/constontaylor/>
<https://icobench.com/u/conston-taylor>

Sep 8 · 2 min read

LINKCHAIN Advisor Announcement: Edenchain Advisor Don Chang joins LINKCHAIN as Technical Advisor.



LINKCHAIN

We are very excited to announce that Don Chang has joined the LINKCHAIN team as a Technical Adviser.

Don is also an Advisor for the Edenchain project, which completed its ICO in

지난 40년간의 기술의 변화

최근으로 들어 올수록 IT 기술의 변화가 비즈니스의 변화를 이끌고 있다.
그리고, 이러한 변화에는 Winner와 Looser 가 존재해 왔다.

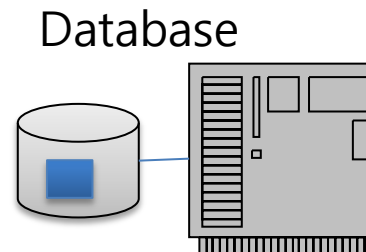
	시대의 키워드	Technology	Winner	Looser
1980'	Centralize Business	Mainframe	IBM	Univac, Unisys
1990'	Down Sizing	분산처리, Relational Database, TCP, Unix	Oracle, MS, Cisco	IBM
2000'	eBuziness	Internet, eCommerce, Intranet ERP, CRM, SCM	IBM, Oracle, SAP, MS	Old ERP
2010'	Digitizing Business	Mobile, Social, Big Data, Cloud, IoT	Google, Amazon, Apple, Salesforce	Existing Global IT vendor
2020'	Cognitive, Decentralized Business	AI, big data, blockchain	Google, Alibaba, Amazon, Ethereum	??

중앙집중

지방분산

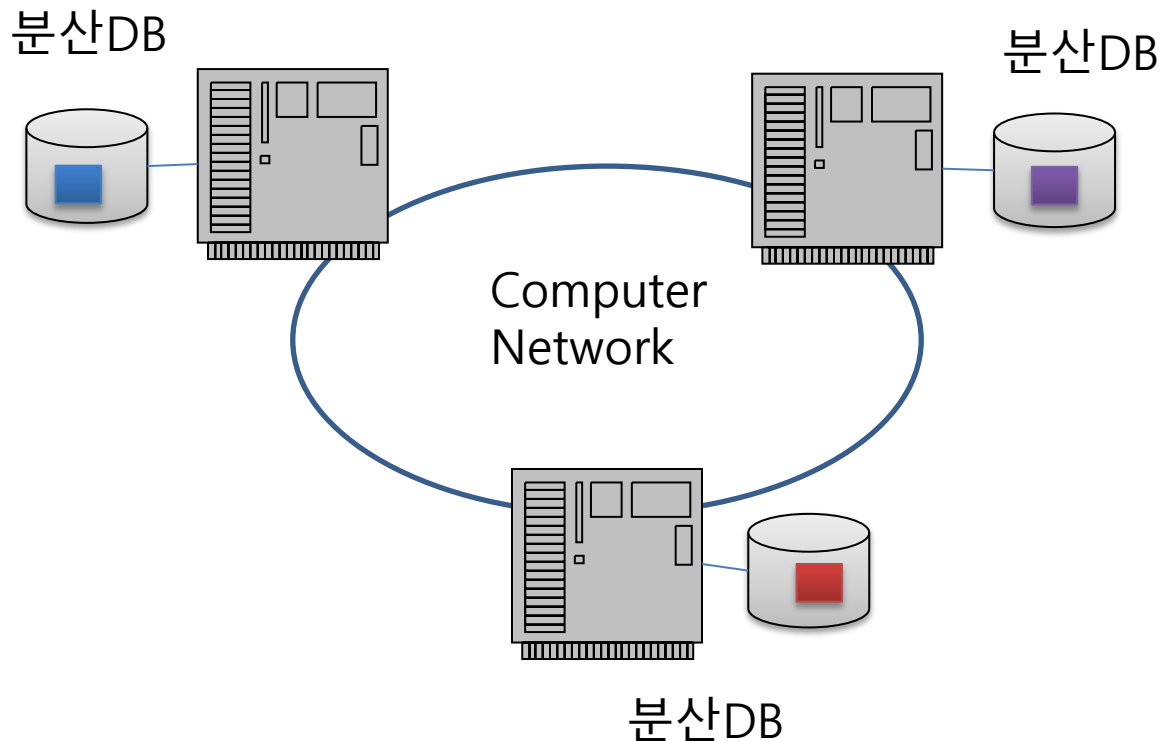
Database 란 무엇인가?

- 데이터베이스 = 많은 양의 데이터를 잘 보관하는 소프트웨어
- 데이터베이스는 컴퓨터 속에 있다
- 엑셀도 일종의 데이터베이스
- 트랜잭션 = 데이터베이스 기록 되는 내용 (내가 은행에 100만원 예금.)
- 오라클 이라는 회사.



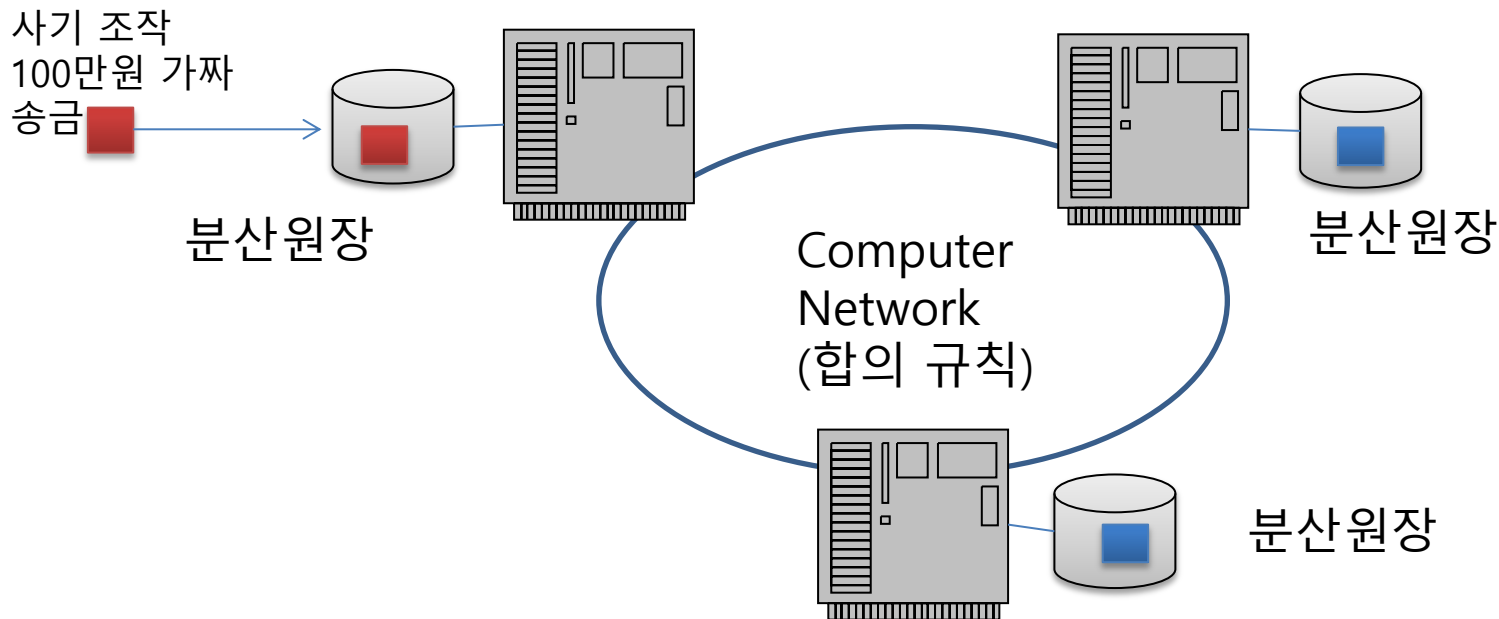
분산 데이터베이스(Distributed Database)

- 데이터가 여러 개의 노드(컴퓨터)에 분산되어 있는 것.
 - 데이터는 각 노드에 분산되어 있으며, 각 노드의 데이터는 서로 같지 않음
 - 사용자의 입장에서는 하나의 커다란 노드에 데이터가 합해있는 것과 같음
- 대용량, 속도, 안정성
- 탈중앙화와 아무 상관없음. (중앙화된 시스템)



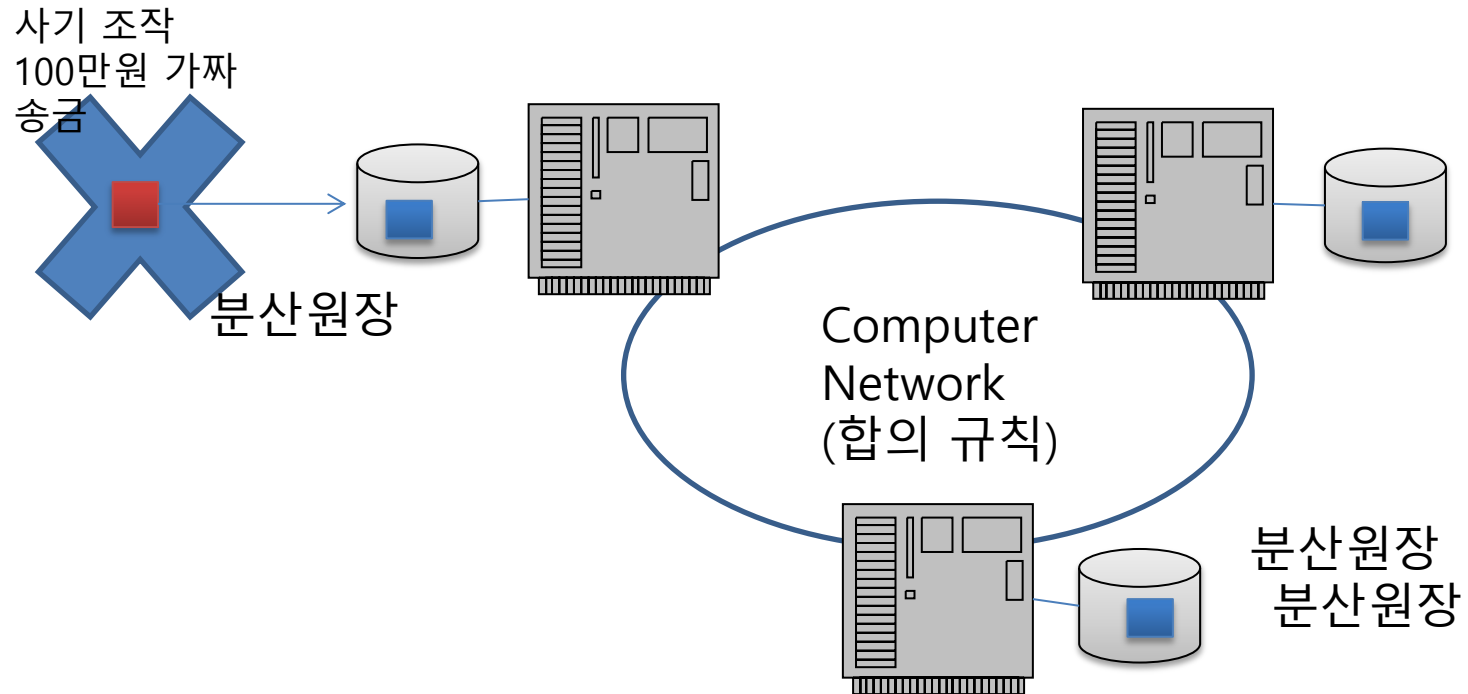
분산 원장(Distributed Ledger)

- 분산원장과 분산DB는 다름. (분산원장 \neq 분산DB)
- 데이터가 여러 개의 노드에 카피되어 있음. 각 노드에 있는 데이터는 서로 같음
 - 각 노드는 서로 신뢰하지 않음 (데이터를 악의적으로 고치려고/틀리게 하려는 노드가 있음을 인정)
 - 이러한 환경에서 각 노드에 있는 데이터를 같게 하기 위한 합의규칙(consensus rule) 필요 함.
- 분산원장은 중앙에 전체를 통제하는 기관이 없음 (탈중앙화)
 - 분산원장기술(DLT = Distributed Ledger Technology)



합의 규칙

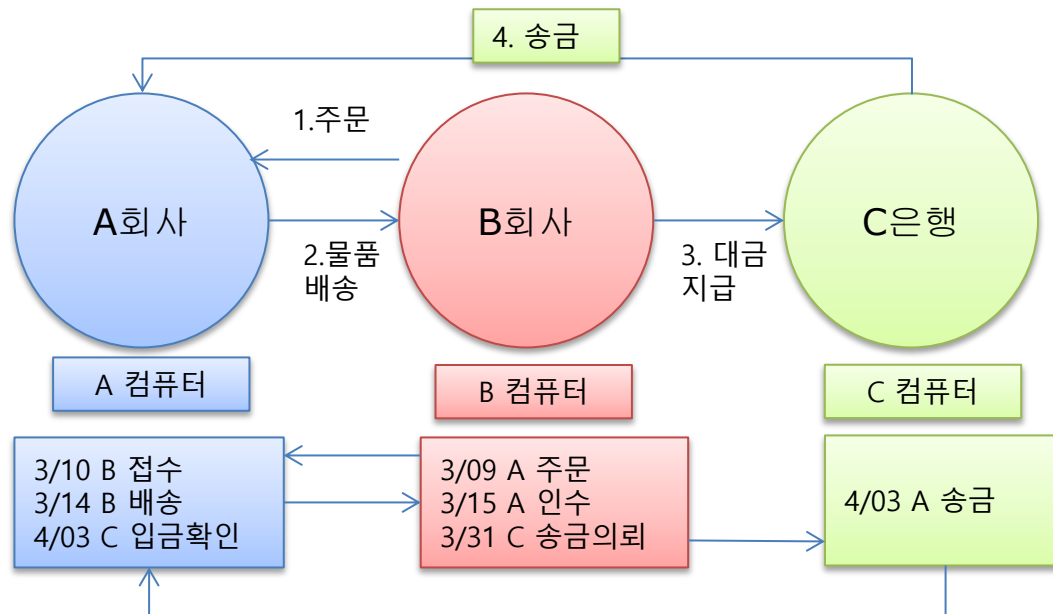
- 가장 쉬운 합의 규칙 = 투표를 해서 다수결로 합의 (51%룰)



- 이 방식은 비트코인, 이더리움에서 사용하고 있음
- 이를 POW(Proof of Work, 작업증명) 이라 함.

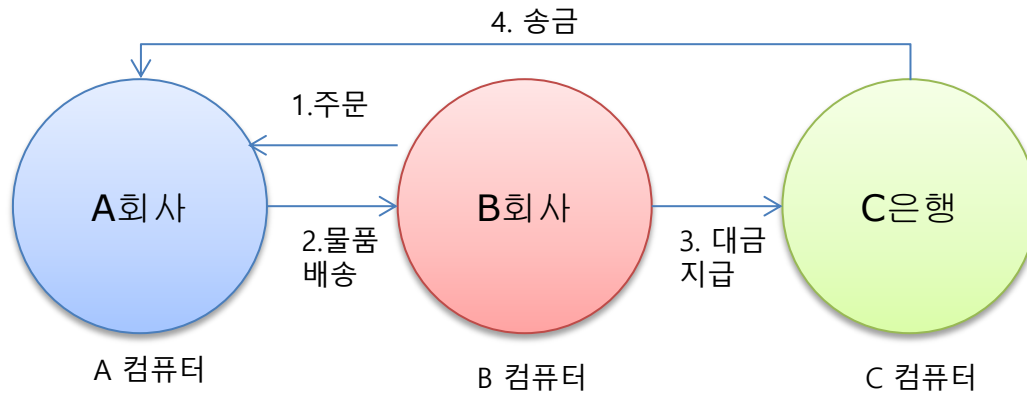
기존 중앙화된 Database

기존 회사간의 거래(트랜잭션)이 많은 분야
주문/지불/정산



- 주문했는데 물건 보내셨나요?
- 물건 보냈는데 받으셨나요?
- 물건에 하자가 있어 반송했는데 다시 보내주세요
- 아직 입금 안되었는데 송금 하셨나요?
- 은행에 송금의뢰 했는데 안 받으셨나요?
- 송금했는데 받으셨나요?
-
- 월말 틀린 것을 발견하기 위해서(원장 대사)

분산원장



- 주문했는데 물건 보내셨나요?
- 물건 보냈는데 받으셨나요?
- 물건에 하자가 있어 반송했는데 다시 보내주세요
- 아직 입금 안되었는데 송금하셨나요?
- 은행에 송금의뢰 했는데 안받으셨나요?
- 송금했는데 받으셨나요?
- ...
- 월말 원장 대사

분산원장

장점

- A,B,C 컨소시엄
- 국가간 거래는 더욱 복잡
- 복잡할 수록 더욱 이익이 크다
- A,B,C가 아주 이름없는 기업이나 은행이라도 OK
- 기업간 업무 프로세스가 정확하고 빨라진다

관세청 “해외 전자상거래 시범사업” (해외직구)

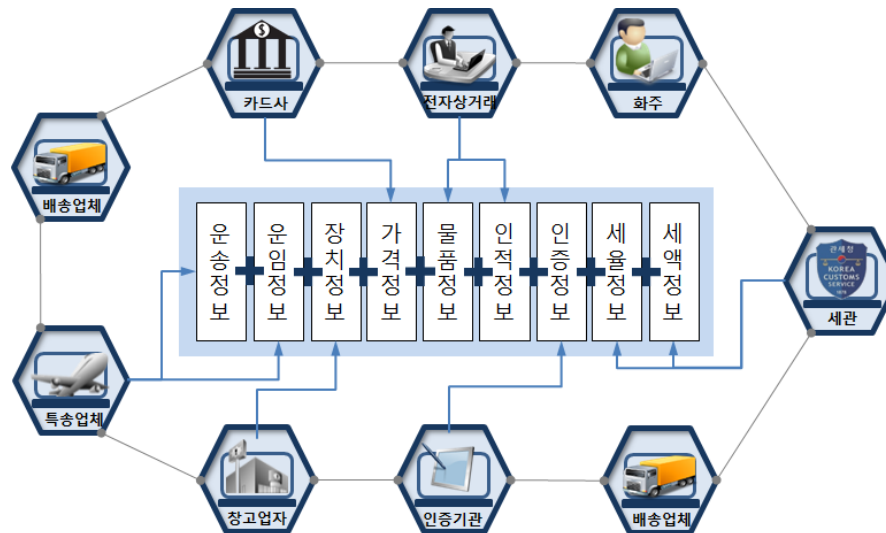
현재

신고서류: 수기작성



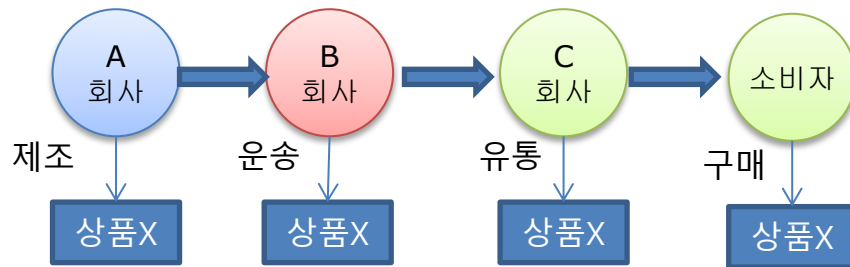
2018년 말

신고서류: 전자화. 내용의 불가역성 보증.



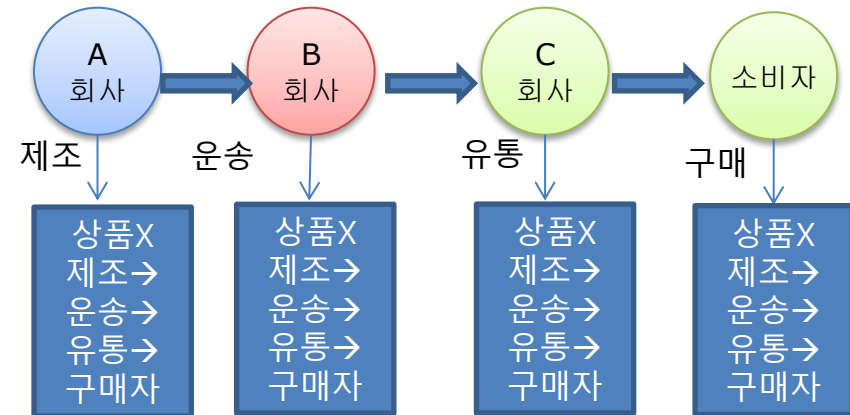
왜 분산원장이 혁신적인가?

현재 (각 기업내 기능중심)



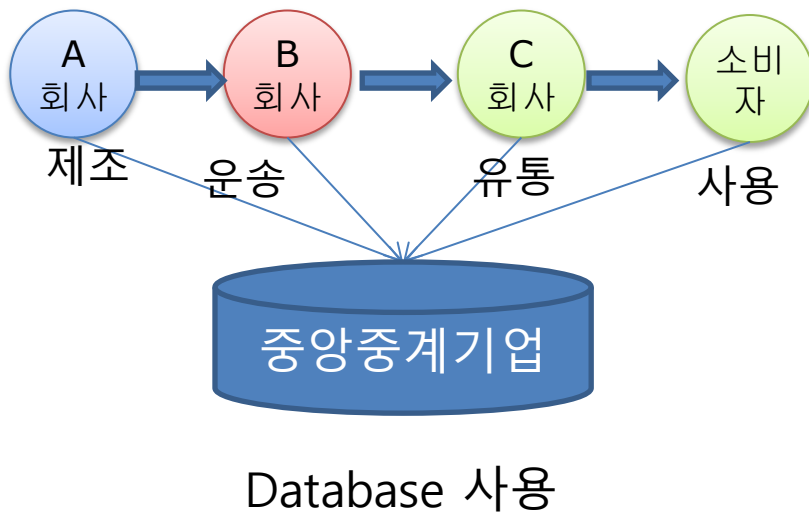
- 각 회사별로 시스템이 되어 있다.
- 상품(Asset)에 대한 거래(Transaction)가 일어날 경우
- 각 회사에서 처리.
- 당연히 각 회사와 회사간 차이가 날 수 밖에 없다.
- 상당 부분은 아직도 시스템과 종이서류를 들고 다닌다.
- 시스템과 상품과 차이가 난다.
- 시간, 비용 뿐 아니라...
- 진품인지 가짜인지 알 수 없고...
- 단계가 많아지면, 누가 만들었는지 추적 불가능..

분산원장 (기업간 프로세스 중심)



- 각 단위 상품별로 되어 있다.
- 상품(Asset)에 대한 거래(Transaction)가 일어날 경우
- 분산원장에 거래내용을 기록
- 차이가 날 수 없다
- 분산원장에 데이터를 기록하려면 무조건 디지털화 시켜야 함
- 시스템과 상품이 차이 나지 않는다
- 시간, 비용 감소는 기본...
- 당연히, 진품인지 가짜인지 알 수 있고...
- 아무리 단계가 많아져도, 누가 만들었고, 운송했고, 유통했는지 추적 가능..

만일 분산원장을 사용하지 않고 중앙에 중계기업을 만들면 어떤가?



- 당연히 가능하다... 그리고 합의규칙 필요 없다
- 분산원장의 장점을 다 사용할 수 있다. 다만 내용을 고칠 수도 있다.
- 그런데... 가입하는 기업의 수가 많아지면 당연히 중앙중계기업은 power는 커진다
- 수수료가 올라간다
- 서비스는 떨어진다. 비용/시간이 많이 든다
- 탈퇴하는 것도 쉽지 않다
- 기존의 대형 인터넷 기업과 같은 효과가 나타난다

- 사례: SWIFT 해외 송금 (swift.com)
 - ✓ 40년전 완성
 - ✓ 11,000 개의 전세계 금융기관 연결
 - ✓ 71억개의 트랜잭션
 - ✓ 송금시간 3일, 수수료 수만원
 - ✓ 수수료 = 송금은행 수수료, 중계은행수수료, 지급은행 수수료

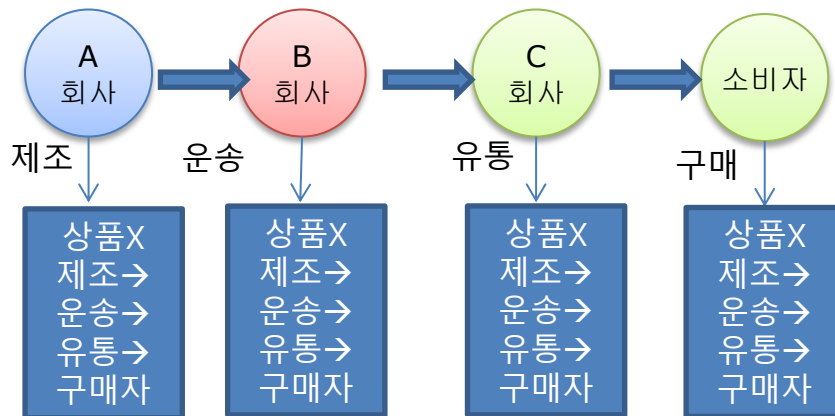
➔ SWIFT를 대체하려는 많은 분산원장 업체 등장

- ➔ 다른 산업에도 SWIFT와 같은 중앙 중계 기업이 있는 곳은 분산원장으로 대체 가능하기 좋은 분야!!
- ➔ Database를 사용하는 중앙중계기업과 분산원장 차이.

분산원장을 도입해야 하는 케이스와 중앙 DB를 만들어야 하는 케이스

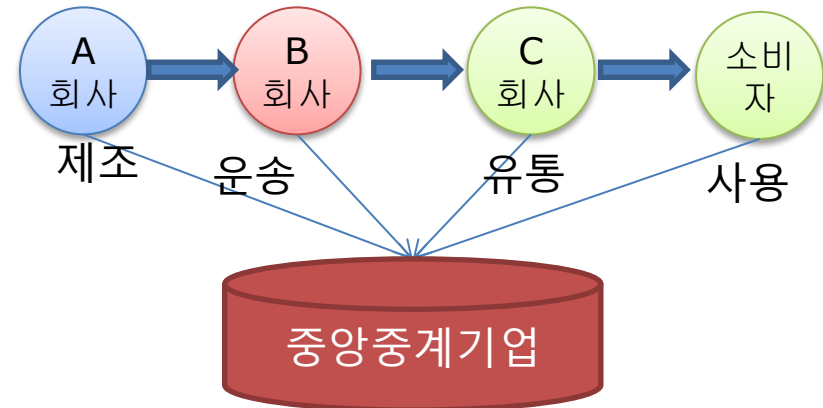
- 다음 두 가지 방식의 차이점을 분명히 이해하고 시작해야 함

분산원장 (기업간 프로세스 중심)



- 모든 구성기업이 분산원장 SW 사용해야
- 기존 시스템은 변경 필요 없음
- 모든 구성 기업이 합의에 의해서 가능

공통 데이터베이스 방식 (중앙중계기업/시스템)

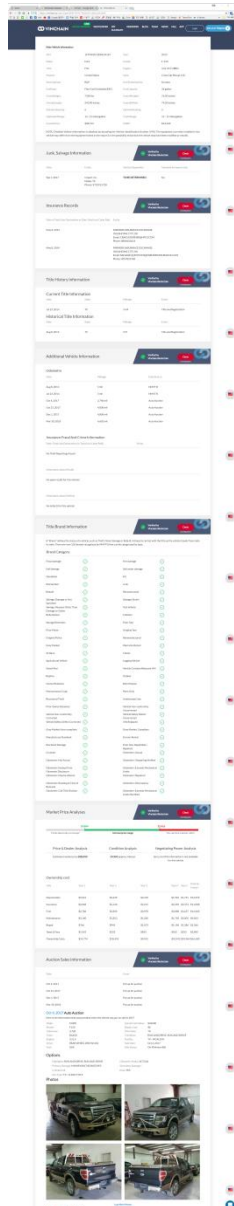


- 모든 구성기업이 필요 데이터를 제공해야
- 기존 시스템 변경 필요
- 오직 중앙 중계 기업을 위해서 시스템 구축 및 운영
- 중앙중계 기업이 힘이 있어야 가능

혁신적인 분산원장을 활용하기 위해서는?

- 1개의 기업에서 사용하지 말고 !!
- 관련된 여러 개의 기업이 Consortium을 맺어서
- 하나의 블록체인 회사를 만들어서(합작, 서비스대행...)
- 특정한 Asset을 (상품, 돈, 무형의 권한(저작권) ...)
- 제조, 구매, 운송, 판매 등의 트랜잭션을
- 디지털화 하고 (서류스캔, IoT 디바이스, 바코드, QR코드 활용 등)
- 분산원장에 기록한다.
- 목적: 진품확인, 원산지증명, 위치증명, 배송확인, 자동청구
- **블록체인을 적용하려면 해당 산업에 대한 깊은 지식과 경험이 필수!!**

예: vinchain.io



Vehicle History Report 2013 Ford F-150 - VIN 1FTFW1ET2DKE44167

Apr 4, 2018

Main Vehicle Information

VIN:	1FTFW1ET2DKE44167	Year:	2013
Make:	Ford	Model:	F-150
Trim:	FX4	Engine:	3.5L V6 TURBO
MakeIn:	United States	Style:	Crew Cab Pickup 4-Dr
SteeringType:	R&P	Anti BrakeSystem:	No data
FuelType:	Flex-Fuel (Unleaded/E85)	FuelCapacity:	36 gallon
GrossWeight:	7350 lbs	OverallHeight:	76.50 inches
OverallLength:	243.90 inches	OverallWidth:	79.20 inches
StandardSeating:	6	OptionalSeating:	5
HighwayMileage:	16 - 21 miles/gallon	CityMileage:	12 - 15 miles/gallon
InvoicePrice:	\$38,514	MSRP:	\$42,440

NOTE: Detailed Vehicle Information is obtained by decoding the Vehicle Identification Number (VIN). The equipment currently installed in the vehicle may differ from the equipment listed in the report (i.e. the possibility exists that the vehicle may have been modified or rebuilt).

출처: <https://vinchain.io/report/get/460f67803273bd8a433cbfa6ca95da89>

Vin = Vehicle Identification Number (차대번호)

Vin 번호를 기준으로 자동차에 대한 모든 정보
- history, 주인이력, 사진, 사고, 가격, 보험....

상당히 유망한 블록체인 기업: 현재 ICO 중

분산원장과 블록체인

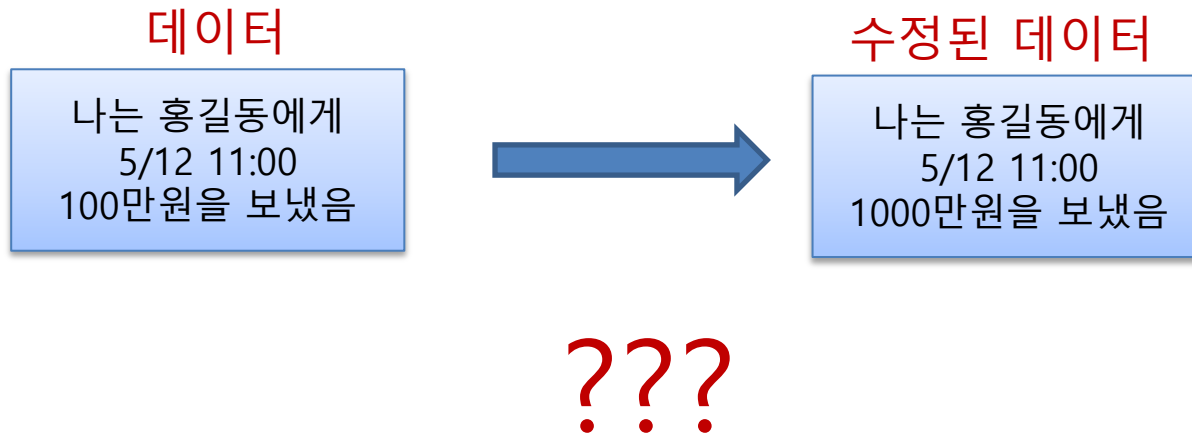
- 분산원장을 구현한 기술 중 **하나가** 블록체인
- 블록체인의 구조는 데이터 블록과 블록을 연결하는 해시(has). 데이터는 계속해서 해시에 의해서 연결됨
- 블록의 크기가 정해짐 (1~2M)
- 중앙 서버가 없으므로 누구나 블록을 만들 수 있게 하고, 먼저 해시 계산을 한 자(채굴자)에게 보상해주는 방식으로 시스템 운영
- 거대한 시스템을 갖춘 소수의 채굴자에 의해서 시스템 운영
- 블록체인 자체가 초기의 database 구조 형태를 갖고 있는 낡은 구조 (2008. Satoshi Nagamoto 논문 - 철학은 혁신적이거나, 방법은 낡은 방법
- 분산원장 개념을 좀 더 혁신적인 방식으로 구현하는 것이 진정한 블록체인!

혁신적인 분산원장을 활용하기 위해서는?

- 1개의 기업에서 사용하지 말고 !!
- 관련된 여러 개의 기업이 Consortium을 맺어서
- 하나의 블록체인 회사를 만들어서(합작, 서비스대행...)
- 특정한 Asset을 (상품, 돈, 무형의 권한(저작권) ...)
- 제조, 구매, 운송, 판매 등의 트랜잭션을
- 디지털화 하고 (서류스캔, IoT 디바이스, 바코드, QR코드 활용 등)
- 분산원장에 기록한다.
- 목적: 진품확인, 원산지증명, 위치증명, 배송확인, 자동청구
- **블록체인을 적용하려면 해당 산업에 대한 깊은 지식과 경험이 필수!!**

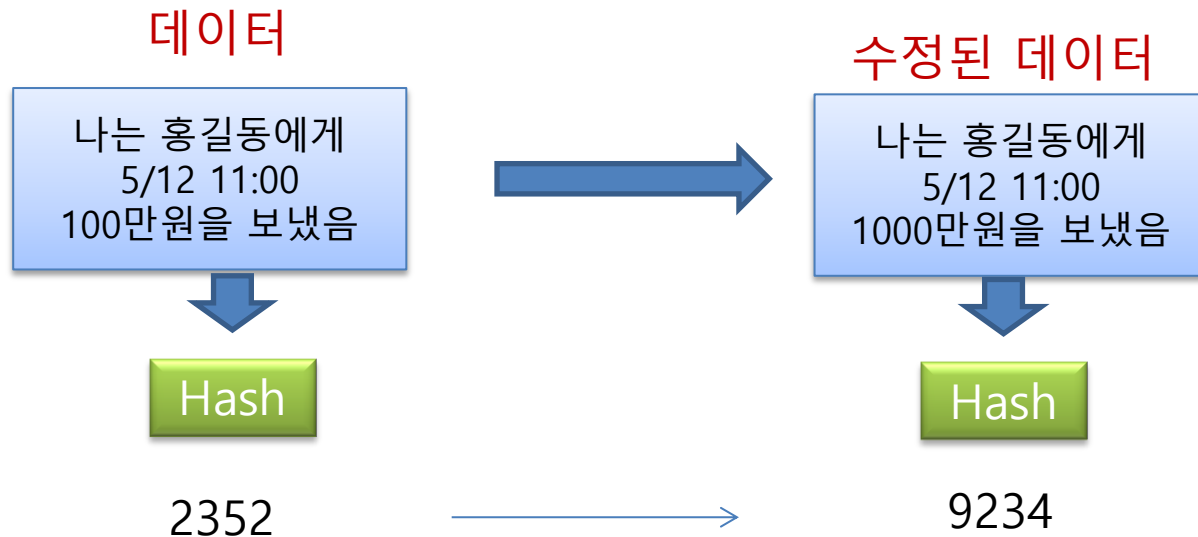
블록체인(Blockchain): 불가역성

- 어떻게 하면 데이터를 수정하지 못하게 할 수 있을까?
그리고 어떻게 하면 데이터를 수정하면 금방 알 수 있을까?
(수정불가)



해시(Hash)

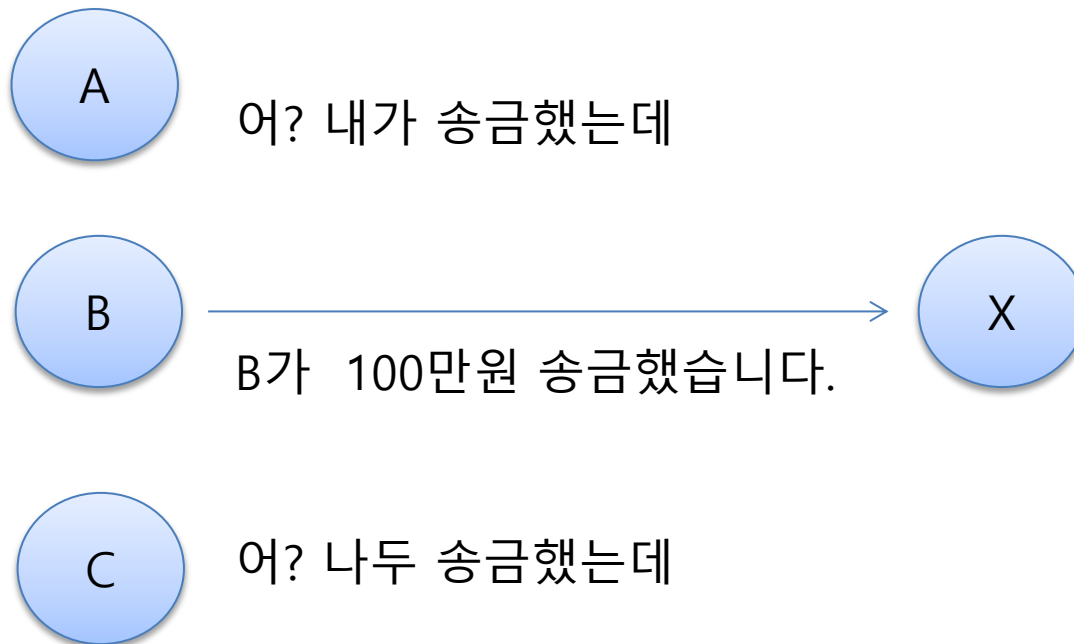
- 해시는 특정한 문자열에 특정한 값을 돌려주는 계산식(해시함수)
- 보내는 사람과 받는 사람이 같은 계산식(해시함수)를 사용한다
- 데이터를 보내는 사람은 데이터와 함께 해시결과를 보낸다
- 받은 사람은 받은 데이터를 계산식(해시함수)로 다시 계산한다
- 결과를 비교한다



값이 다르면 데이터가
수정되었음을 알 수 있음 !!

블록체인(Blockchain): 지불거부

- 어떻게 하면 내가 보낸 메시지(예: 송금의뢰)가 내가 보냈다고 증명할 수 있을까? 다른 사람이 보내고 안 보냈다고 할 때, 이를 어떻게 증명할 수 있을까?



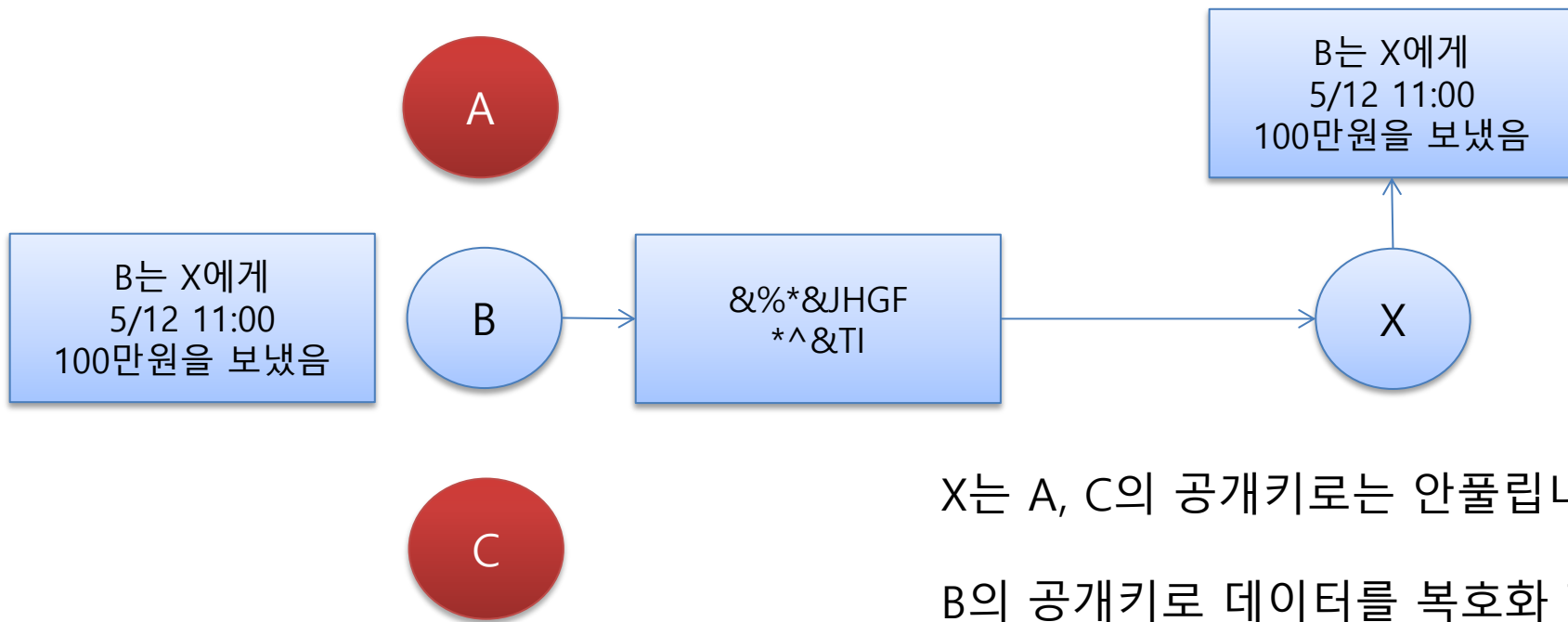
개인키(private key) + 공개키(public key)

- 암호화폐를 사면 각 사람에게 개인키와 공개키를 나누어 줍니다.
- 개인키와 공개키는 항상 쌍으로 존재합니다.
- 개인키로 암호한 데이터는 공개키로만 풀 수 있습니다.
- 반대로 공개키로 암호화한 데이터는 개인키로만 풀 수 있습니다.
- 모든 사람은 자신의 공개키를 공개합니다. 그래서 누구나 다 알 수 있죠.



블록체인(Blockchain): 지불거부

B는 메시지를 보낼 때, 자신만의 개인키로 암호화시키고, 보냅니다.
이것을 디지털 서명(Digital Signature)라고 합니다.

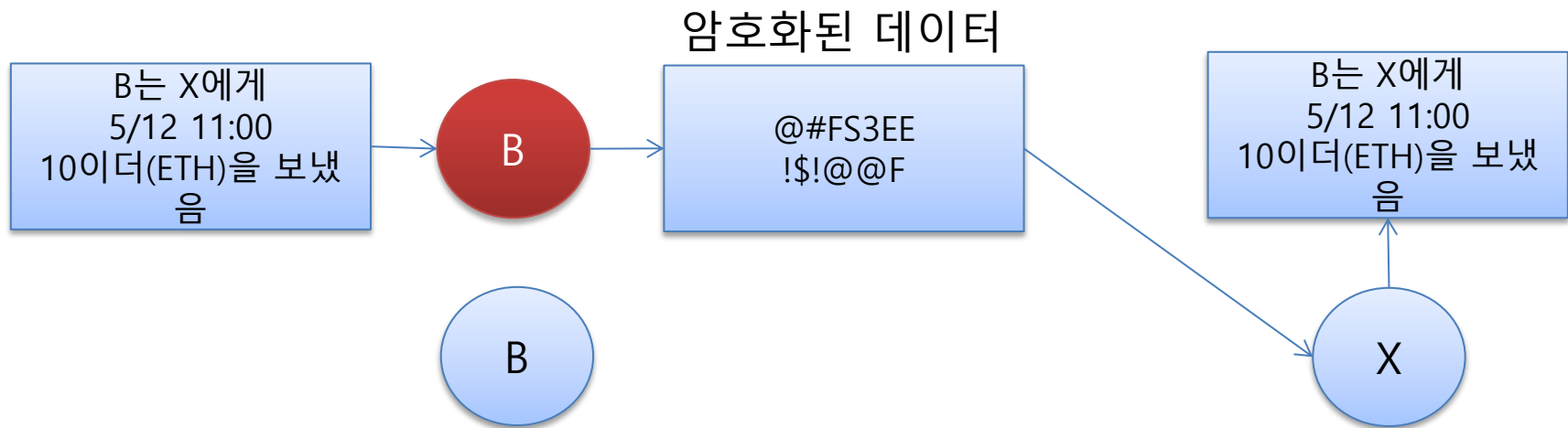


X는 A, C의 공개키로는 안풀립니다.

B의 공개키로 데이터를 복호화 합니다. 풀리죠. 그러니까 B가 보낸 것 맞습니다.

블록체인(Blockchain): 해킹

만일 A가 B의 개인키를 해킹해서 데이터를 X에게 보내면 어떻게 될까요?
그리고 자신의 주소(IP)를 B의 공개키로 바꿉니다.



- B의 공개키로 데이터를 복호화 합니다. 풀리죠. 그러니까 B가 보낸 것이라고 생각.
- 그러면, X는 B에게 10이더값 300만원을 보내겠죠... ππππ

해시(Hash)

- SHA256 Hash : 64 Hex character (256 bit)
 - 어떤 임의 text 로 64자 16진수(unique 64 Hex character)
 - 해시 알고리즘은 블록체인 플랫폼 별로 다름
- Blockchain header
 - header 6 개 필드 → SHA256 Hash 64자 16진수
- Mining (채굴)
 - 5개 필드 + nonce 를 계속 +1 시켜서 hash 처음 4~6 자리 값이 특별한 값(0000)이 될 때까지 hash 값을 계산

SHA256 Hash

Data:	이것은 블록체인의 시작입니다.
Hash:	c0bedd468233f95b5fa22e2cb4dc44c924739d61108f1280b0c923c56f870828

출처: <https://anders.com/blockchain/>

디지털 서명(digital signature)

- 디지털 서명(digital signature) – 특정인이 그 내용을 보냈음을 객관적으로 밝히는 것.
 - <https://anders.com/blockchain/public-private-keys/keys.html>
 - 개인키(private key)와 공개키(public key)
 - 개인키(private key)와 공개키(public key) (개인키로 공개키를 만듦. 공개키로 개인키는 못 만듦)
 - 암호화폐를 사거나 팔 때, 반드시 개인키와 공개키를 줌
 - 공개키는 일명 주소. (보통 비트코인 주소, 이더리움 주소)
 - 주소는 공개키이므로 남에게 보여줄 수 있다.
 - 그러나.... 개인키는 절대, 절대, 절대 주면 안된다.
 - 개인키는 공개키만 있으면 만들 수 있으나, 개인키는 절대로 못 만든다.
 - 개인키를 잃어버리면, 끝!! (어떤 방법으로든 복구할 수 없음!!)

Public / Private Key Pairs

Private Key

22111553667154668763649197166111426701393325092708151748791879328870986743961

Random

Public Key

04db102df8140a15daacf090366930ad1a66fc1a95ef43d4eaa01a32b9095fb29ecf85470d50314157919d26d25a5903c7154fa9f67cf2cfdb67ea08ca45401f

디지털 서명(digital signature)

- 디지털 서명(digital signature) :
 - 개인키로 text를 암호화 해서 보낸다.
 - (개인키는 아무도 모른다. 본인만 안다)

Signatures

Sign Verify

Message

Text → 내일 12시에 여의도역 1번 출구에서 만나자

Private Key

개인키 → 22111553667154668763649197166111426701393325092708151748791879328870986743961

Sign

Message Signature

암호화 Text → 30440220380d5f081a9ae60ba3631f0ace95379384f1da31ca9300d285d2a80bcfb7dfdf022020f2fbfcf08ad7539656d92b074175f05141c96f3aedd8b06348aa

디지털 서명(digital signature)

- 디지털 서명(digital signature)
 - 보낸 암호된 Text를 내 공개키로 복호화
 - 성공하면 내가 보냈다는 것을 증명 = digital signature

복호화
Text

→

Signatures

Sign Verify

Message

내일 12시에 여의도역 1번 출구에서 만나자

Public Key

04db102df8140a15daacf090366930ad1a66fc1a95ef43d4eaa01a32b9095fb29ecffe85470d50314157919d26d25a5903c7154fa9f67cf2cfdb67ea08ca45401f

Signature

30440220380d5f081a9ae60ba3631f0ace95379384f1da31ca9300d285d2a80bcfb7dfdf022020f2fbfcf08ad7539656d92b074175f05141c96f3aedd8b06348aa

Verify

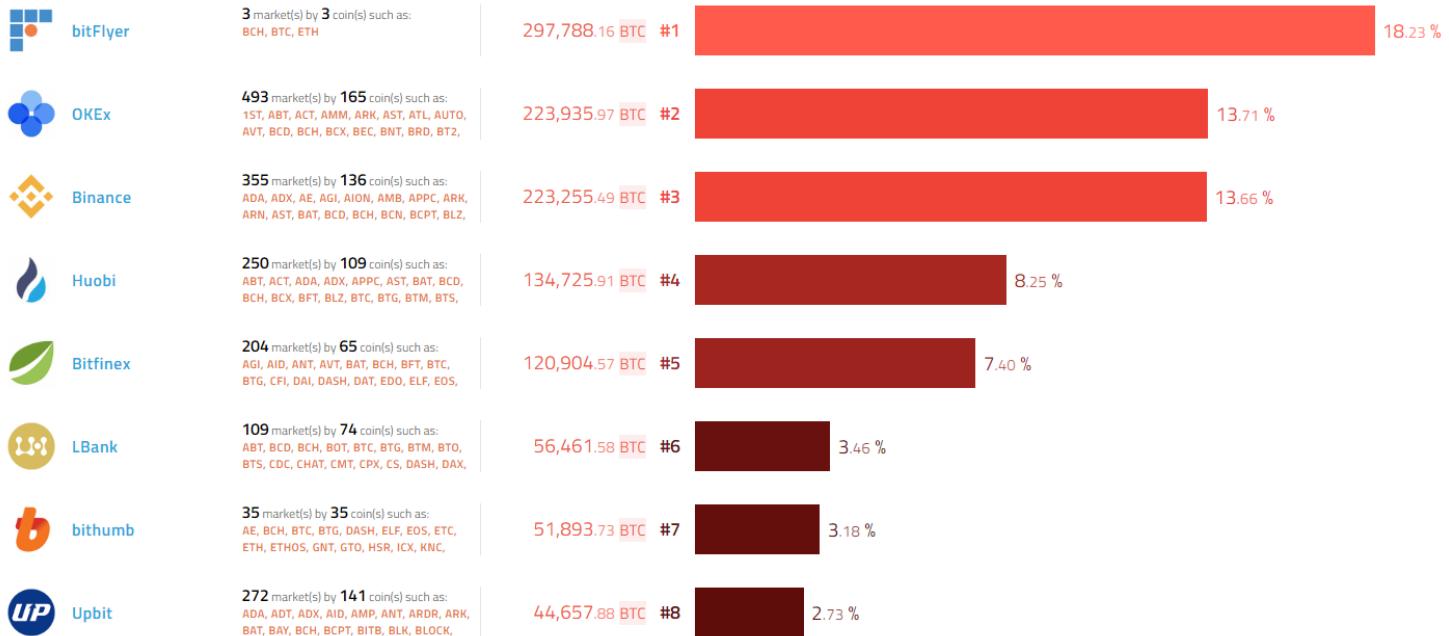
월렛=지갑=Wallet

- 월렛은 각 블록체인 플랫폼별로 있다.
 - 이더리움계열의 월렛
 - 비트코인계열의 월렛
 - 암호화된 개인키와 공개키가 다르기 때문이다.
- 월렛에서 개인키와 공개키가 만들어진다.
 - PC에 월렛을 설치했다가 이 PC를 포맷하면 개인키가 사라지게 된다.
 - 개인키가 사라지면 복구할 수 없고, 보유하고 있는 암호화폐를 다 잃게 된다. 따라서
 - 월렛을 사용할 때는 반드시 공개키/개인키를 어딘엔가 복사해 놓아야 한다.
- 거래소에서 거래를 하려면 월렛이 있어야 한다.
 - 거래소는 이 개인이 가지고 있는 월렛의 총합
 - 거래소를 해킹한다는 것은 이 월렛에 있는 개인키를 가져간다는 뜻
- 비트코인계열:
 - Coinbase, blockchain.info, MyCelium
- 이더리움계열:
 - 미스트(Mist; <https://github.com/ethereum/mist/release>),
MyEtherWallet(myetherwallet.com)
- Jaxx(jaxx.io) : 여러 플랫폼을 지원

암호화폐 거래소

- 암호화폐 거래소의 거래량 순위 (2018.6.13)
 - <https://www.coinhills.com/market/exchange/>

일본



블록체인(Blockchain)의 구조

- 블록의 구조(이더리움)
- 블록헤더: 블록헤더가 해시 되어 이후 블록에 블록해시에 저장됨
 - 블록번호(number)
 - 시간(timestamp) : 블록이 생성된 시간
 - 머클트리 루트(root) : 개별 거래정보가 위치한 디렉토리의 해시값
 - 부모 블록해시(parent hash) : 앞 블록헤더 해시값
 - 난이도(difficulty) : 채굴 난이도 조절용 수치
 - 넌스(nonce): 최초 0 시작 조건을 만족하는 해시값을 찾을 때까지 1개씩 증가하는 횟수
 - 기타 gas limit, gas used, extra data
- 블록바디
 - AccountNounce
 - 받는주소(Recipient)
 - Amount
 - Payload (옵션으로 임의의 메시지, 계약생성코드)
 - GasLimit(거래 실행시 수행되도록 허용된 최대 트랜잭션 수행 횟수)
 - Price(계산 단계마다 발신자가 지불하는 수수료)

이더리움의 현황

<https://etherscan.io>



LOGIN

Search by Address / Txhash / Block / Token / Ens

GO

Language

HOME

BLOCKCHAIN

TOKENS

RESOURCES

MORE

Just released: **Ethereum Nodes Tracker**. [Explore Now!](#)



MARKET CAP OF \$21.395 BILLION

\$207.34 @ 0.03255 BTC/ETH ▼1.09%

LAST BLOCK

6701016 (14.0s)

Hash Rate

243,342.51 GH/s

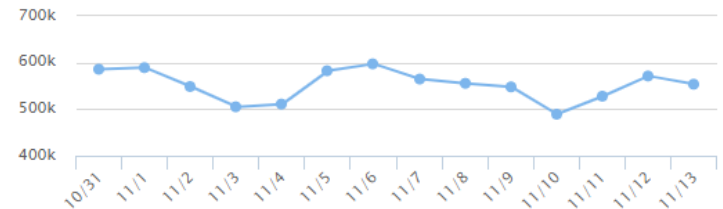
TRANSACTIONS

342.26 M (6.7 TPS)

Network Difficulty

3,025.23 TH

Ethereum Transaction History in 14 days



Blocks

View All

Block 6701016

>28 secs ago

Mined By [MiningPoolHub_1](#)

42 Txns in 5 sec

Block Reward 3.04342 Ether

Block 6701001

>1 min 17 secs ago

Mined By [Ethermine](#)

6 txns in 3 sec

Block Reward 3.00363 Ether

Block 6701000

>1 min 20 secs ago

Mined By [SparkPool](#)

82 txns in 17 sec

Block Reward 3.12427 Ether

Block 6700999

>1 min 37 secs ago

Mined By [MiningPoolHub_1](#)

74 txns in 5 sec

Block Reward 3.2457 Ether

Transactions

View All



TX# 0X5D14C5ED93BFF6143ECD0E9...

>28 secs ago

From 0x2e05a304d3040f1... To [NewContract]

Amount 0 Ether



TX# 0X78AEBD45350E934852738DB...

>28 secs ago

From 0xeb1c12ef37b8803... To 0x515dea727d31cb...

Amount 0 Ether



TX# 0X7100985B1ABAE6F315EB6E6...

>28 secs ago

From 0xe861ec4b2e6f125... To 0x27d16a670bec2e...

Amount 0 Ether



TX# 0X405DFC9689CACC656556E0F...

>28 secs ago

From 0x9880f0fff5dc757cf... To 0xd112f302969901f...

Amount 0 Ether

블록체인(Blockchain)의 구조 (header)

Block #6701083

[Home](#) / [Blocks](#) / [Block Information](#)

Overview

Comments


Block Information ◀ ▶

Height:	6701083
TimeStamp:	4 mins ago (Nov-14-2018 05:11:33 AM +UTC)
Transactions:	87 transactions and 96 contract Internal Transactions in this Block
Hash:	0x03cf002e428f01b0b5aa5abb88d9b085bfc7c247520a0fff6ccd9f5e68de318a
Parent Hash:	0xd1dad474de7588c107cca3ef701147f9749f1fab7005c8e0a22fe1a80f8d1cb9
Sha3Uncles:	0x0d77972346abc5b1c5e2266389128689a89a62f30fbb67ad7644309e62f48abf
Mined By:	0x5a0b54d5dc17e0aad383d2db43b0a0d3e029c4c (SparkPool) in 7 secs
Difficulty:	3,062,107,569,293,554
Total Difficulty:	7,797,262,000,015,177,879,683
Size:	14978 bytes
Gas Used:	7,998,478 (99.98%)
Gas Limit:	8,000,029
Nonce:	0xc47819e01c32ea09
Block Reward:	3.140487828412131025 Ether (3 + 0.046737828412131025 + 0.09375)
Uncles Reward:	2.25 Ether (1 Uncle at Position 0)
Extra Data:	sparkpool-eth-cn-hz (Hex:0x737061726b706f66c2d6574682d636e2d687a)

블록체인(Blockchain)의 구조 (Trx 바디)

Transaction 0x8531f7f370ba9b0048acb7563e0f4fca411a079a742db23de3748d30c8ab8076 

[Home](#) / [Transactions](#) / [Tx Info](#)

Sponsored:  **UTIX** - "Revolution in Blockchain", "Future of ticketing". Secure, Transparent & Fraud proof. [Join us, invest today!](#)

Overview

Comments

Buy ▾

Crypto Loan ▾

Transaction Information ◀ ▶

Tools & Utilities ▾

TxHash: 0x8531f7f370ba9b0048acb7563e0f4fca411a079a742db23de3748d30c8ab8076

TxReceipt Status: **Success**

Block Height: **6701083 (2 Block Confirmations)**

TimeStamp: 40 secs ago (Nov-14-2018 05:11:33 AM +UTC)

From: 0x83f72edb61f3fe03b4d934dfd0c9324025da878c

To: 0xd20a47af3a5aca87514e09134067df928b6c2279

Value: 1.04805219 Ether (\$217.15)

Gas Limit: 21000

Gas Used By Transaction: 21000 (100%)

Gas Price: 0.000000008 Ether (8 Gwei)

Actual Tx Cost/Fee: 0.000168 Ether (\$0.03)

Nonce & {Position}: 0 | {86}

Input Data:

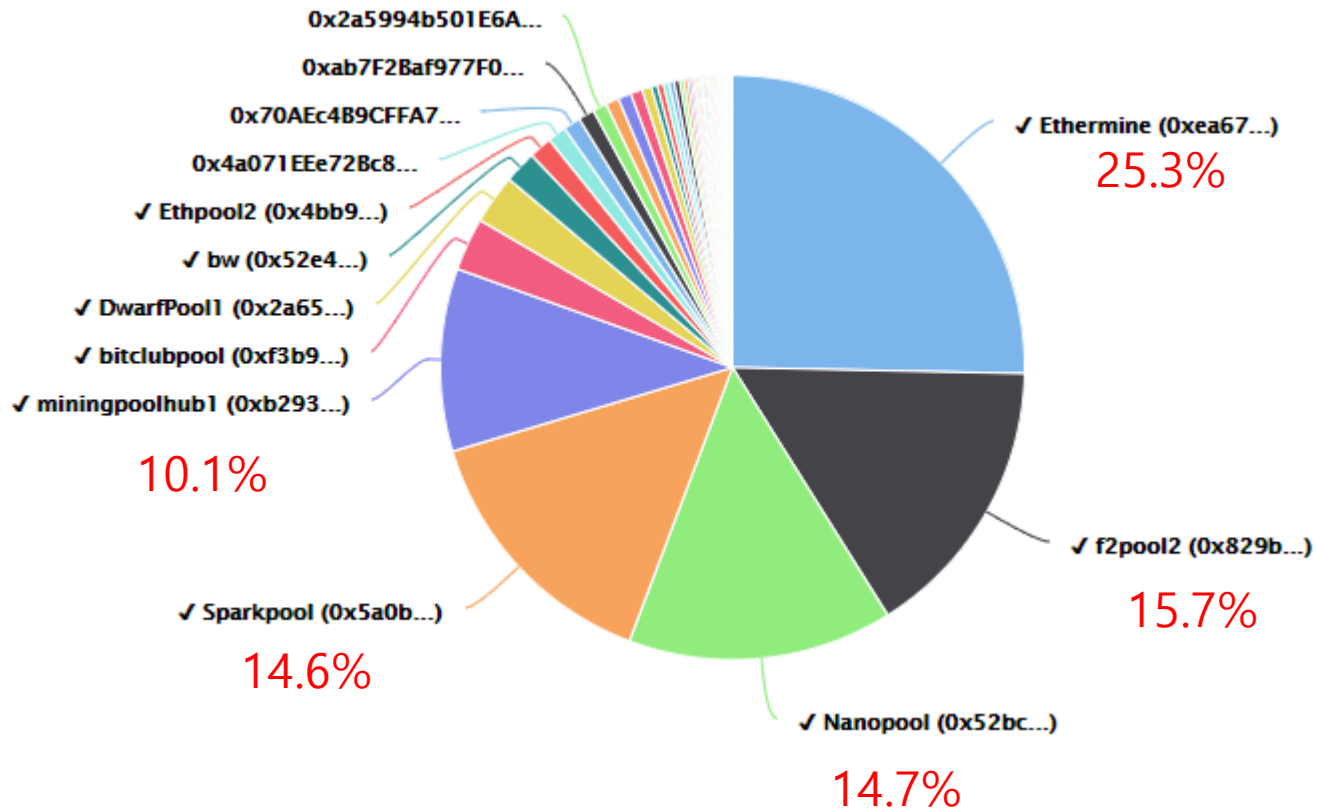
0x

암호화폐에서 채굴이란 무엇인가?

- 암호화폐를 서로 사고 팔 수 있도록 하기 위한 시스템 운영 = 채굴 (또는 Mining)
- 블록체인이 아무나 가입할 수 있을 경우, 채굴자를 선정해서 블록을 만들어 다른 가입자들에게 복사해야 함
- 채굴자를 선정하는 방법 = consensus rule (합의 규칙)
- 암호화폐를 서로 사고 팔 때 생기는 거래 기록 = 블록
- 블록을 생성해주는 업자 = 채굴자
- 암호화폐를 거래하는 수수료가 채굴자에게 제공

** 참고: 채굴업은 거대한 컴퓨터 시스템 필요함 (처음 블록을 생성해주는 업자에게 수수료가 돌아가므로. 현재는 주로 중국인들. 현재, 이더리움 경우 블록당 3이더 = 240만원 정도)

이더리움의 채굴자들



이더리움은 상위 5개 채굴업자 80.1% 차지함
- 단합의 위험성, 이들의 목소리가 커짐, 이해관계 보증

채굴과 합의규칙(consensus rule)

- 채굴
 - 해시를 계산하는 과정. CPU 타임이 많이 듦 = 전기 (GPU, FPGA)
 - 채굴에 보상.
 - 채굴이 없으면 블록체인이 존재할 수 없음
 - 채굴업자의 기업화. 10개 미만의 업체가 90% 이상 점유
 - 채굴업자의 파워가 점점 커짐. 이 업체들이 단합한다면? (51% rule)
- 합의규칙(consensus rule)
 - 채굴의 규칙
 - 비트코인, 이더리움 = Proof of Work (POW). 아무나 다 할 수 있음. 채굴업자 파워
 - 이것을 Proof of Stake(POS) : 일정량 이상 해당 코인 보유자가 채굴. 수수료 지급. 많은 컴퓨팅 파워가 필요 없음, 51%문제에서 비교적 안전.
 - 이더리움 차기 버전(Casper)에서 POS 적용예정
 - DPoS(Delegate Proof of Stake) : 대표자 선정. EOS, Steem 에서 사용
 - 기타 대단히 많다.
 - Performance에 결정적인 영향

Hard fork, Soft fork, Segwit

- Hard fork
 - Fork 라는 용어는 컴퓨터에서 새로운 프로세스(프로그램 실행) 하나 띄우는 것을 의미
 - 블록체인이 자꾸 길어지는데, 특별한 이유(대규모 업그레이드, 내부 구성원의 의견 불일치)로 블록체인 잘라서 따로 살림을 차리는 것을 의미한다
 - The DAO 사건으로 이더리움이 이더리움 클래식과 이더리움으로 갈라졌고 , 비트코인이 비트코인과 비트코인 캐시 갈라진 케이스 등이 있다
- Soft fork
 - 소프트웨어 업그레이드 방식으로 구버전과 호환성 유지
 - 채굴자들은 모두 새버전을 사용해야 하므로 채굴자들의 동의가 필요
- Segwit (Segregated Witness : 증인분리)
 - 트랜잭션 중 전자서명(digital signature)과 관련된 부분을 분리해서 블록의 마지막 부분에 보관
 - 원래는 트랜잭션 데이터와 전자서명이 하나의 블록(1M)에 있었는데 이를 분리해서 트랜잭션 데이터만 하나의 블록(1M)에 저장하고 전자서명은 다른 블록에 저장
 - 더 많은 트랜잭션을 처리할 수 있음

스마트 컨트랙트(Smart Contract)

- 1994. Nick Szabo
 - 신뢰할 수 없는 인터넷 환경에서 디지털 계약을 준수하도록 하는 프로토콜
- 목적
 - 비트코인 script 단순 실행 프로그램만 지원
 - 이더리움: 상태의 변경과 데이터의 저장 등을 통해서 상태 전이가 가능
 - Tuning complete 코드로 발전
 - 블록체인에서 data manipulation이 가능한 프로그램을 실행
- 내용
 - 복잡한 컨트랙트 (ICO의 토큰발행) – 조건, recursive 등 수행 가능
 - EVM (Ethereum Virtual Machine) 에서 작동
 - Solidity (스마트 컨트랙트 분야에서 가장 많이 사용)
 - Serpent, LLL, Mutan 등
- 실행
 - 개발 후 컴파일. 바이트 코드로 생성. 컨트랙트 배포. Geth 내의 EVM에서 실행
 - 새로운 스마트 컨트랙트 생성, 특정 스마트 컨트랙트 함수 실행, 이더 전송
 - 코드 라인 당 실행 비용인 gas 부가
 - 한번 실행되면 변경 불가능. Source code는 오픈된다.
- 스마트 컨트랙트의 버그수정, 업데이트
 - 새로운 기능 추가, 기존 프로그램 수정은 어려움(블록체인 기능)

이더리움의 문제점

- 퍼포먼스(Performance)
 - 이더리움: 20 tps
 - 합의규칙(POW), 무작위 채굴, 채굴난이도 조정
 - Long chain(계속 커나감) : Hard fork, Soft fork
- 내용 보안(confidentiality)
 - 거래 내용을 누구나 다 볼 수 있다.
- 거버넌스(Governance)
 - 전체 운영의 주체가 없으므로 (탈중앙화) 운영의 문제점이 있어도 시정이 어렵다
- 개발환경 (블록체인 일반)
 - Geth, Mist, Solidity, truffle : 잘 아는 환경이 아니다.
 - 지금의 개발 환경에 비해서 열악하다. Tool도 별로 없다
- 채굴 비용
 - Gas 비용. 스마트 컨트랙트는 더 비쌈.
 - Gas에 따라서 채굴업자의 처리 우선순위가 바뀐다
- 파이널리티(finality)
 - 데이터가 완전히 블록체인에 write된 것을 확정하는데 걸리는 시간
- 스마트 컨트랙트의 버그수정, 업데이트
 - 새로운 기능 추가, 기존 프로그램 수정은 어려움(블록체인 기능)

이더리움의 좋은 영향 – 다양한 블록체인 형태 등장

- 이더리움의 스마트 컨트랙트 등장으로 단순히 암호화폐를 만들고 유통하는 것 뿐 아니라, 일반 기업체에서 블록체인 기술을 도입하려는 시도가 있음
 - ✓ 비트코인, 이더리움은 기본적으로 퍼블릭 블록체인 (토큰 발행)
 - ✓ 기업환경에 적용은 프라이빗 블록체인(토큰을 발행하지 않음)
- 이더리움의 스마트 컨트랙트는 이더리움 내에 다양한 블록체인 서비스를 만들 수 있도록 했음
 - ✓ 블록체인 플랫폼은 이더리움 같이, 내부에서 블록체인 서비스를 해줄 수 있는 시스템
 - ✓ 블록체인 서비스는 블록체인 플랫폼에서 와인, 부동산, 진품추적과 같은 서비스를 제공
- 블록체인 서비스는 꼭 블록체인 플랫폼에서만 받을 수 있게 되면 블록체인 플랫폼에 dependency가 생기므로...
 - ✓ 블록체인 서비스를 만들 수 있는 소프트웨어가 등장 → 블록체인 소프트웨어 (대체적으로 무료. Open Source Software)

이더리움의 좋은 영향 – 다양한 블록체인 형태 등장

- 블록체인 서비스는 꼭 블록체인 플랫폼에서만 받을 수 있게 되면 블록체인 플랫폼에 dependency가 생기므로...
 - ✓ 블록체인 서비스를 만들 수 있는 소프트웨어가 등장 → Hyperledger
 - ✓ 블록체인 소프트웨어 (대체적으로 무료. Open Source Software)
- 비트코인, 이더리움을 운영하다 보니, 탈중앙화 철학에 문제가 생김
 - 블록체인의 탈중앙화 철학은 중앙에 어떤 대표자들이나 하나의 대표/기관이 없이 누구나 다 서로 거래를 할 수 있게 하는 것.
 - 그런데, 기존의 합의로직으로 인한 퍼포먼스 저하, 스마트 컨트랙트를 의도적으로 코딩, 거대 채굴자 등장으로 인한 51%넘을 위험성 – 전체 운영에 문제가 생김
 - 모든 문제는 아무다 다 받아주지 말고 특정한 기준을 만들어서 차별적으로 받아주자 ... → Permissioned Blockchain
 - 아니다. 문제가 있어도 탈중앙화의 정신을 살려야 한다! → Permissionless Blockchain
 - 프라이빗 블록체인은 당연히 Permissioned Blockchain
 - 퍼블릭 블록체인은 Permissionless Blockchain 도 있고, Permissionless Blockchain 도 있다. 3세대 퍼블릭 블록체인 추세는 Permissionless 보다는 Permissioned Blockchain 로 가는 경향이 있음.

비트코인, 이더리움의 문제점을 해결하는 방향

1. 분산원장기술(DLT: Distributed Ledger Technology)
 - Blockchain 구조를 사용하지 않음
 - 기존의 Database에 분산원장 개념 도입
 - 퍼포먼스, 보안 등을 강화
 - R3 Corda, IOTA, Hyperledger
2. 이더리움을 업그레이드
 - 이더리움 재단이 돈이 많다(?).
 - OS 세계의 Microsoft 처럼 blockchain 세계의 표준이 되고 싶어함
 - 업그레이드 하는 비즈니스 창출 (ICO 를 통한 솔루션 비즈니스)
 - EEA (Enterprise Ethereum Association): 기업환경에서 이더리움 활용
3. 3세대 블록체인 플랫폼
 - EOS, STEEM, QTUM, ICON, Cardano, Edenchain
4. DB의 블록체인화
 - Bigchain DB, HbaseChain DB, FlureeDB

1. 분산 원장 기술(Distributed Ledger)

- 블록체인의 문제점인 채굴, 보안(confidentiality), 퍼포먼스, 거버넌스를 해결
- 분산원장의 장점: 탈중앙화, 거래의 추적, 신뢰성의 없는 네트워크에서도 데이터의 동일성 유지
- 이것을 분산원장기술!
 - R3 Corda (R3CEV)
 - Hyperledger (Linux Foundation)
 - IOTA Tangle (IoT 분야)

Hyperledger

- Hyperledger
 - Linux Foundation 2015.12. 17개 회원사 시작. IBM 강하게 지원
 - Pluggable consensus rule
 - 현재 200+ 컨소시엄 업체
 - 국내 (한국거래소, 예탁결제원, 코스콤, SDS 등)
 - Platform: Fabric, Sawtooth, Burrow, Iroha
 - Tool: Cello, Composer, Explorer, Indy
 - 개발환경 IntelliJ IDEA : Go plugin
 - Smart Contract: Chain Code
 - Miner → Validating Peer
- PBFT(Practical Byzantine Fault Tolerant)
 - 요청 클라이언트 → 어플리케이션 → 비검증노드에서 요청 → 리더노드가 검증노드들에게 요청을 전송 → 검증노드 합의 및 컨펌 → 체인코드 실행 → KVS에 기록
 - 즉 검증먼저 실행 나중
 - 참고: Sieve - 실행 먼저 검증 나중.
- 검증노드(validating peer)
 - 리더 노드가 비검증 노드의 트랜잭션 요청을 받아서 검증노드에게 전송
- Chaincode (스마트 컨트랙트)
 - 검증노드(validating peer)가 docker container 에 배포하고 실행함
 - 트랜잭션 = chaincode의 실행
 - 비즈니스 로직을 chaincode로 구현
- KVS(Key-value-store : Couch DB(NoSql의 일종))
 - 트랜잭션 실행결과 state 상태, 데이터 저장
 - Key : chaincode ID + cKey
 - Value : 데이터

R3 Corda 특징

- R3
 - 월스트리트의 베테랑들인 David Rutter, Jesse Edwards, Todd McDonald가 모여 창립한 분산원장 기반의 핀테크 스타트업
 - R3CEV 컨소시엄 결성. Corda 개발. 분산원장기술(Distributed Ledger Technology). 국내 5개은행(국민, 신한, 하나, 기업, 우리)
- Corda 의 데이터 공유
 - 네트워크 참여자들 모두 공유되는 데이터가 없음.
 - 거래 당사자들만 공유
 - 거래상대방끼리 "개별 거래 단위"로 합의를 도출한다.
 - 다양한 합의 규칙
- 관찰노드(observer node)
 - 규제, 감독기구에게 관찰 노드(Observer node)를 제공
- 스마트 컨트랙트
 - 인간 언어(human-language)와 법률언어(Legal-language)을 명시적 링크
- 일반 개발 언어
 - Java, Kotlin으로 개발 JVM에서 실행
- 암호화폐
 - 토큰을 발행하지 않음

Ethereum, Hyperledger, Corda 비교

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	– Generic blockchain platform	– Modular blockchain platform	– Specialized distributed ledger platform for financial industry
Governance	– Ethereum developers	– Linux Foundation	– R3
Mode of operation	– Permissionless, public or private ⁴	– Permissioned, private	– Permissioned, private
Consensus	– Mining based on proof-of-work (PoW) – Ledger level	– Broad understanding of consensus that allows multiple approaches – Transaction level	– Specific understanding of consensus (i.e., notary nodes) – Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)	– Smart contract code (e.g., Kotlin, Java) – Smart legal contract (legal prose)
Currency	– Ether – Tokens via smart contract	– None – Currency and tokens via chaincode	– None

Table 1: Comparison of Ethereum, Hyperledger Fabric and Corda

2. 이더리움 자체의 로드맵

- Casper: Vitalik Buterin
- 1단계 프론티어(Frontier) 2015
 - 암호화폐 블록체인 시대
- 2단계 홈스테드(Homestead) 2016
 - Smart Contract, Dapp
- 3단계 메트로폴리스(Metropolis)
 - Oct 2017 1차 비잔틴 하드포크
 - ➡ – 2018 2차 콘스탄티노플 하드포크 예정 (PoS 변경 = Casper)
 - Privacy (zk-SNARKs)
 - Easier programming for developers
 - Predictable gas charges
 - Increase security for wallet
 - Mining adjustment
- 4단계 세레니티(Serenity) ?
 - Sharding : block을 잘라서 (shard) 계산. 병렬처리
 - 플라즈마 : 사이드체인 기술

2. 이더리움 입장에서 해결하려는 노력

- 퍼포먼스 문제 해결
 - Layer 2 프로토콜: 대부분의 트랜잭션을 layer 2 에서 처리, 여기를 나가고 들어갈 때만 블록체인에 기록
 - 샤딩(sharding), 사이드체인(sidechain), 오프체인(offchain)
- 데이터 privacy 문제 해결
 - Rochkchain (rochain.org)
 - Enigma.co
- 이더리움 미래
 - 2세대 블록체인 플랫폼
 - 스마트 컨트랙트(solidity)
 - 이더리움의 토큰발행 기능 – ICO 에코 시스템 형성
 - Microsoft와 McIntosh 비교 ??
 - 과연 이더리움은 현재의 문제점을 해결하고 블록체인의 표준으로 성장할 것인가?

3. 새로운 3세대 블록체인에 요구사항

새로운 블록체인에 대한 요구사항 (이더리움의 문제를 해결)

- 퍼포먼스(Performance)
 - 최소: 1000tps 이상
 - 좀 더 나은 합의규칙(consensus rule)
 - growing chain : 해결 방안 강구
- 내용 보안(confidentiality)
 - 거래 내용의 암호화.
- 거버넌스(Governance)
 - 탈중앙화 개념을 가지면서 거버넌스를 유지하는 방안
 - 오직 허가된 회원만 가입(permissioned blockchain)
 - Public blockchain 에서도 허가된 대표자만 마이닝
- 채굴 비용
 - Public blockchain : 부담없는 가격
 - Private blockchain : consortium 가입 / 유지비 / 기타 metering 방법
- 개발환경
 - 기존의 잘 알고 있는 개발환경을 사용할 수 있도록...

3. 새로운 3세대 블록체인에 대한 요구사항

- 신속한 파이날리티(finality)
- 스마트 컨트랙트의 버그수정, 업데이트 가능
 - 새로운 기능 추가, 기존 프로그램 수정이 가능하게 하는 방안 강구
- On-chain, Off-chain, Side-chain
 - 다양한 운영환경 제공
- 외부 데이터와 연동하면서 보안 유지
 - 외부 데이터 소스(Oracle)와 연동
- Big Data, deep learning, machine learning 과 연동
 - 기존의 정보계/의사결정 시스템과 연동
- 새로운 개발 방법론 개발
 - blockchain software engineering 방법론 / tool
 - Blockchain process modeling / tool
 - Blockchain based BPM (Business Process Management) tool

3세대 블록체인

Private blockchain

- Hyperledger (Linux Foundation)
- R3 Corda (블록체인이기 보다는 분산원장, R3CEV 컨소시엄)

Public blockchain

- EOS
- Cardano (ADA)
- QTUM
- NEO
- STEEM : Steemit (SNS), Dtube(Youtube)...
- ICON : 한국기업, blockchain
- Eden Chain : 한국기업, name space, e-Oracle,

4. Database를 블록체인화 : Bigchain DB

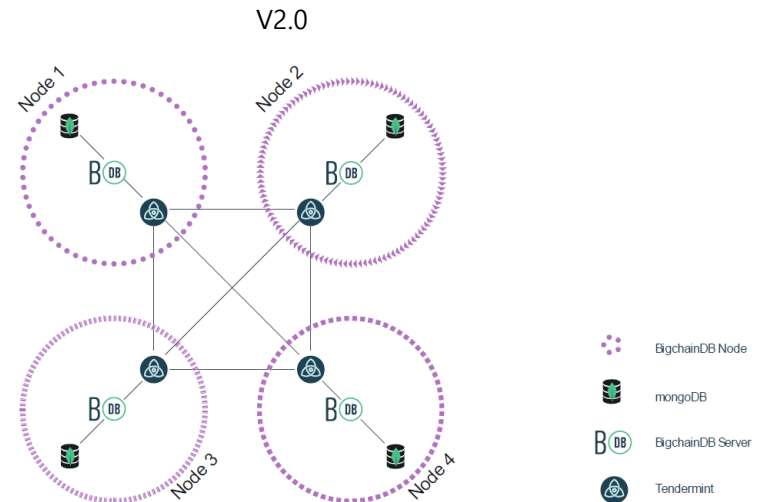
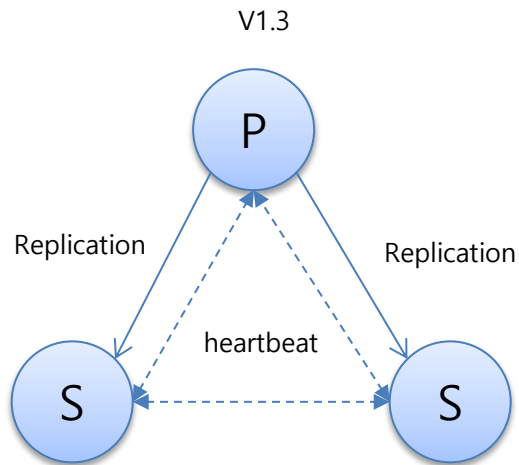
- DB에서 출발한 블록체인 플랫폼
 - Bigchain DB (DB에 분산원장 기술을 적용함)
 - HBaseChain DB (Scalable blockchain framework on Hadoop ecosystem)
 - FlureeDB
- Ascribe.io
 - Bruce Pon, MIT Sloan 출신
 - Bitcoin, Ethereum – 너무 늦어서 service를 올릴 수 없다
 - Art blockchain service. 플랫폼을 개발하기로 결정
 - 현재 bigchain DB 2.0
- 목표
 - 100,000 tps.
 - Peta byte DB
 - Query 가능 (indexed and queryable)
 - 금융, SCM, 송금, 지불, 에너지 등 high transaction 분야를 타겟
- 방법
 1. 기존의 블록체인 기술을 발전시켜서 퍼포먼스, 빅데이터, 쿼리 등을 해결하는 방법
 2. 기존의 빅데이터DB를 개조시켜서 블록체인화 하는 방법 (*Bigchain DB 방식)

4. Database를 블록체인화 : Bigchain DB

	Typical Blockchain	Typical Distributed Database	BigchainDB
Decentralization	✓		✓
Byzantine Fault Tolerance	✓		✓
Immutability	✓		✓
Owner-Controlled Assets	✓		✓
High Transaction Rate		✓	✓
Low Latency		✓	✓
Indexing & Querying of Structured Data		✓	✓

Bigchain DB - 어떻게 DB를 블록체인화 할 것인가?

- 탈중앙화
 - 트랜잭션에 대해서 투표
 - 블록단위로 (1개의 블록에 여러 개의 트랜잭션 포함)
 - Consensus Algorithm : Tendermint (DPoS + PBFT)
- 내용을 바꾸지 못하는 방안
 - 블록전체를 hash 해서 연결
 - Asset 은 digital signature



3세대 블록체인

- 시중에 나와있는 거의 모든 블록체인은 3세대라고 주장
 - 4세대 블록체인을 이야기하는 스타트업도 있음
- 향후 100개 정도의 3세대 블록체인이 나올 것임
 - 90년대 RDBMS 100여종
 - 2010년 초반 Big Data NoSQL DB 120여종
 - 2020년 블록체인 100여 개는 기본으로 나올 것임
- 그러나, 5~8년 후면 10개 미만으로 정리될 것으로 예상

퍼블릭 블록체인 플랫폼 정리

V 1.1

UNBIASED COMPARISON OF PLATFORMS

	Neblio	Nuls	Lamden	NEO	Waves	Lisk	EOS	QTUM	ICON	Ark	Stratis	Wanchain
												
PROGRAMMING LANGUAGE (SUPPORT)	Python, JavaScript, Go, Ruby, Obj C, Java, C#, PHP	Java	Python	Python, Javascript, VB.NET, Java, C#, F#, Golang, Kotlin C++	Scala	JavaScript, TypeScript	C, C++, WebAssembly	Solidity	Python	Python, Elvish, RPC, Lua, Java, R, C, Go, Kotlin, PHP C++, .NET, Nucleid, Ruby, Swift iOS, Rust, Adv Powershell	C#, .NET	Solidity
PROTOCOL	PoS	PoC	DPoS + BFT	dBFT	LPoS	DPoS	DPoS	PoS	LFT	DPoS	PoS	PoS
BLOCK TIME (SEC)	120	10	1	15-20	3	10	0.5	120	1	8	60	N/A
QUICK SYNC	✓	✗	CDNR *	✓	CDNR *	CDNR *	CDNR *	✗	✓	CDNR *	✗	✗
ATOMIC SWAPS	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗
TOKEN LAUNCH COST	10 NEBL	N/A	N/A	500 GAS	1 WAVES	Dynamic	N/A	N/A	N/A	N/A	N/A	N/A
MASTERNODES	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓
SIDECHAINS	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓
PRIVATE CHAINS	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
MAINNET LAUNCH DATE	Jul 2017	May 2018	Q3 2018	Oct 2016	Jun 2016	Q2 2016	Jun 2018	Oct 2017	Jan 2018	Mar 2017	Aug 2016	Jan 2018
DEC* TOKEN CREATION	✓	✓	✓	✗	✓	✓	✓	✓	N/A	✓	N/A	N/A
TRANSACTION COST	0.0001 NEBL	0.01 NULS	Free	Free	0.001 WAVES	0.1 LSK	Free	0.004 QTUM	0.01 ICX	0.1 ARK	0.001 STRAT	N/A
WALLETS	Desktop(Win, Mac, Linux), Android, Docker, Electrum, Pi, Orion Web	ERC20	ERC20	Windows, MacOS, Linux, Ledger	Windows, MacOS, Linux	Web, Windows, MacOS, Linux	ERC20	Web, Ledger Desktop(Win, Mac), Android/iOS	Web	Desktop, Ledger, Web	Desktop(Win, Mac, Linux), Android, Pi, Electrum, Ledger, Breeze	Windows, MacOS, Linux
MAIN SELLING POINT	NTP1 Rest APIs	Modular	Developer Flexible	NEP-5, Digital Identity	Fast and Secure	SideChains	Scalable Flexible	Best of BTC/ETH	Multiple Blockchain Integration	Smartbridges	Simple Easy SideChains	Asset Privacy

N/A = NO ANSWER * DEC = DECENTRALIZED * CDNR = CHAIN DOWNLOAD NOT REQUIRED



Telegram @JamieD1 - Contact for edits/corrections | Design by @sonikitz & @JamieD1

차세대 Public blockchain platform에 대한 요구사항

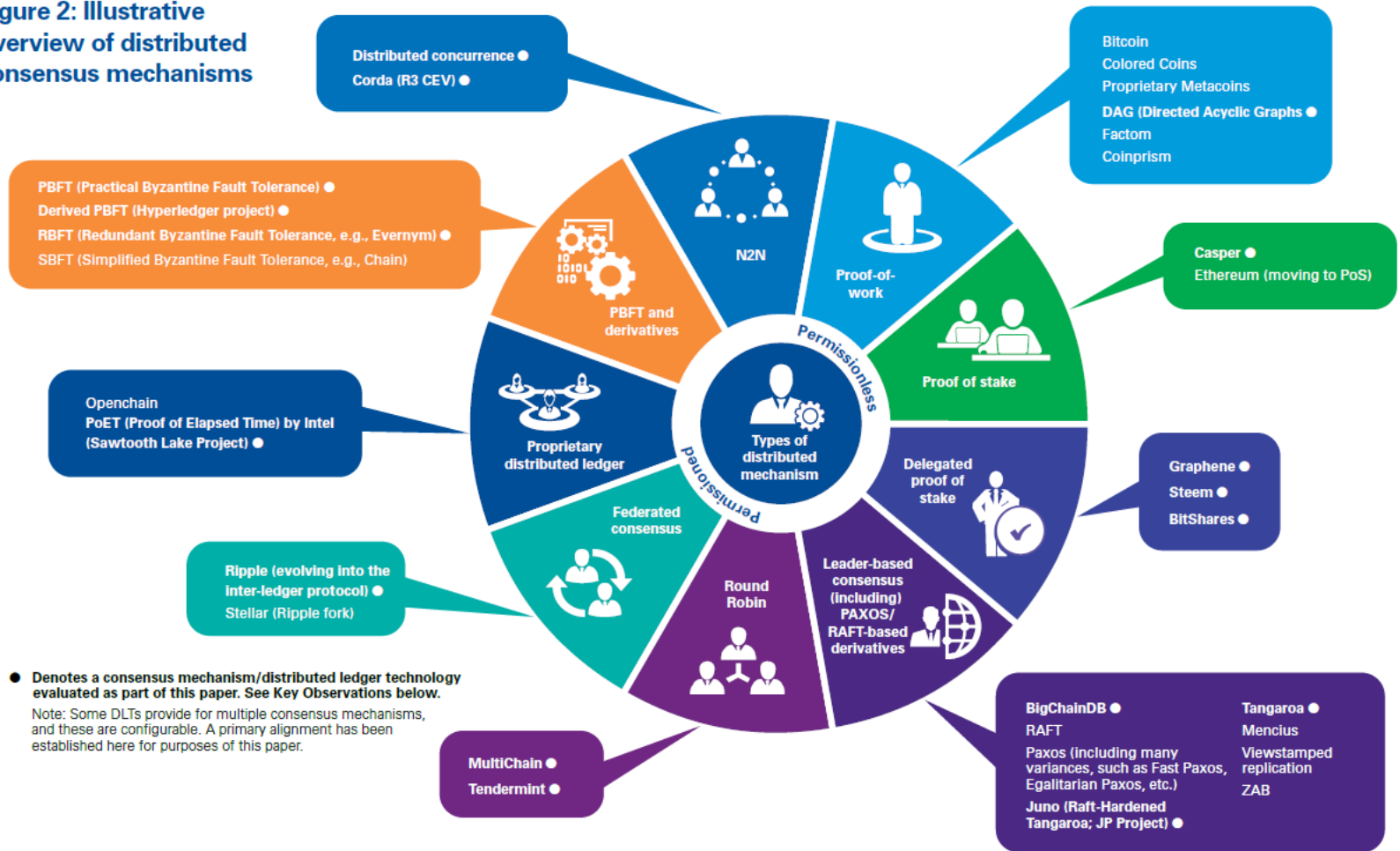
- 기존 2세대 이슈는 완전히 해결
- 신속한 Smart contract, Dapp 개발툴
- 산업별 템플릿
- 자유로운 visibility
- 다양한 OS에 포팅: Android, Mac OS, Windows..
- Big Data, AI, machine learning 과 연동
 - 기존의 정보계/의사결정 시스템과 연동
 - AI기반의 Consensus logic
- 새로운 개발 방법론 개발
 - blockchain software engineering 방법론 / tool
 - Blockchain process modeling / tool
 - Blockchain based BPM (Business Process Management) tool
- Blockchain Sandbox (blockchain test bed)
 - 클라우드 기반
 - 쉽게 pilot 를 만들어 테스트

Public blockchain platform에 대한 정리

- 블록체인 플랫폼의 퍼포먼스, 채굴 방식, delegation을 운영하는 방식등 결정적으로 consensus rule에 달려 있다.
- 탈중앙화와 중앙화 사이의 결정을 consensus rule 이 한다
- 새로운 consensus rule이 연구되고 개발되고 있다
- 퍼블릭 블록체인 플랫폼을 만들기 위해서는
 - ✓ Consensus rule
 - ✓ Delegation 운영
 - ✓ governance
 - ✓ Master node 유무
 - ✓ Token economy
 - ✓ Fee structure (biz model)
 - ✓ Token 발행 방법
 - ✓ Token 거래소

Consensus Rules 정리

Figure 2: Illustrative overview of distributed consensus mechanisms



다양한 블록체인 개념과 종류

	퍼블릭 블록체인 (암호화폐 있음)	프라이빗 블록체인 (암호화폐 없음)
Platform	Bitcoin, Ethereum, EOS, IOTA, QTUM, VeChain, ICON 등 (ICO 전략, 기업의 Reverse ICO 전략)	아직 없음
Service	Medibloc, (ICO 전략, 기업의 Reverse ICO 전략)	Everledger Diamond, Walmart (기업의 프라이빗 블록체인 도입 전략)
Software	Bitcoin, Ethereum, Hyperledger(v1.1)	R3 Corda(v2.0), Hyperledger(v1.1) FlureeDB, Bigchain DB(Alpha)

- Permissioned Blockchain : 멤버가 되는 조건이 있음
- Permissionless Blockchain : 멤버가 되는 조건이 없음
- 모든 프라이빗 블록체인은 Permissioned Blockchain !!
- 퍼블릭 블록체인은 원래 Permissionless 추세는 Permissioned
- 현재까지 블록체인 software가 많지 않음. ICO의 대상이 되는 퍼블릭 블록체인 플랫폼이나 서비스를 Hyperledger를 기반으로 customizing 하고 있음

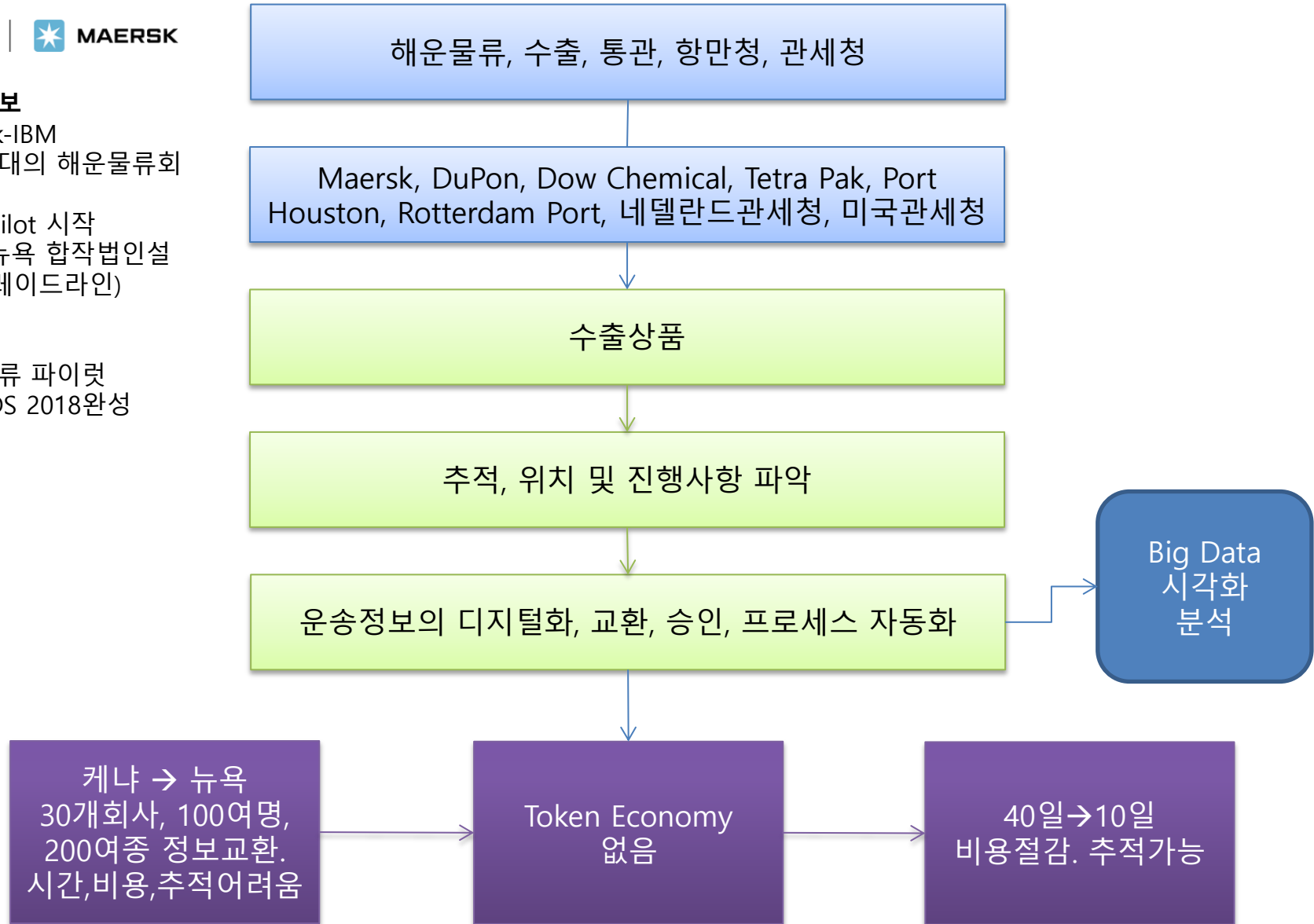
Maersk (해운물류)



회사정보

Maersk-IBM
세계최대의 해운물류회사
2016 Pilot 시작
2018 뉴욕 합작법인설립 (트레이드라인)

한국:
해운물류 파이럿
삼성SDS 2018완성



관세청 “블록체인 기반의 수출통관 물류서비스 시범사업”

프로젝트 개요
한국 관세청
2018.7~2018.12
현재 RFP

병행 프로젝트:
FTA국가간 원산지 증명
서 자료교환(e-C/O) 서
비스

전자상거래 업체와 블
록체인 시범사업



정성적 효과

- **(통관물류 혁신)** 4차 산업혁명의 선도기술인 블록체인 기술 기반으로 국가물류 정보망을 재편, 국가 물류의 표준을 선도적으로 정립하여 민간의 물류혁신 활성화의 토대를 마련함
- **(신기술 시장 활성화)** 수출입 공급망 관련 기업의 실증 참여를 통해 무역·물류 분야에 특화된 블록체인 기술개발이 활성화되고 이에 따른 민간의 일자리 창출로 연계 기대
- **(블록체인 국제표준 선도)** 전략적인 시범사업 추진을 통해 해외 IT업체들의 블록체인 기반 무역기술 연구에 대응한 경쟁력을 확보해 국제표준으로서 선점 가능
- **(제도보완 검토)** 블록체인 기반의 수출입 공급망 시범적용을 통하여 다양한 물류 주체별 검토사항 및 제도적인 보완사항 파악하여 검토 할 수 있음

정량적 효과

- **(물류비용 절감)** 수출입 공급망의 정보공유 시스템 개선(블록체인망) 및 통관물류의 진정한 無서류화(디지털화)에 따라 물류의 신속한 처리에 따라 물류비용 절감
- **(전자정부 수출시장 확대)** 우리나라의 UNI-PASS를 블록체인 기술 기반으로 국제특허를 출원하여 현재 개도국 위주에서 중도국 이상의 국가로 확대하여 수출 증대
- **(수출신고비용 절감)** 수출신고서 작성시의 재입력 작업비용 절감효과 : 약 240억원
 - 수출 기초서류(상업송장, 포장명세서)를 조회하고 다운로드하여 수출신고서 작성을 위한 별도의 신고정보 재입력 작업을 최소화함(편의성 제고, 수작업 오류 감소)

MOBI (자동차 업계)

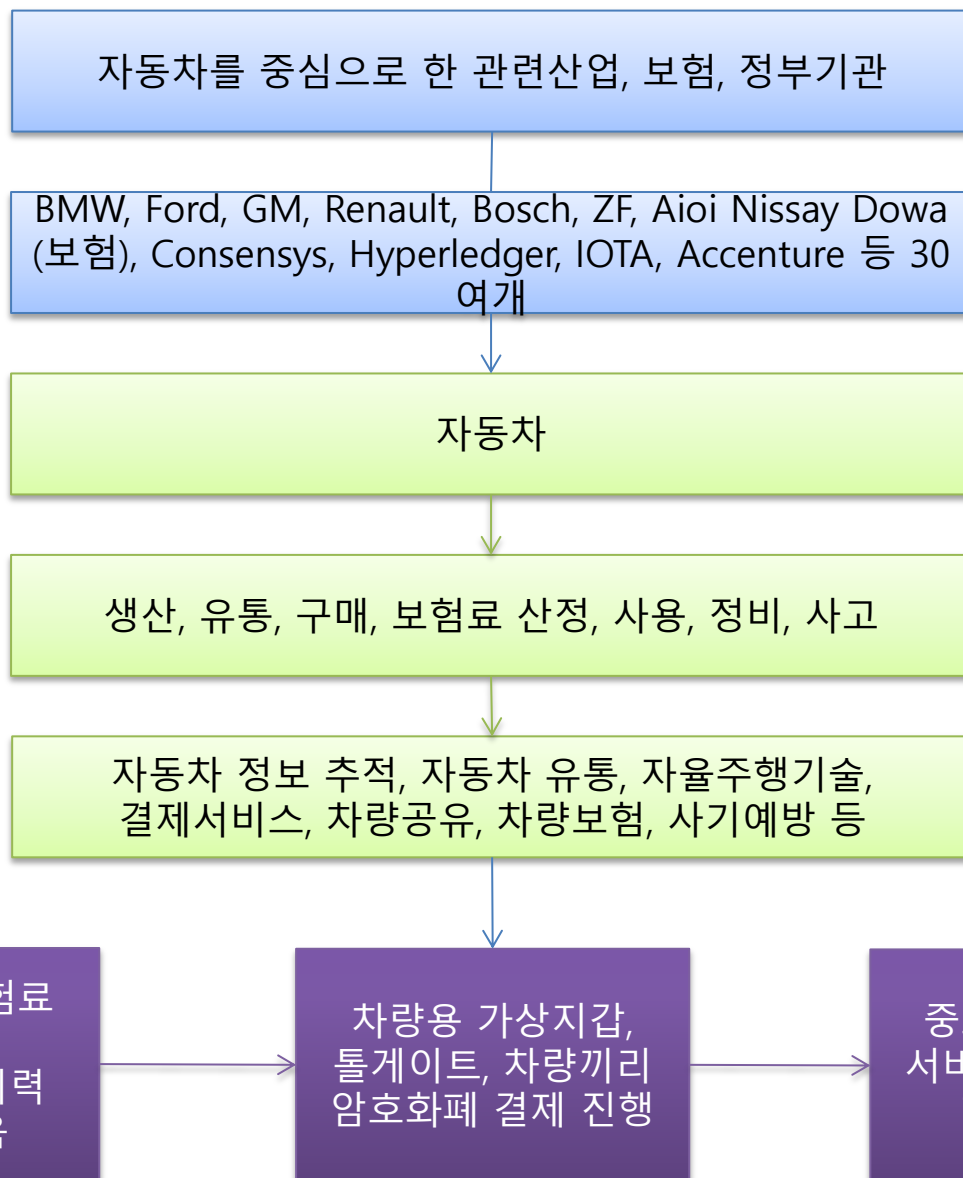


회사정보

CEO: Chris Ballinger
2018.5.2 설립
지금 시작. 데이터수집

공통의 인터페이스를
만드는 것에 집중

프라이빗, 퍼블릭
블록체인 동시 지원
(IOTA - IOT 전용
public blockchain
Hyperledger - private
blockchain)



배경

- 자동차 운행에 대한 다양한 정보는 현재 Apple(Car Play), Google(Android Auto), Amazon(Alexa) 등이 소유
- **자동차업계의 인터넷거대 기업에 대한 위기의식**
- 데이터에 대한 정보를 탈중앙화 방식으로 공유.
- 자동차 차량 운행, 센서 데이터 등 빅데이터 수집하여 공유
- 자동차의 생산에서 신차판매, 소유, 정비, 사고, 보험, 중고차판매, 폐차까지 Tracking하는 비즈니스를 시도할 수 있음 (산업재편)
- 자동차 제조분야(SCM), 고객취향의 변화를 반영한 신차 디자인

블록체인 시대 무엇을 할 것인가?

- 무한한 생각, 생각, 생각 → “왜 꼭 이렇게 하지?”
 - 항상 “탈중앙화”의 이점이 무엇인지.
 - 중앙화의 장점과 결합하면서 탈중앙화를 지향하는 방법은 없나?
 - 기존 DB에 탈중앙화 성격을 부여한다면??
 - 좀더 빠른 합의규칙(Consensus Rule)은 없는가?
 - 꼭 이런 툴을 써야 하나?
- 어느 쪽 선택할 것인가?
 - 개발은 플랫폼/환경/툴이 중요
 - 이더리움 – 현재도 엄청난 투자
 - 분산레저(금융) – R3 블록체인은 역시 금융
 - 하이퍼레저 – 범용성이 있는 프라이빗 블록체인 솔루션, IBM backup
 - Microsoft Coco blockchain framework
 - 기타... 플랫폼을 만들어보는 쪽?

블록체인 시대 무엇을 할 것인가?

- 퍼블릭 블록체인

- 무수한 ICO (2018년, 최소 1000개, 개당 200억 정도) : 돈이 있다 = "좋은 개발자 구함"
- 퍼블릭 블록체인 - 과거의 인터넷 (제2인터넷). 치열한 경쟁에서 살아남아야.
- 고객은 블록체인(Dapp)으로 만들었다고 사용하지 않는다. 기존 앱과 차별화 방안
- 현재는 white paper 만으로 ICO하기 힘들다.
- 기존 인터넷 비즈니스의 일부에 블록체인 적용 → Reverse ICO 컨설팅

- 프라이빗 블록체인

- 프라이빗 블록체인 - 과거의 인트라넷(컨설팅, SI 업 및 솔루션판매)
- 기존 전산화 부분의 10% 정도는 블록체인화
- "IT의 중흥기 도래"
- "탈중앙화"의 장점을 살릴 수 있는 분야를 발견하는 것, 파이롯 프로젝트 시작 → 전략 컨설팅
- 결국 프로세스를 기준으로 모델링 → 프로세스 모델링 컨설팅
- ERP업체, 특히 SCM 부분을 블록체인 적용가능성 높다
- 무수한 프라이빗 블록체인 솔루션 시장 등장 (개발툴, 모델링툴, 통합툴, 분석툴...)
- 클라우드와 결합(Microsoft COCO blockchain framework, IBM Hyperledger -Bluemix, Oracle)
- 기존 글로벌 IT 업체가 블록체인에 사활을 걸 것임

블록체인 시대 무엇을 할 것인가?

- 개발 분야
 - 블록체인 엔진 분야: 블록체인 내부구조, hashing, digital signature, merkle tree, IPFS
 - Dapp 개발(web, javascript)
 - Smart Contract 분야 개발(Solidity, Golang)
- 없는 분야를 개발하는 스타트업 (ICO찬스)
 - 블록체인과 프로세스 모델링
 - 블록체인과 AI, Big Data, Machine Learning과 결합
- 없는 산업으로 들어가자 (Reverse-ICO찬스)
 - 금융, 우리나라는 대부분의 대기업이 수직 계열화되어 있음
- 새로운 것에 대한 오픈 마인드
 - 탈중앙화와 기존 중앙화에 대한 차이점 인식

블록체인 시대 기업은 무엇을 할 것인가?

- **블록체인을 활용하면 좋은 분야**
 - 반드시 여러 기업, 여러 party가 상호 거래하는 분야.
 - 하나의 자산을 처음 생길 때부터 사라질 때까지 tracking해야 하는 분야
 - 진짜임을 꼭 증명해야 하는 분야(diamond, 농산/축산/수산물 원산지, 양주, 예술품, 명품 등)
 - 전체 수직 계열화된 분야를 블록체인화: 제조, 물류, SCM 등
 - 정부공공 분야는 매우 많은 업체와 연결(의료, 인증, 주택거래, 자동차등록, 기타....)
 - Digital Intellectual Property : 음악, 디지털 아트, 영화, 기록물...
 - Programmable Economy (Edenchain, Gartner) : 나의 1시간 블록체인 강의, 유명 셰프의 출장 요리, 1시간 출장 청소봉사, 기타 전통적으로 표현되지 못한 서비스를 거래
- **개별기업 내부를 위한 시스템을 블록체인으로 바꾸지 말 것**
 - 어떤 형태로든 1개의 기업에서 사용하는 분야는 그냥 기존 DB할 것
 - 아직은 블록체인은 비싸다 (인력, computing power, Tps, 기타..)
 - 블록체인 도입 및 활용전략 우선
 - 블록체인으로 모든 문제를 해결하려고 하지 말 것
- **Reverse ICO 기회**
 - 블록체인 및 빅데이터, AI 에 대한 이해와 능력이 있어야
 - 기존의 business에 블록체인을 도입하면 효과가 뚜렷한 분야 (디지털 콘텐츠, 원산지증명, 명품 거래 등)
 - 기존에 쌓은 포인트의 코인화는 좋으나 코인을 다른 곳에서 편하게 사용할 수 있어야
 - Alliance 능력: 블록체인으로 더 많은 제품과 서비스를 연합, 융합하는 능력

결론

- 기존 application의 10% 정도는 블록체인을 도입해야
- 정부,공공 분야의 블록체인 수요가 대단히 많을 것
- 블록체인은 OLTP 시스템이다
 - 규모가 크다 (수백억 대 이상)
 - 국내기업의 수직계열화 부분 때문에
 - 앞으로 블록체인으로 차차세대 시스템 구축을 하게 될 것
- 앞으로 탈중앙화를 지향하는 퍼블릭 블록체인과 기존의 인터넷 글로벌과 싸움(Google, Amazon, Facebook, Youtube, Airbnb, Uber 등)
 - 콘텐츠 제공자와 사용자에게 보상을 할 수 있는 토큰이 큰 매력
 - ICO로 싸울 수 있는 실탄은 있으나 Moral hazard 우려
 - 개발자 절대 부족
 - 새로운 고객 전략
- 블록체인으로 새로운 시대는 열수 있으나...
 - 블록체인 진영이 해결해야 하는 무수한 문제들이 있다
 - 결국 스마트한 전략과 마케팅 능력, 뛰어난 개발자를 가진 스마트한 스타트업이 승리할 것
 - 기회의 땅은 맞다.

The background of the slide features a blurred image of a person in a dark suit holding a transparent blue globe. Surrounding the person is a network of white lines connecting various circular icons. These icons include a globe with a cityscape, a globe with a bar chart, a globe with silhouettes of people, a globe with hands holding it, a globe with a laptop, a globe with a map, and a globe with a cityscape. The overall theme is global connectivity and business.

감사합니다.

AiBB Lab

donchang0725@gmail.com

010-5259-9509