

Blockchain.

“Disruptive Technology”

루프체인 & 적용사례

Aug 2018

(주) 더루프



금투협, 세계 최초 블록체인 공동인증 서비스 선택



Blockchain ISP

관세청 개인통관 PJ

국내 2번째 ICO, 최대 모집금액, 국내최초 상장,
블록체인전문회사 최대 자산 규모



Private Coin 지급결제 수단 적용

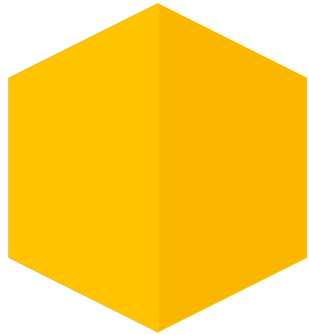


서울시 핀테크랩 업무협약



보험사 업무 Smart Contract 를
통한 자동청구





Contents

- I. **Blockchain 에 대한 오해**
- II. How Blockchain
- III. Case Study
- IV. loopchain™ & ICON™
- V. Q & A

11 Common Myths About Blockchain And Cryptocurrency You Shouldn't Believe



Forbes Technology Council ⓘ

Mar 27, 2018, 07:00am • 9,751 views • #NewTech

1. 'Blockchain Equals Bitcoin'

2. 'Blockchain's Only Application Is Cryptocurrency'

3. 'Information On Blockchain Activity Isn't Publicly Available'

4. 'Crypto Transactions Are Anonymous'

5. 'Blockchain Will Change Everything About Business Transactions'

6. 'Cryptocurrencies Are Volatile, So Blockchain Must Not Be Reliable'

7. 'Cryptocurrencies Are Best For Criminals'

8. 'Blockchain Is Just A Storage Mechanism'

9. 'Cryptocurrency And Blockchain Are For Technology And Finance People Only'

10. 'Tokens And Coins Are The Same Thing'

11. 'Cryptocurrency Is Fundamentally Different From Other Currencies'



[논점 & 오해]

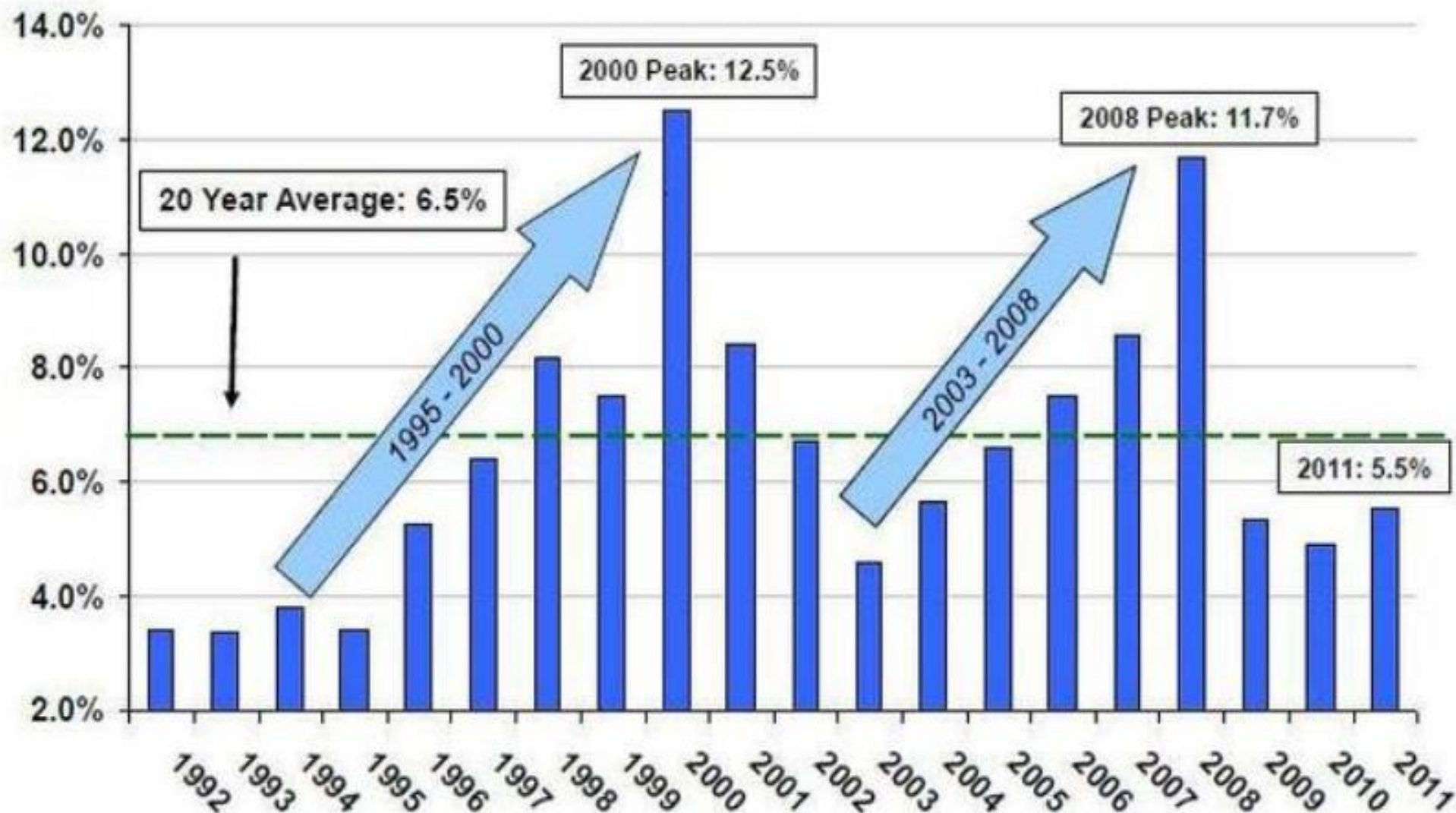
1. 법정화폐가 될 수 없다 ?
2. 퍼블릭 블록체인에서 인센티브(암호화폐)없이 운영이 가능?
3. 사용하는데 보셨어요 ? 아무데도 쓸데가 없다 ?
4. 코인이 왜 이렇게 많은가 ?
5. 블록체인의 보안성이 아직 불안하다 ?
6. 비트코인은 해쉬 난이도가 증가에 따라 채굴비용이 증가하여 결국에는 채굴자가 떠나서 자동으로 비트코인은 붕괴된다?
7. 1세대 2세대 3세대 블록체인이 나오면서 1세대 블록체인은 소멸될 것이다



인센티브 없이 운영이 가능하다?



Completed Global M&A as a Percentage of Market Capitalization



사용하는데 보셨어요 ?

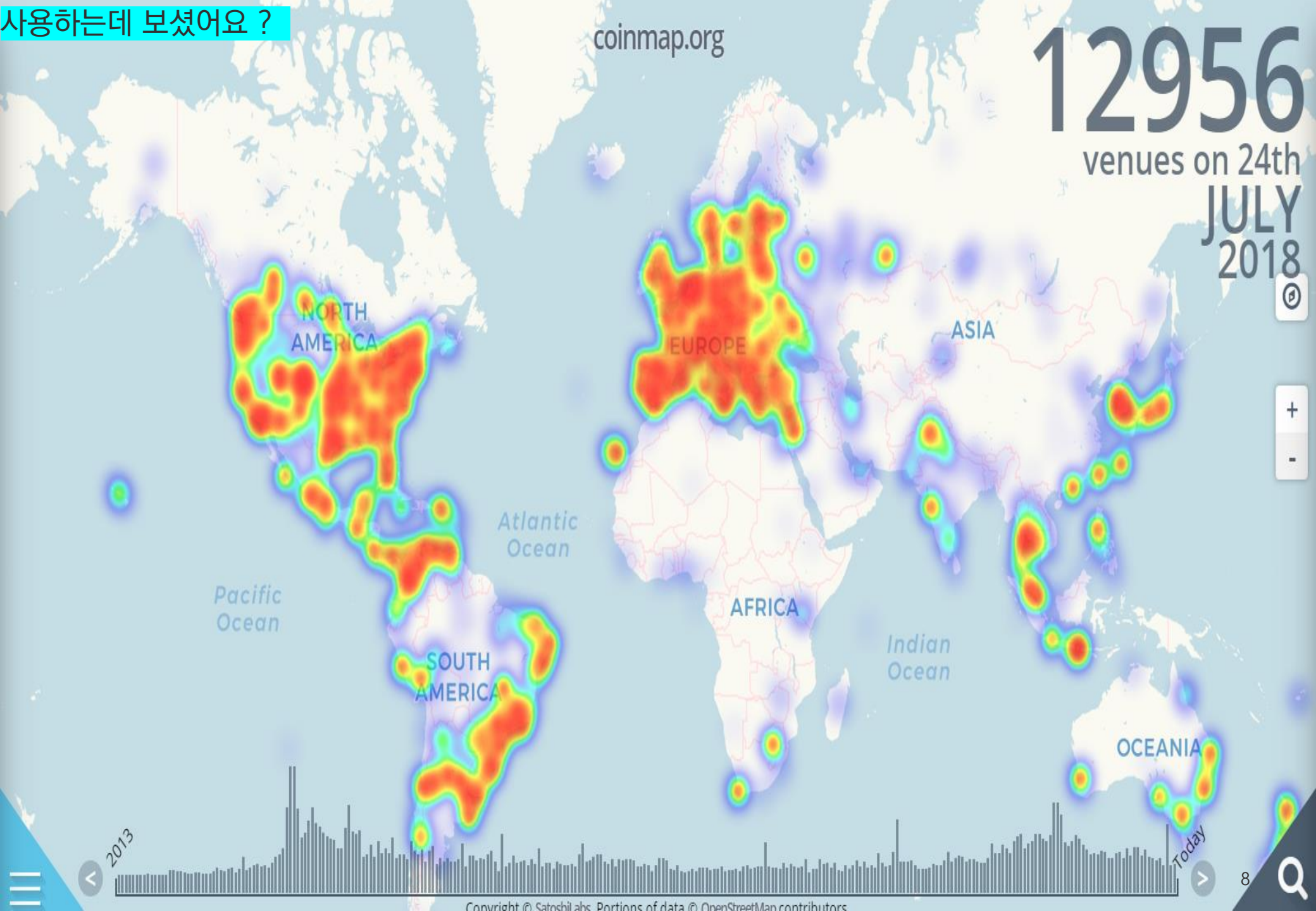
coinmap.org

12956

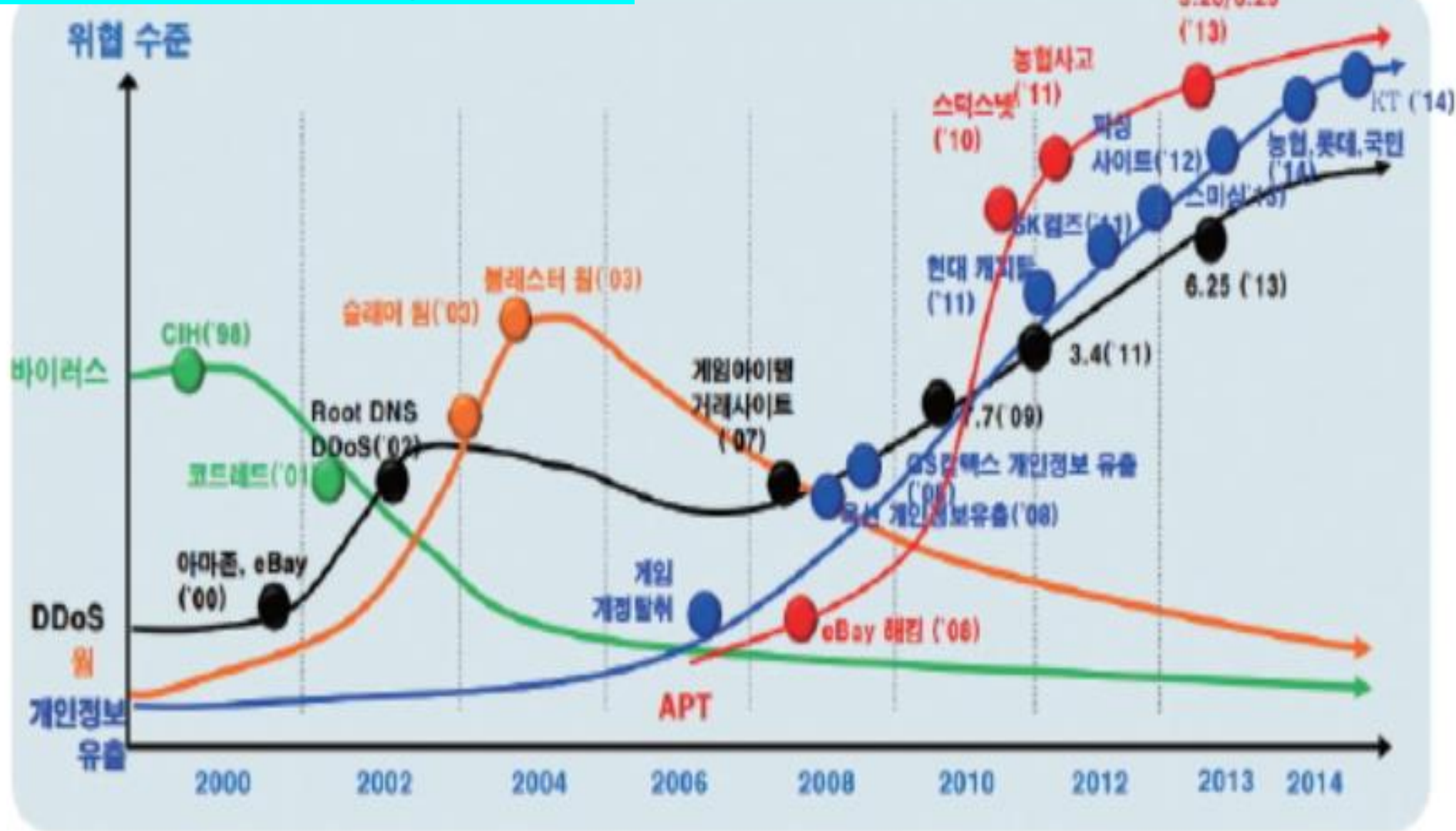
venues on 24th

JULY

2018



블록체인 보안성이 불안해서 적용하지 못한다?



자료: 한국인터넷진흥원(2015. 6) 「사이버공격 최신 동향 및 사이버대피소 소개」, KINX Peering Forum 2015



Difficulty Target and Re-Targeting

As we saw above the target determines the difficulty of finding a solution to the Proof-of-Work algorithm. Why is the difficulty adjustable, who adjusts it?

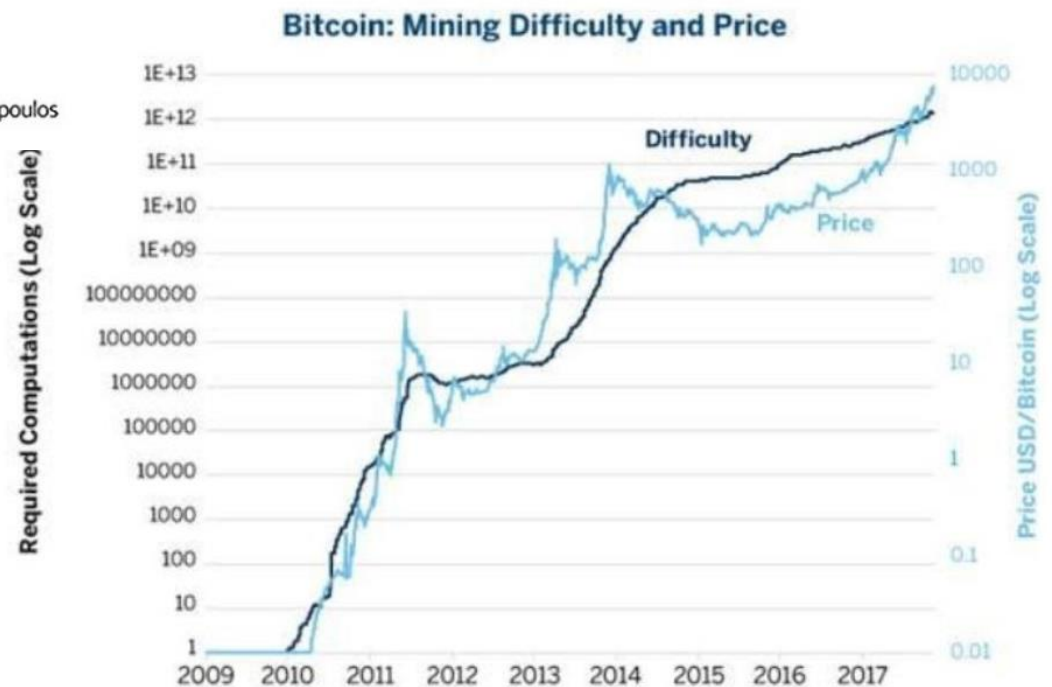
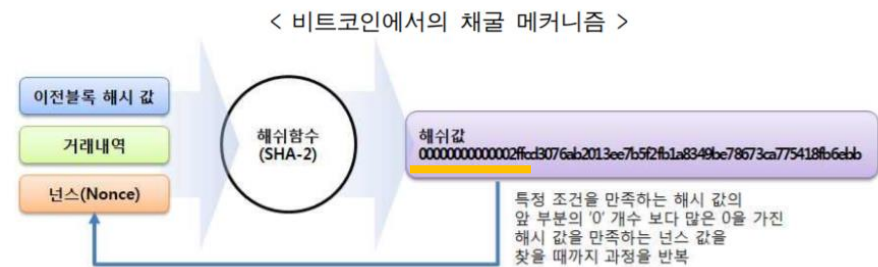
Bitcoin's blocks are generated every 10 minutes, and underpins the frequency of currency issuance and the speed of transaction settlement. It has to remain constant not just over the short term, but over a period of many decades. Over this time, it is expected that computer power will continue to increase at a rapid pace. Furthermore, the number of participants in mining and the computers they use will also constantly change. To keep the block generation time at 10 minutes, the difficulty of mining must be adjusted to account for these changes. In fact, difficulty is a dynamic parameter that will be periodically adjusted to meet a 10-minute block target. In simple terms, the difficulty target is set to whatever mining power will result in a 10-minute block interval.

How then is such an adjustment made in a completely de-centralized network? Difficulty re-targeting occurs automatically and on every full node independently. Every 2016 blocks, all nodes re-target the Proof-of-Work difficulty. The equation for re-targeting difficulty measures the time it took to find the last 2016 blocks and compares that to the expected time of 20160 minutes (two weeks based upon a desired 10 minute block time). The ratio between the actual timespan and desired timespan is calculated and a corresponding adjustment (up or down) is made to the difficulty. In simple terms: If the network is finding blocks faster than every 10 minutes, the difficulty increases. If block discovery is slower than expected, the difficulty decreases.

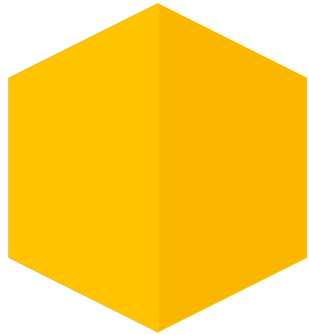
The equation can be summarized as:

$$\text{New Difficulty} = \text{Old Difficulty} * (\text{Actual Time of Last 2016 Blocks} / 20160 \text{ minutes})$$

Here's the code used in the Bitcoin Core client



Source: <https://blockchain.info/charts/market-price?timespan=all> and <https://blockchain.info/charts/difficulty?timespan=all>



Contents

- I. Blockchain 에 대한 오해
- II. How Blockchain**
- III. Case Study
- IV. loopchain™ & ICON™
- V. Q & A

“ Blockchain is NOT , All or Nothing . ”

Princeton Univ

Blockchain Good or Bad (Key word)

Good

공유 협업 수평적
다수의 **가치**의
Middleman 이동 및 저장
Autonomous
(Self- Execution)
HA :Zero down time
Immutable DB

Bad

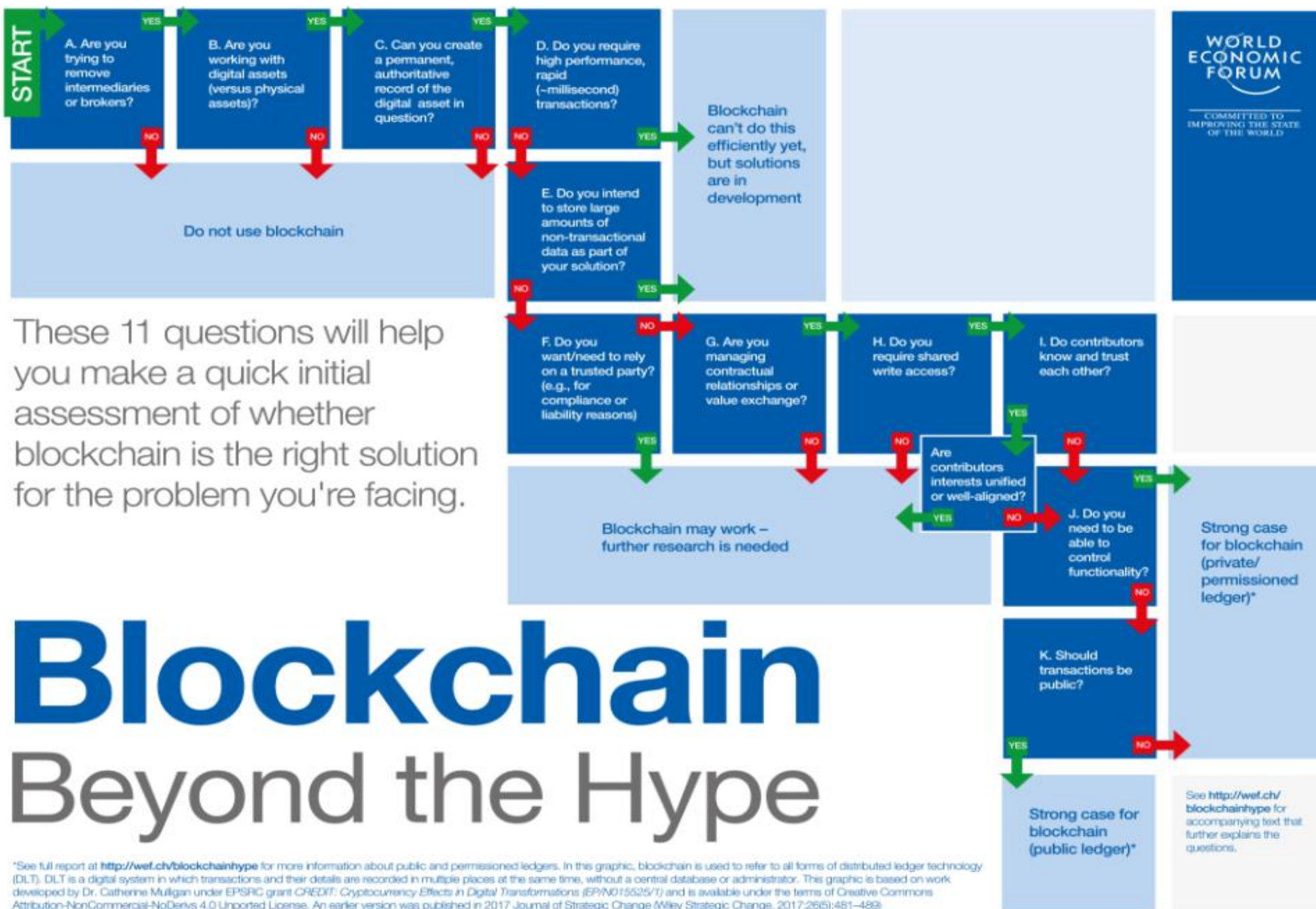
수직적
Ultra low latency
Storage
Big Size Data
RDB
regulation

가치의 저장과 이동에 관한 필수영역

차세대인증(B.FIDO) / 계약 / 지불 (On chain payment)

Horizontal

- 1) 차세대 인증 : 가치의 저장과 이동의 주체 확인 (도메인을 넘어서는 통합인증에 효과적임)
- 2) 계약 : 가치의 저장과 이동을 문서로 저장
- 3) 지불 : 가치의 이동을 실행



Public (open) vs. Private Blockchain (closed)

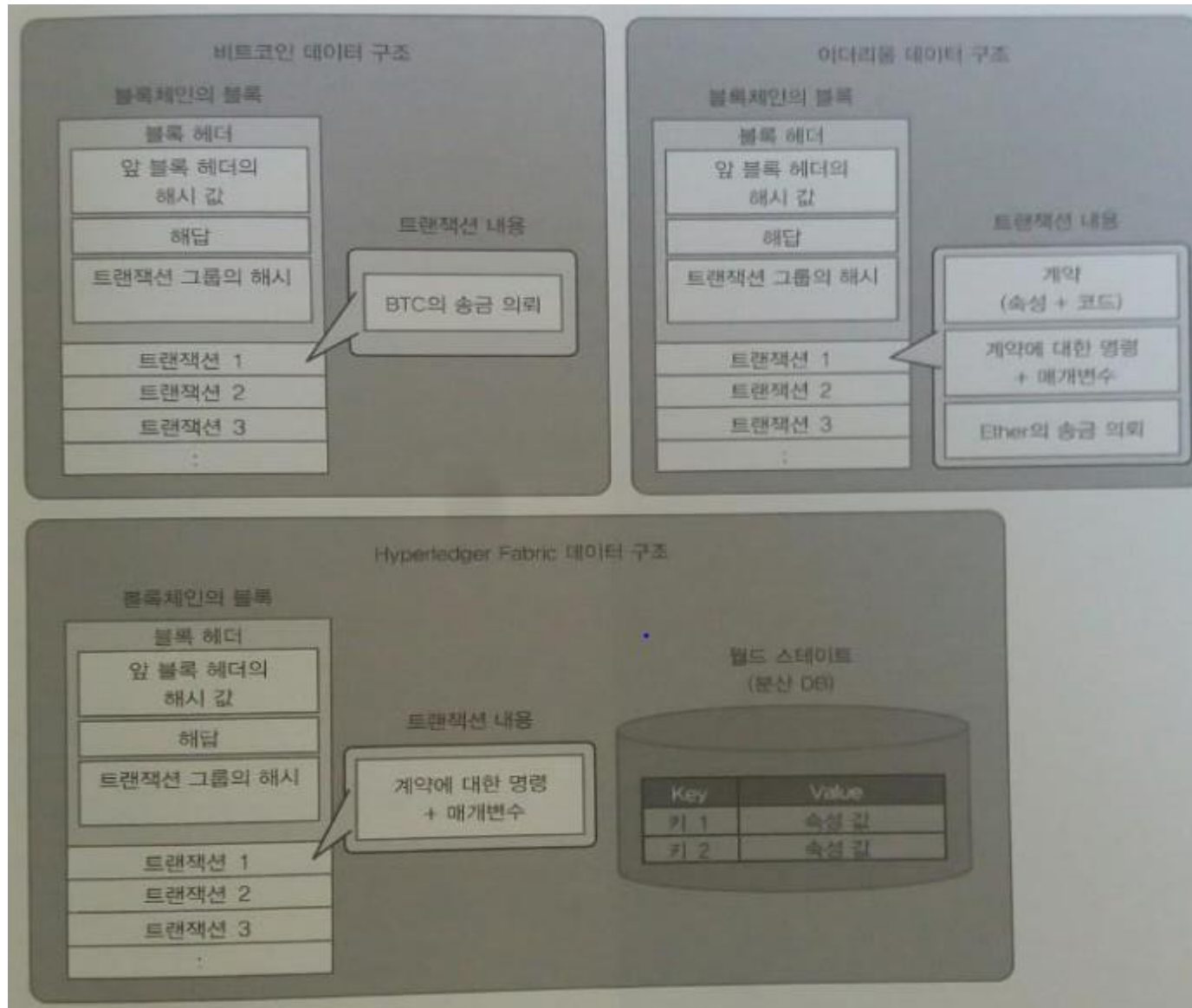
	Public	Private
Access	Open read/write access to database	Permissioned read/write access to database
Speed	Slower	Faster
Security	Proof-of-Work/ Proof-of-State	Pre-approved participants
Identity	Anonymous/Pseudonymous	Known identities
Asset	Native Assets	Any asset
Costs	Expensive	Cheaper

Finality	No	Yes
No of Min Node ¹	2	4
Data Model	UTXO ²	State DB
Anonymity (in TX)	No	Yes ³
SmartContract	Script ⁴ , Solidity ⁵	Native Code ⁶

[범례]

1.장애대응노드 1개 포함 2.집계하기 위해서 모든 블록참조 3.트랜잭션 데이터를 Pub key를 암호화가능 4.비트코인, 반복문,분기구분제한 튜닝불완전 5.이더리움 튜닝완전체 (EVM 위에서 동작) , Gas 개념 6.Python , Java , Go, 소스로부터 네이티브코드 생성 직접실행

블록데이터 구조 비교



프라이빗 블록체인에서 문제점 및 해결방향

P2P 네트워크에 대한 문제

네트워크 단절이나 공격등 안정성 문제

노드 신뢰성과 브로드캐스팅 확장성문제

전송횟수나 네트워크 지연 등 성능 문제

합의 알고리즘에 대한 문제

파이널리티 불확실성 문제

51% 문제 및 트랜잭션 생성 등
악의적참가자 문제

실시간 업무 처리 문제

보안에 대한 문제

블록체인 정보의 기밀성 문제

계정의 정당성 검증과 개인정보 문제

➤ 허가형 네트워크

블록체인 네트워크의 참가자를 관리, 신뢰된
멤버로만 구성

➤ 효율적인 합의알고리즘

PBFT 등 효율적인 합의알고리즘 채택
파이널리티의 확실성 보장, 지연 및 자원낭비
감소, 블록생성 및 검증 시간 절약

➤ 블록체인 정보암호화

거래정보나 속성정보를 공개키로 암호화
(개인키를 가진자만 접근)

➤ 인증정보 변경 (매 트랜잭션)

트랜잭션마다 인증키를 변경, 정당성보증과
개인정보보호 확보

블록체인 프로젝트 시 고려사항

경영진 의지 및 전사적 참여
(현업 Pain Point 도출)

법률문제 ex.개인정보

적용단계

처음적용해보는 기술

TFT 구성 , 사내 해커톤

TFT내에 변호사자문 포함
서비스오픈시 개인정보 위수탁동의절차

POC , 파일럿 , 확산으로 구분
*POC , 파일럿 : 사내직원이나 협력사로 국한

기획시 테스트기간 *2

끊임없는 질문 ? Why Blockchain ?

Copyright@ 2017 DAYLI Intelligence All rights reserved.

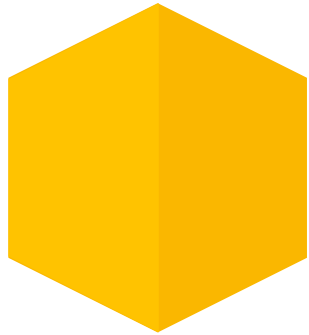
※ 양사 협력과제 발굴은 1차(6월), 2차(9월)로 진행하며, 수시발굴 작업도 병행함

6.11~6.27 (3W) 6.28~29 7.9~12

각 분과별 협력과제 Pool 도출
(우선순위 평가 포함) 도출과제
보고/리뷰 내부보고/리뷰

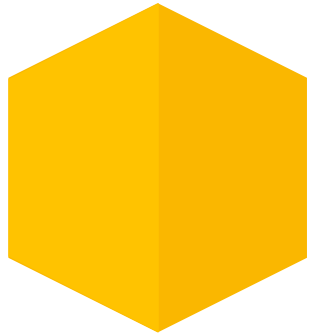
8월 4일 금요일

5. 1차 최종과제정의서 : 불독제인(1/6)[illegible]



Contents

- I. Blockchain 에 대한 오해
- II. How Blockchain
- III. Case Study**
- IV. loopchain™ & ICON™
- V. Q & A



Use Case

- I. 금융투자업권 공인인증서 대체 ‘블록체인 공동인증서’
- II. K생명, SmartContract를 이용한 자동청구시스템
- III. 계약플랫폼 : Chain Sign (SmartContract 기반 -보험 약정서)
- IV. 지불결제 시스템 ‘uCoin, 위비코인’, 지방자치 단체, 모바일 상품권
- V. 해외사례 (은행 & 혁신모델)

금투협, 세계 최초 블록체인 공동인증 서비스 오픈

입력 2017-10-31 12:01:00 | 수정 2017-10-31 12:01:00



개발을 진행해온 금투협 산하 IT위원회는 지난해 4월부터 회원사와 함께 블록체인 분과를 구성하고 기술분석, 자본시장 활용분야를 연구했다. 이후 10월에는 국내 26개 금융투자회사와 5개 기술업체가 블록체인 컨소시엄을 발족, 첫 사업으로 자본시장 공동인증 서비스 구축을 위한 양해각서를 체결했다.

김정아 금투협 경영지원본부장은 "복잡한 현재의 공인인증 제도를 블록체인 기술로 대체하면 금융소비자는 안전하고 편리한 전자금융거래 서비스를 누릴 수 있다"며 "금융회사도 적은 비용으로 보안을 강화하는 효율적 금융IT 환경이 마련되었다"고 말했다.

이어 "앞으로 채권청산결제와 장외주식거래 등에도 블록체인 기술을 적용해 금융투자업계의 디지털 혁신을 지속해 나갈 계획"이라고 덧붙였다.

'인증 한 번으로 금융투자 OK'...블록체인 공동인증서비스 오픈

송고시간 | 2017/10/31 12:00

f t v ... | 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

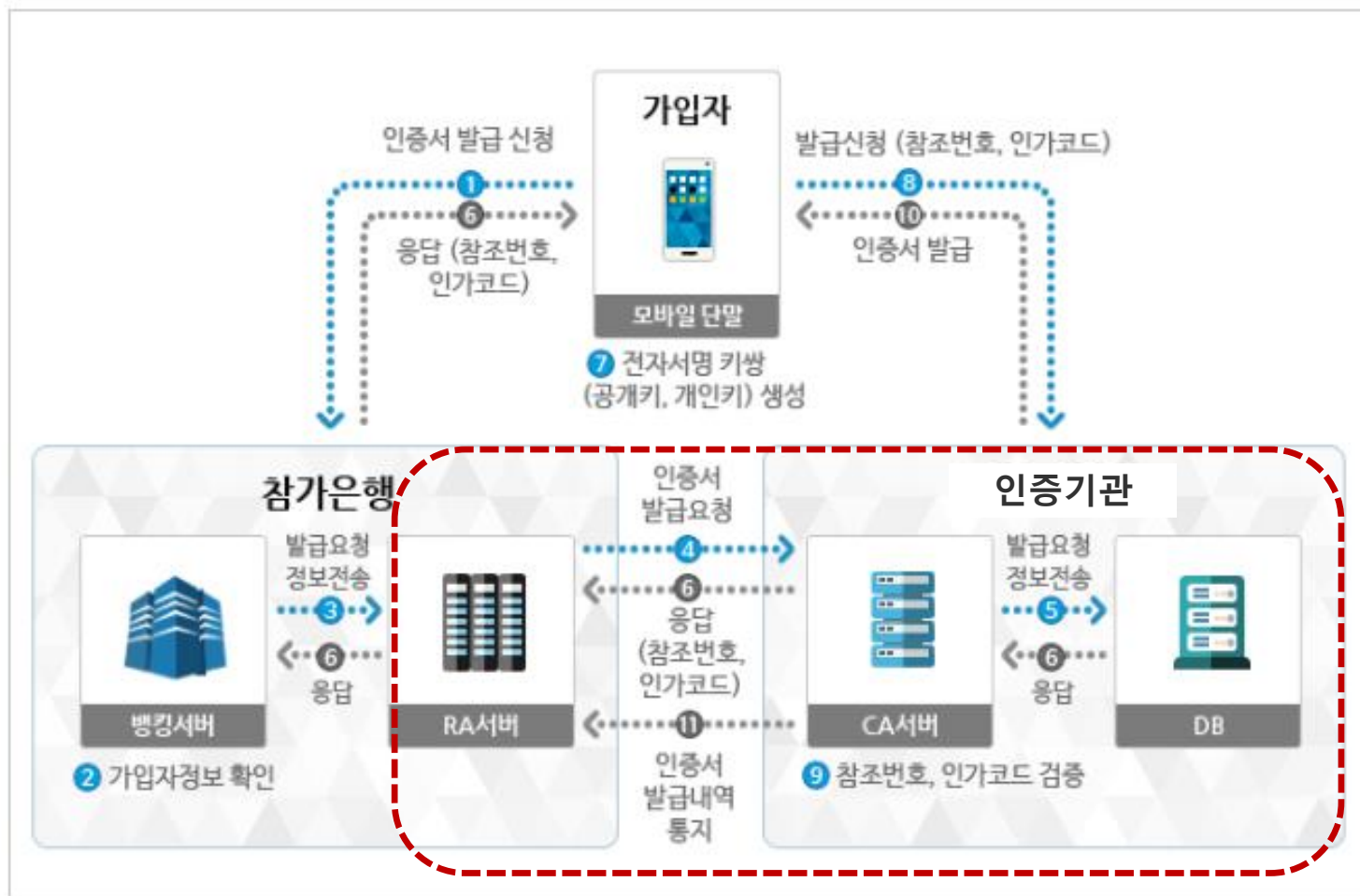
11개 증권사 참여 'CHAIN ID' 시범서비스...한차례 인증으로 여러 증권사 이용
투자자 편의성·안정성 ↑...참여회사는 비용 절감 효과



먼저 연간 수십억 원대 인증 비용이 절감된다. 증권회사에서 기존에 사용하는 인증서비스는 제3의 공인인증기관을 통해 인증이 이뤄졌다. 이때 공인인증서 발급, 해지, 정지 등 인증서 관리에 비용과 노력이 투입됐다.

이용자 입장에서 최초 인증 이후에는 타 금융기관 이용을 위한 인증서 등록과정에서 계좌 확인, ARS전화, 일회용비밀번호(OTP)인증 등 복잡한 절차를 거치지 않아도 된다.

공인인증기관, '제3자의 3자'



공인인증체계와 사설인증체계의 보안적/편의적 장점을 충분히 활용한 인증체계 구축

	공인인증서	(개별) 사설인증서	금투업권 공동인증서
발급자 (서명자)	공인인증기관 (금융결제원, 코스콤 등)	개별 금융기관	블록체인 참여사 (합의 / 공동서명)
거래가능 범위	증권거래 및 보험거래 전자정부민원서비스	W 발행기관 단독 사용	참여자 전체 (참여기관 확대에 따라 사용성 ↑)
인증서 유효성 확인	W OCSP 이용, 비실시간 CRL 폐기목록 검증 필요	내부 구축된 인증서 목록 활용	S 블록체인에 기록된 인증서 정보 활용
인증서/ 개인키 저장 위치	W 주로 디바이스의 정해진 위치(NPKI폴더)	자체 정책으로 결정 (안전한 저장공간 선택 가능)	S 물리적으로 분리된 안전한 저장공간
개인키 접근 방식	W 복잡한 PW 방식 (생체인증 추진 중)	S 생체, PIN, 패턴 등 다양한 방식 가능	S 생체, PIN, 복잡한 비밀번호 등 다양한 방식 가능

S Strong point W Weak point

블록체인 인증서비스 구현 목표

블록체인을 통해 발급된 공동인증서 사용으로 효율적, 안정적인 전자서명 체계 구축

블록체인을 활용한
“인증기관 없는”
전자서명 체계 구축



인증 시스템 효율화

- 인증기관을 통한 인증서관리 및 유효성 검증에 소요되는 리소스 절감
- 정보의 중앙 집중으로 발생하는 Risk 및 타기관 의존요소 제거



고객의 인증서 사용편의 증대

- 자체 인증정책 적용을 통한 다양한 편의요소 제공
- 참여기관 지속적 확장을 통한 사용성 확대



블록체인 네트워크 활용 사업영역 확대

- 향후, Trading 영역에 블록체인을 적용할 인프라 선구축 및 블록체인 기술 관련 사전학습효과 기대
- 본인확인 서비스제공 등 추가 사업기회 발굴

II. 공동인증 주요특징 및 정책



금융투자업권 공동인증 app 구축

참여사간 공동인증 Application 구축으로 기존 인증기관이 제공 중인 서비스 완전대체 및 다양한 기능 제공

APP 역할

- ✓ **키쌍 생성**
단말 소유자의 공개키와 개인키를 생성하고 인증서 발급을 요청
- ✓ **인증서 관리**
블록체인에서 발급된 인증서 저장 및 관리
- ✓ **전자서명생성**
MTS의 요청에 따라 개인키로 서명하여 전자서명을 생성

금융투자업권 공동인증 App 구축



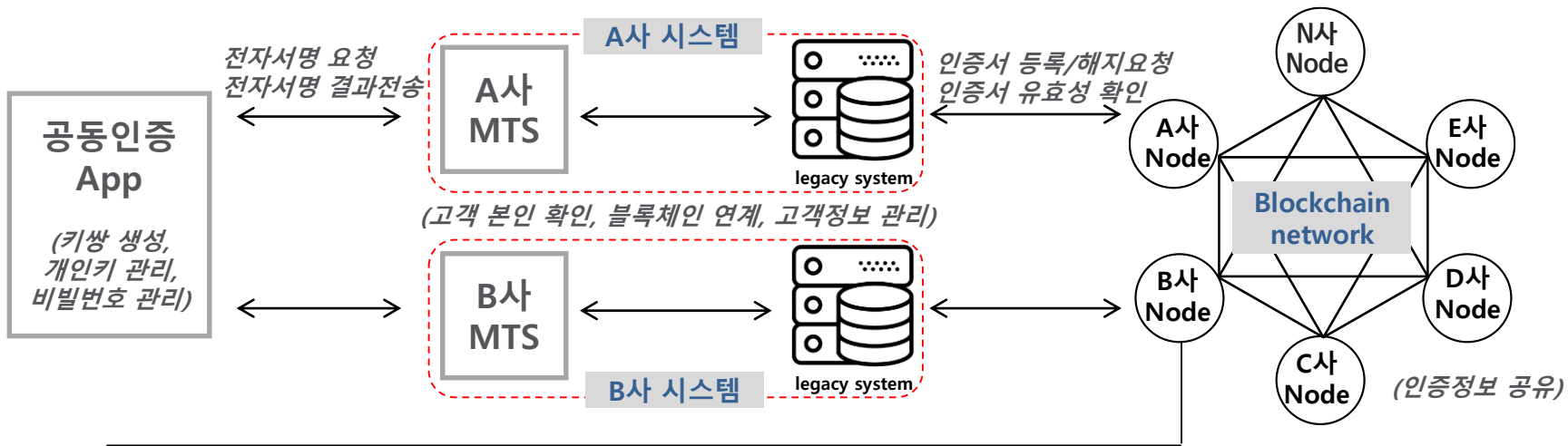
APP 특징

- ✓ **개인키의 안전한 관리**
모바일 디바이스의 안전한 저장 공간에 개인키 저장
- ✓ **다양한 개인키 접근방식 기능**
모바일 디바이스의 각종 생체 인식 기능을 활용한 생체인증 서비스 제공
- ✓ **MTS와 유연한 연계**
인증서 등록, 인증서 사용 등 모든 고객 접점에서 자연스러운 app간 연동 구현

공통인증 서비스 구조

[공통인증 app ↔ MTS ↔ legacy ↔ 블록체인]의 단계적 연동구조로 유기적 인증시스템 구축

서비스 구조



블록체인 노드의 구성



금융투자업권 공동인증 특징 - (1) 다중요소 인증체계 확보 개념

인증의 Factor 로는 크게 3가지가 있으며 금융거래에서는 2가지 이상의 Factor를 결합하여 인증을 강화

지식기반 인증

사용자와 서버가 미리 설정하여
공유한 비밀 정보를 기반으로
사용자 인증

ID / PW 인증, 질문-응답 확인

- 별도의 하드웨어 불필요 : 운영비용 低
- 인증강도가 낮아 보안에 취약

소유기반 인증

약속된 인증토큰의 소유를
전제로 인증

One Time Password

- 1회 이상의 대면을 통한 본인확인 필요
- 인증토큰을 늘 소유하여야 하는 불편

특징기반 인증

인증자에게 귀속된 고유한 형태의
신체구조 또는 행동결과를
기반으로 인증

지문, 홍채, 걸음걸이, 서명필압

- 생체구조의 패턴의 분석과 활용을 위한
시스템구축비용 高
- 생체정보의 훼손 시 문제 발생

다중
요소
인증

인증기술요소 중 2개 이상의 요소를 결합하여 인증체계를 구축한 경우
다중요소인증(Multi Factor authentication) 으로 인정됨

- ATM 이용 : 체크카드(소유) + 비밀번호(지식)
- 인터넷뱅킹 : 계좌번호/계좌비밀번호(지식) + OTP(소유)

금융거래 등에서 보안 강화를 위해
다중요소 인증을 사용함

금융투자업권 공동인증 특징 - (1) 다중요소 인증체계 확보 적용

스마트폰, 태블릿PC 등 개인이 소유한 모바일 단말 단위로 인증서를 발급하고 해당 device만 인증가능하도록 설정하여 안전하고 편리한 인증 체계 구축



모바일 단말기의 안전한 공간에 개인키 저장

- ✓ 최근 생산된 스마트 기기에는 생산당시부터 물리적으로 분리된 안전한 저장공간이 존재(EX : TEE)
- ✓ 구형기기의 경우 분리된 저장공간이 없어도 허가된 app만 접근가능한 데이터 영역 구성 가능
- ➔ 외부의 접근이 불가능한 영역에 개인키를 저장하여, 개인키의 유출가능성 사전봉쇄

다양한 개인키 암호화 방식 제공

- ✓ PIN 방식 : 6자리 숫자, '간편비밀번호'라는 이름으로 상용 중
- ✓ PW 방식 : 공인인증서와 같이 영문/숫자/특수문자를 복합한 암호 설정으로 유출 가능성 하향
- ✓ BIO 방식 : 각 Device에서 제공하는 생체인식 기능을 개인키 암호로 활용

* 기타 정책에 따라 다양한 방식 추가 가능

금융투자업권 공동인증 특징 - (2) 타기관인증서 자동등록

공동인증 참여기관간 고객의 인증정보를 공유함으로써 타사에서 인증서를 발급받은 고객이 당사에 최초로 인증서 사용을 원할 경우 간단한 고객확인 후 사용 가능

자동등록 Process

- 금융기관은 고객확인(ID/PW 로그인, 계좌번호 확인 등) 절차로 고객 식별
- 식별된 고객정보로 BID를 추출하여 블록체인에 정보와 mapping



각 주체별 보유정보



* BID : Blockchain ID, 비식별화 된 개인 고유의 값
 ** DN은 공동인증 사용고객인 경우에 한해 저장할 수 있음

■ 블록체인에는 인증서 사용을 위한 최소한의 정보만 저장하며 인증서 사용에 개인정보는 불필요

금융투자업권 공동인증 특징 - (3) 인증서비스 주요 운영 정책

업권 담당자로 구성된 비즈니스 분과에서 고객 편의와 보안적 요소를 고려한 공동인증 정책 수립

인증서 유효기간



✓ 인증서 유효기간 3년

* 인증서의 유출/이동 가능성은 없으나, 고객의 단말기 분실/변경 사유는 발생 가능하므로 단말기 변경주기와 비슷한 기간인 3년으로 설정

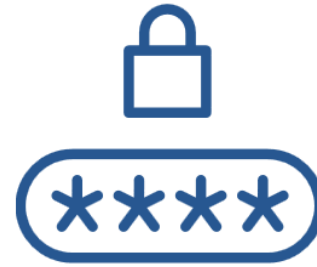
단말기 등록대수



✓ 1인당 5개의 단말기 등록 가능

* 다수 단말기를 사용하는 고객의 편의를 위하여 총 5개의 단말기 등록허용
* 1단말기에 1명의 인증서만 등록

비밀번호 오류 정책



✓ 비밀번호 체크, 오류횟수 관리는 공동App이 수행

* 인증 암호는 공동app이 관리하며, 5회 오류시 해당 사용 정지 처리(인증서폐기)
* 지문인증 5회 오류는 지식기반 인증을 통해 초기화 가능

인증서 폐기



✓ 만료/해지된 인증서를 동일 단말기에서 사용하려면 재등록

* 인증서 유효기간 연장, 인증서 초기화 등의 프로세스 대신, 등록된 인증서의 사용 중단이 필요할 경우 기존 인증서 삭제
* 인증서의 재사용처리가 필요할 경우 단말기 등록절차 필요

공공인증 VS 공인인증 비교

각종 편의적 보안적 요소에서 대체로 공인인증보다 우위에 있거나 비슷함

구분	category	공동인증	비교	공인인증(증권전용)
사용가능 기관	편의	블록체인 참여사	<	온라인증권거래 및 보험거래 전자정부민원서비스
타기관 등록절차	편의	간단한 고객확인 후 가능	>	계좌확인, ARS인증, OTP인증 등 복잡한 절차
발급절차	편의	공인인증과 동일한 프로세스로 진행	=	본인확인 (계좌번호, 계좌비번 등 확인)
부인방지	보안	가능	=	가능
개인키 저장공간	보안	TEE 또는 앱 영역 (모든 단말기 가능)	>	지정된 경로(파일)
개인키 접근가능여부	보안	불가	>	가능
유효기간 정책	편의/보안	3년	>	1년
개인키 암호화 방법	편의/보안	PIN/PW/BIO 등 다양	>	PW
개인키 암호 오류대응정책	편의/보안	인증 app이 비밀번호 통합 관리함 → 사용 시도한 금융기관에 상관 없이 총 오류횟수가 임계치에 도달하면 인증서 사용 불가처리	>	개별 금융기관에서 관리
인증서 유효성 확인 Process	편의	각 사의 Node에서 확인 가능	>	외부기관과 I/F 필요(OCSP) CRL 폐기목록 확인(비실시간)

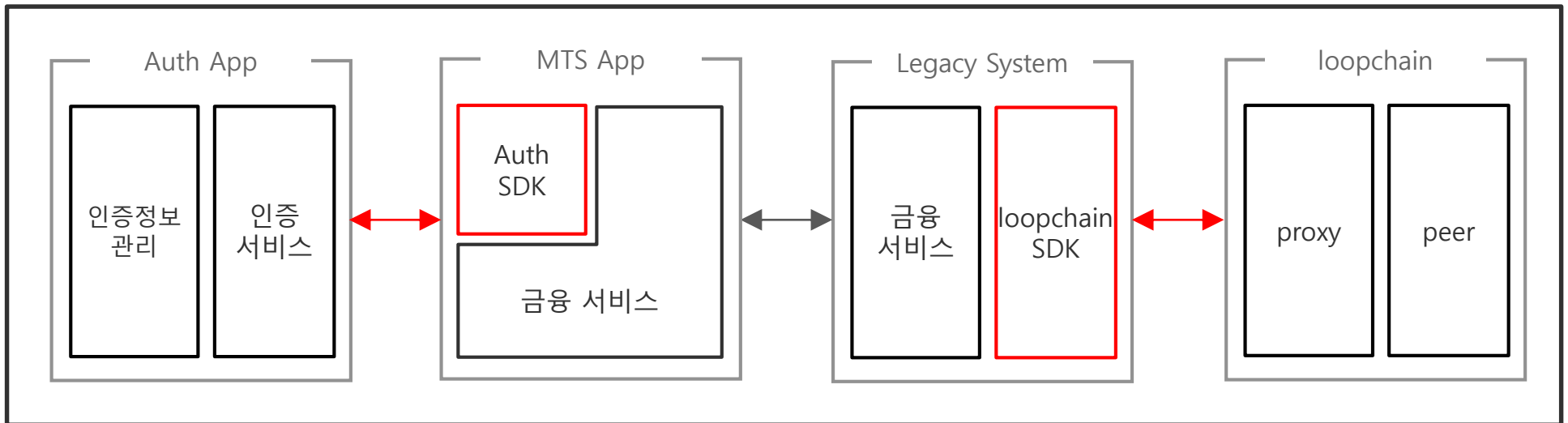
I. 공동인증(CHAIN ID) 프로세스

- 인증서 발급
- 인증서 로그인
- 인증서 해지/파기



공동인증 SDK 구성

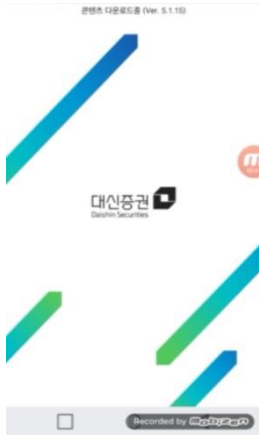
- 금융서비스 서버와 루프체인간 통신을 위한 loopchain SDK와 MTS앱과 공동앱간 통신을 위한 Auth SDK로 구성



I. 공동인증(CHAIN ID) 프로세스

인증서 발급 (스크린샷)

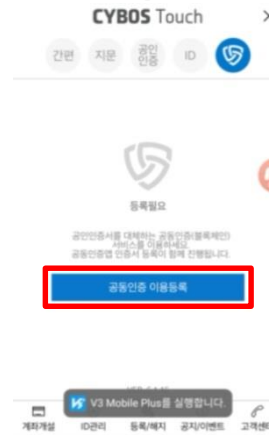
①A사 MTS 로그인 (공동인증)



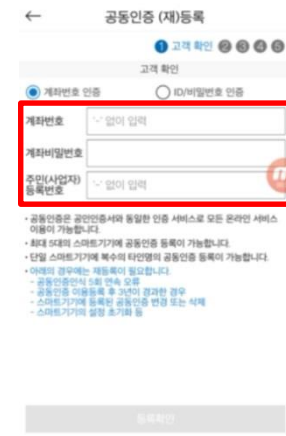
②CHAIN ID 실행 (연동)



③공동인증서 발급요청



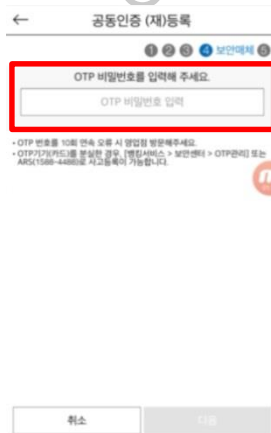
④계좌정보 입력



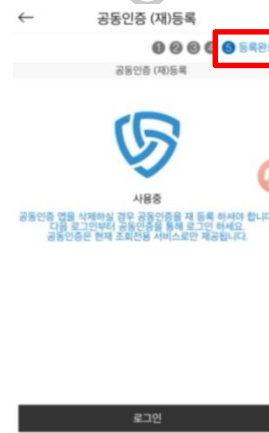
⑤ARS 전화인증



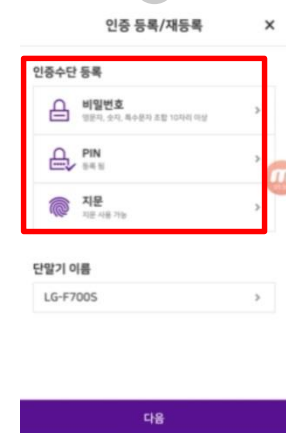
⑥OTP 인증



⑦인증서 등록완료



⑧개인키 등록 신청



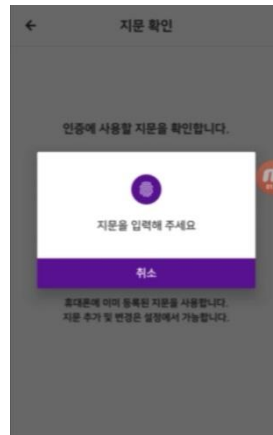
I. 공동인증(CHAIN ID) 프로세스

인증서 발급 (스크린샷)

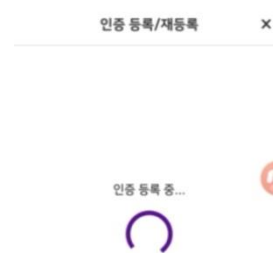
⑨PIN번호 등록



⑩지문 등록

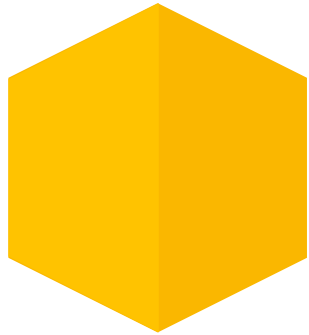


⑪개인키 등록



⑫발급 및 등록 완료





Use Case

- I. 금융투자업권 공인인증서 대체 ‘블록체인 공동인증서’
- II. K생명, **SmartContract**를 이용한 자동청구시스템
- III. 계약플랫폼 : Chain Sign (SmartContract 기반 -보험 약정서)
- IV. 지불결제 시스템 ‘uCoin, 위비코인’, 지방자치 단체, 모바일 상품권
- V. 해외사례 (은행 & 혁신모델)

[리빌딩 파이낸스 2017]서류없이 블록체inser 원스 톱 처리...실손 보험금도 자동으로 입금 가능

교보생명 연내 세계 첫 서비스
보험산업 효율성·신뢰도 제고
해외선 재보험사 중심 표준화

서울경제

정영현기자 | 2017-08-24 18:22:57 | 보험카드



Case : K생명. 스마트청구



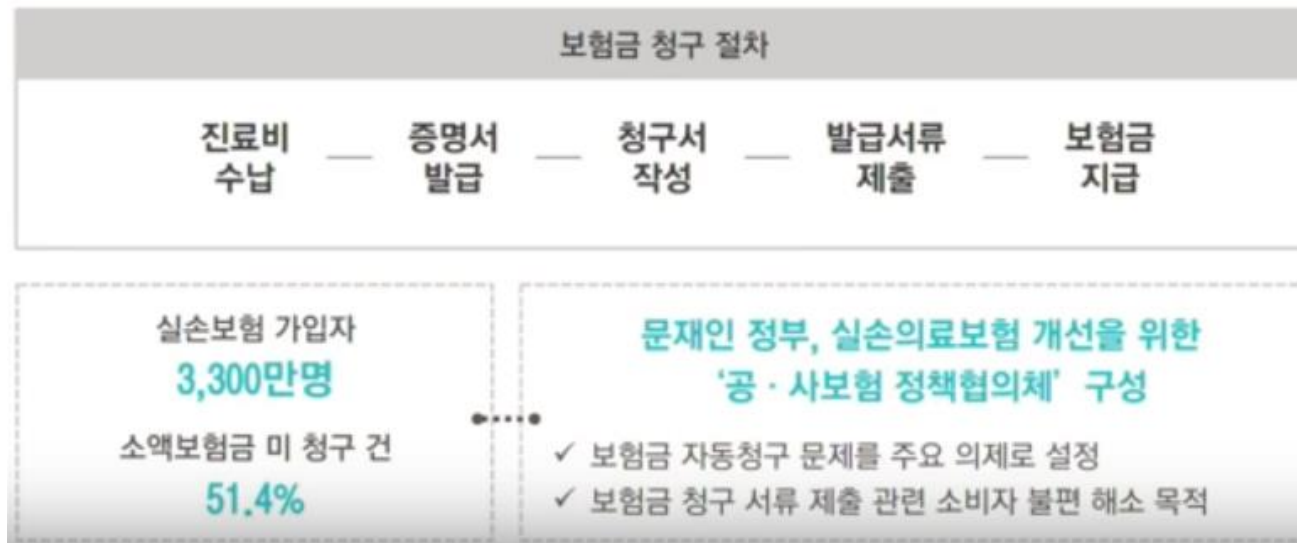
요즘 글로벌 보험시장에서 교보생명이 굉장한 관심을 불러모으고 있다. 세계에서 처음으로 블록체인 기술을 상업보험료 지급결제와 연결하는 '실험'에 나섰기 때문이다. 외신까지 교보생명 사례를 다룰 정도다. 블록체인 기술의 성공 여부에 따라 한국 보험사들도 글로벌 시장을 선도할 가능성을 엿볼 수 있는 단적인 사례다.

24일 금융권에 따르면 교보생명은 지난 4월 정부가 주관하는 사물인터넷(IoT) 활성화 기반 조성 블록체인 시범사업에 컨소시엄으로 참여해 사업자로 최종 선정됐다. 컨소시엄에는 인슈어테크 전문기업 '디레몬', 블록체인 기술기업 '더루프', 병원 의무기록 서비스 기업 '원'이 참여했다. 이들이 구현할 핵심 기술은 블록체인과 IoT 간편인증 기술을 활용해 보험계약자에게 실손보험금 등 소액 보험금을 자동 지급하는 서비스를 제공하는 것이다.

Case : K생명. 스마트청구

Pain Point ❖ 소액보험금 미청구 건 51.4% (국정감사)

“복잡한 보험금 청구절차에 대한 개선요구 증대”

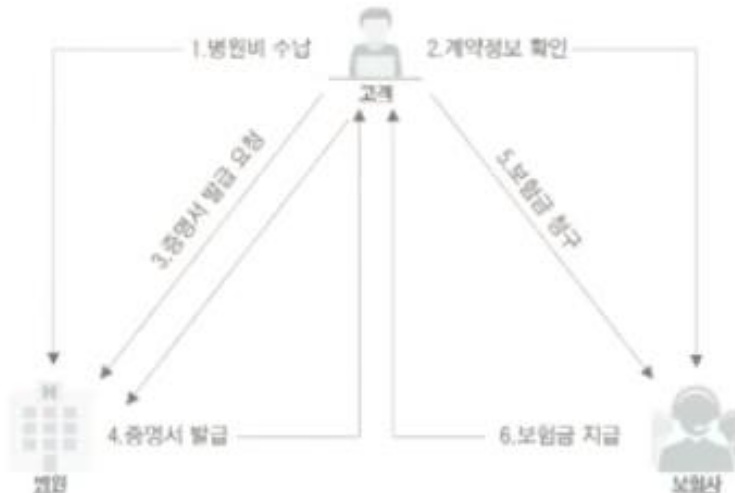


Case : K생명. 스마트청구

타권역간에 사용된 최초의 블록체인기반 공동인증 (보험 <> 병원)

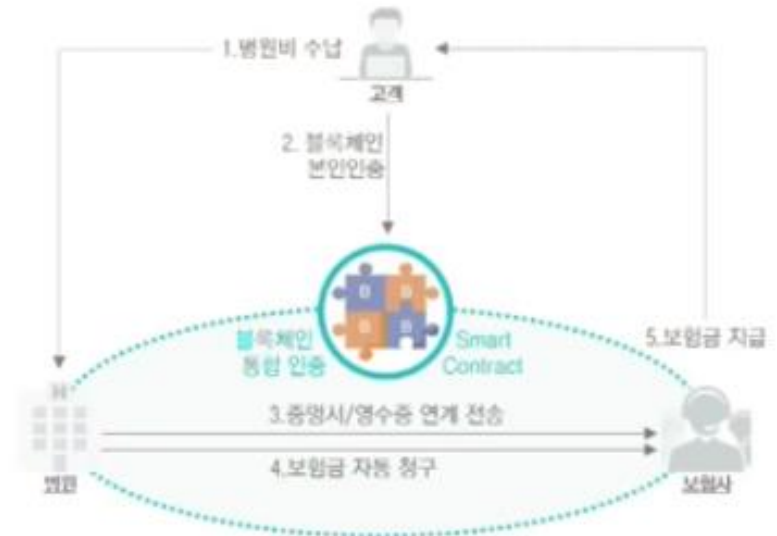
As-Is

보험금 청구를 위해
고객의 복잡한 절차 수행 필요



To-Be

블록체인 기술 적용으로
고객의 보험금 자동 청구 실현



Case : K생명. 스마트청구

■ Service Flow

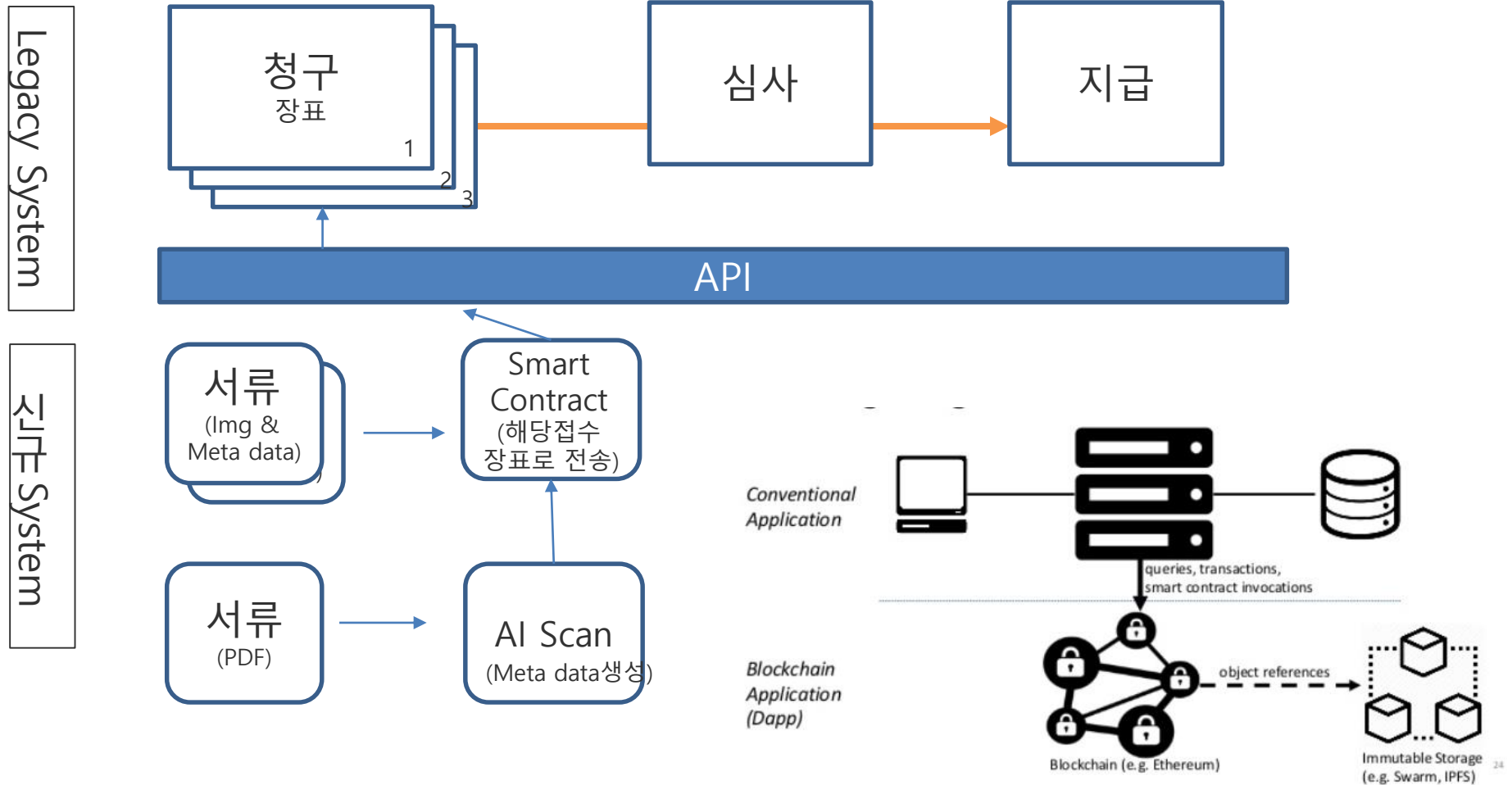


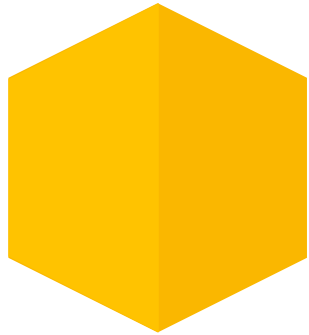
Case : K생명. 스마트청구

■ Service Flow



Case : K생명.확대





Use Case

- I. 금융투자업권 공인인증서 대체 ‘블록체인 공동인증서’
- II. K생명, SmartContract를 이용한 자동청구시스템
- III. 계약플랫폼 : Chain Sign (SmartContract 기반 -보험 약정서)**
- IV. 지불결제 시스템 ‘uCoin, 위비코인’, 지방자치 단체, 모바일 상품권
- V. 해외사례 (은행 & 혁신모델)

Case : 계약플랫폼

www.chainsign.co.kr

Chain SIGN

서비스 소개

법적효력

FAQ

사전에약

Service Introduction

서비스 소개



문서관리 전문회사인 (주)사이버다임과 블록체인 플랫폼 전문회사인 (주)더루프가 함께 만든
최초의 블록체인 기반 계약 플랫폼.

기존의 전자계약 시스템에 블록체인 기술을 활용하여 신뢰를 추가하는 새로운 ‘계약 플랫폼’입니다.
기존 전자계약의 <공증>에 준하는 효과를 가질 수 있습니다.

	기존 전자계약	Chain SIGN
구성요소	서버, 사설인증서, 전자계약	블록체인 노드, 공동인증서, 전자계약
플랫폼 기술	Client Server 프로그램	블록체인
보안성	시스템 제공자와 계약자 중 한 측이 합의하면 쉽게 조작 가능	임의적 조작 불가, 신뢰성과 보안성 증대
공증	공증에 대한 신뢰 부족	*저렴한 공증효과 ¹⁾
연속성	시스템 장애시 서비스 중단 (Single Point)	무정지 시스템 구현 가능 (Oracle RAC 동일 효과) 임의적 조작이 불가능
인증매체	법인 인증서 및 사설 인증, 개인인증	*차세대 인증 시스템 통합 (생체인증+블록체인) 18년 하반기 적용 예정

1) 다수의 참여자가 진위를 동일한 절차에 의해서 증빙할수있으면 공증의 효과에 준한다. (법해석. 법무법인)

* 는 2018년 하반기 적용 예정



서울 핀테크랩 이색 현장, 종이 대신 블록체인으로 '업무협약'

발행일 : 2018.04.04



<박원순 서울시장(왼쪽 네번째)과 김기식 금융감독원장(왼쪽 세번째), 핀테크랩 참여기관이 국내 최초로 블록체인 기술을 활용해 업무협약을 체결했다.>

이 날 개관식에서는 국내 최초 블록체인 기술을 활용한 업무협약을 체결했다. 태블릿PC를 활용해 종이 서류에 서명하지 않았다. 블록체인 기술과 전자계약 플랫폼을 활용한 전자서명 방식으로 진행했다. 박원순 서울시장과 국내 파트너 기관 대표 33명이 동시에 전자서명을 했다.

Pain Point

- 1.서울시 첨단 핀테크도시의 이미지
- 2.다자간의 계약, 대표자를 설정하기가 곤란
시장님 31번의 날인이 필요



**Blockchain기반의
전자계약서
"블록체인, 공증을 대체하다"**



서울 핀테크 파트너스 협약식

2018. 4. 3 서울 핀테크 랩

Block17
Block18
Block19

파트너사	협약서 해위	제경상항	파트너사	협약서 해위	제경상항	파트너사	협약서 해위	제경상항
서울특별시	bf1967...	✓	스위스위리러투자진흥원	28269f...	✓	포스코기술투자	94e76...	✓
금융감독원	5c665c...	✓	스파크랩	12361...	✓	하나금융데이터	7e0c70...	✓
농협중앙회	0be88...	✓	시제스파트너스	d5b7c...	✓	한국투자파트너스	87e5c9...	✓
대일리금융그룹	95c063...	✓	신원투자시스템	acd9a...	✓	한국핀테크산업협회	24cd7...	✓
대일리벤처투자	a080d...	✓	안전회계법인	b7053...	✓	Company B	05c2e1...	✓
롯데백화점캐이티	664f9c...	✓	엘스톤	ae78f5...	✓	KAIST융합교육연구센터	1397e...	✓
법무법인 비트	4cd47...	✓	우리은행	70c46f...	✓	KB금융지주	2c0460...	✓
법무법인 상상	b01b7...	✓	주한호주무역대표부	0ef907...	✓	L&S벤처캐피탈	3e5c3e...	✓
법무법인 플랜	dc67e...	✓	캡스톤파트너스	6a9c09...	✓	Wework	2f2379...	✓
벤처스캐어	00fbd...	✓	코스콤	e95a5...	✓			
비즈니스	0a144...	✓	우공	835d0...	✓			

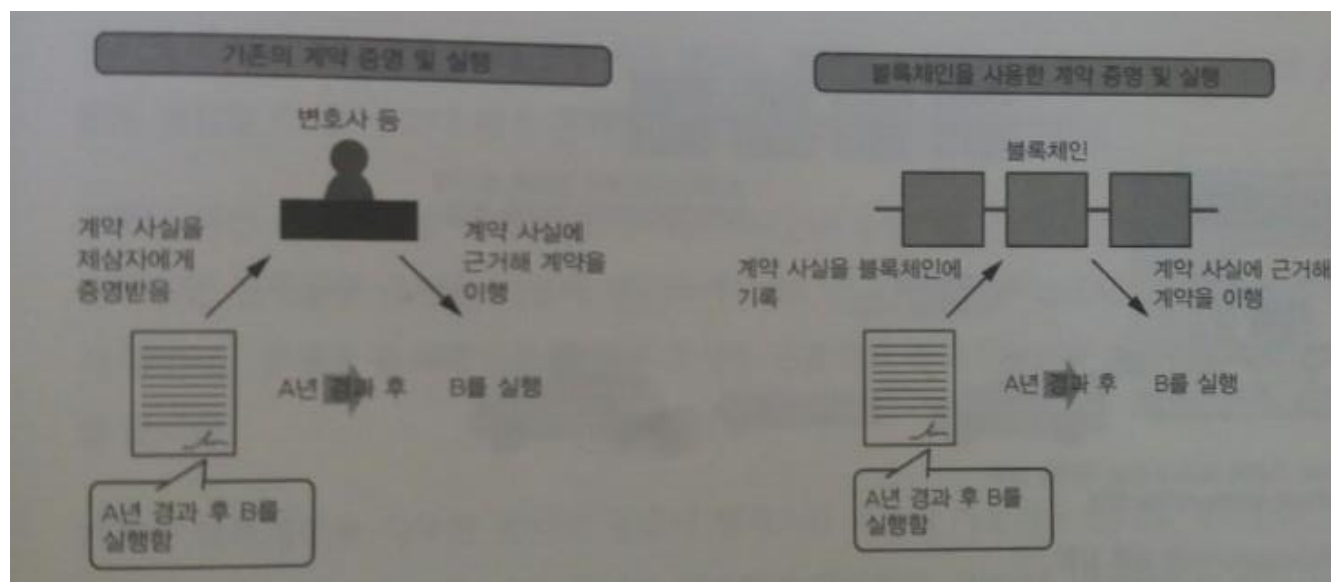
Chain SIGN © 2018 FINTECH LAB SEOUL. All Rights Reserved.

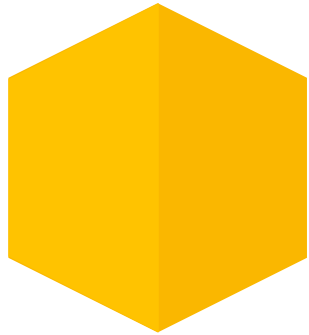


Case : 계약

■ 미래발전모델

- ❖ '공증' 기능을 가진 전자계약
- ❖ 조건에 따른 자동실행
- ❖ ' Smart Contract '를 이용한 계약의 조건에 따라 계약 이행
- ❖ ' Smart Contract '를 활용 , ESCROW 기능 제공
- ❖ ' On chain payment'를 이용한 계약의 자동집행
- ❖ 사회적인 문제인 연쇄부도 방지
- ❖ 계약과 연계된 다양한 금융연계 간소화





Use Case

- I. 금융투자업권 공인인증서 대체 ‘블록체인 공동인증서’
- II. K생명, SmartContract를 이용한 자동청구시스템
- III. 계약플랫폼 : Chain Sign
- IV. 지불결제 시스템 ‘uCoin, 위비코인’, 지방자치 단체- 모바일 상품권**
- V. 기타 : 물류, 투표시스템

서울경제

우리銀, 디지털화폐 '위비코인' 발행...'한국판 비트코인' 만든다

블록체인 기반 연내 발행
대학·지자체 등 중심 사용 확대

김보리 기자 | 2017-08-16 18:13:17 | 금융정책



가 가



16일 우리은행 중구 본점에서 열린 '우리은행 데일리인텔리전스 더루프와 블록체인 및 디지털 화폐 사업협력을 위한 업무협약식'에서 조재현(가운데) 우리은행 디지털금융그룹장이 이경준(왼쪽) 데일리인텔리전스 대표이사, 김중철 더루프 대표이사사와 기념촬영을 하고 있다. /사진제공=우리은행

우리은행 디지털화폐

디지털화폐명 위비코인(가칭)

기술방식 폐쇄형 블록체인 기반
선불 전자지급수단 방식

사업 일정

- 1 → 2 → 3
- 1 우리은행 직원거래로 디지털화폐 기술 검증 (발행, 충전, 결제, 송금)
- 2 우리은행 거래대학으로 디지털화폐 사용 확대
- 3 지자체 등으로 전자화폐 연계 추진



암호화폐 자판기 서강대에 국내 최초 등장

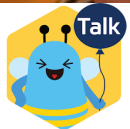
중앙일보 | 2017.12.26 17:14



중앙일보



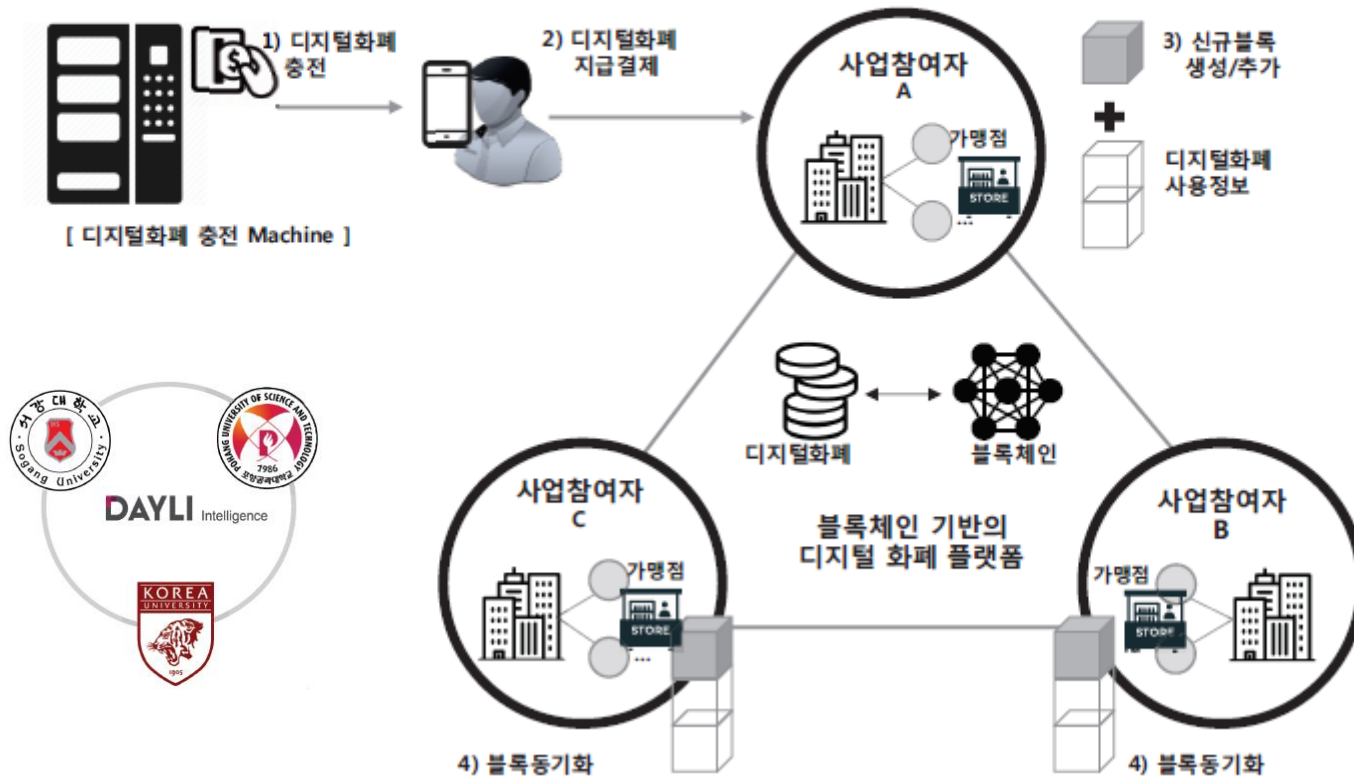
암호화폐로 물건을 살 수 있는 스마트 벤딩 머신. [사진 데일리인텔리전스]



Case : 지불결제.대학화폐 (uCoin),지자체 모바일상품권

블록체인 기반 디지털 화폐 플랫폼 서비스 구조

- 디지털화폐는 스마트컨트랙트를 기반으로 발행되고 사용자는 디지털화폐를 충전하여 가맹점에서 사용
- 거래장부 역시 블록체인 기반으로 관리되어 부인방지 및 이중지불방지 등 디지털화폐에 필수적인 보안성 확보



Refer: NIA workshop 2017

Benefit



**Cash flow ,
Local economy promotion**



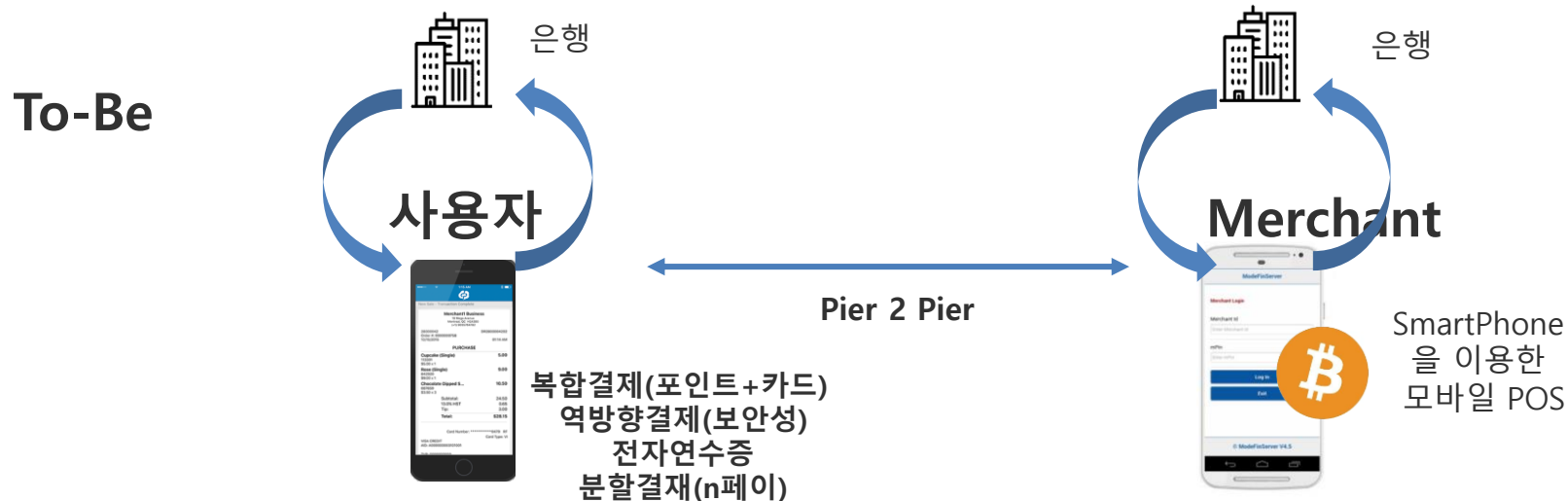
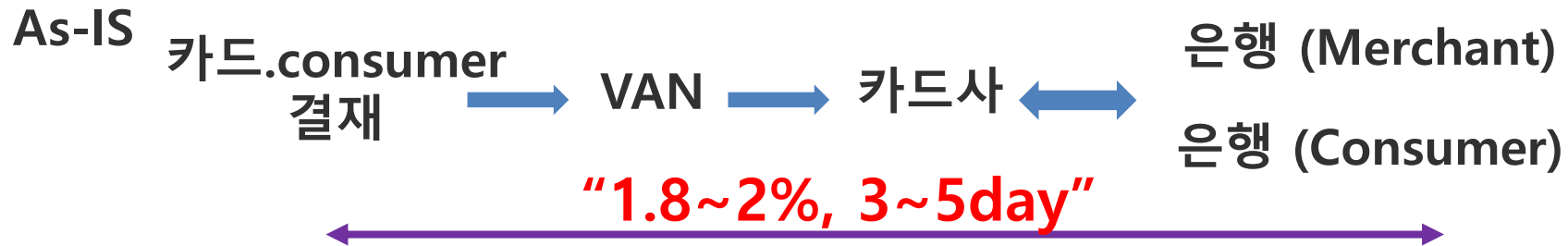
**Convenience, Easy Transfer,
Extra bonus**



**No credit card fee , POS / VAN less
Daily settlement**

Case : 지불 결제 vs 카드

카드 (Middle man)



서비스 화면



< '서강코인' PoC 현장 >

지방자치단체 전자상품권 필요성



지방공무원 신규 복지수당, '고향사랑 상품권'으로 지급

송고시간 | 2017/09/14 14:00



고향사랑 상품권은 1999년 강원 태백출남 예산경북 고령 등 3개 지자체를 시작으로 현재 전국 56개 지자체에서 발행하는 상품권이다.

변성완 행안부 지역경제지원관은 "인구 과소지역 등 일선 시군에서 고향사랑 상품권을 이용해 골목상권 등 서민경제 활성화를 추진할 수 있도록 적극적으로 지원하겠다"고 말했다.

KDI 경제정보센터

고향사랑 상품권으로 결혼식 축의금까지?

행정안전부 지방재정경제실 지역경제지원관 지역금융지원과 | 2017.09.15 | 3p | 보도자료

행정안전부는 14일 정부서울청사에서 일선 시군 등 지자체를 대상으로 「고향사랑 상품권 설명회」를 개최하여 행안부의 '고향사랑 상품권 지원 방안'을 설명하고 우수 지자체 사례를 확산하는 시간을 가졌다고 9.15.(금) 밝혔다.

- 이날 설명회는 '신규 도입 복지수당과 복지포인트의 30%를 고향사랑 상품권으로 지급할 수 있도록 해 골목상권을 활성화'하자는 국정과제의 일환으로, 최저임금 인상에 따른 소상공인·자영업자의 부담을 완화하고 지역경제 활성화를 제고하기 위해 마련되었음.

- 설명회에서는 '고향사랑 상품권의 의미'에 대한 전문가 교육을 시작으로 춘천시·양구군·나주시 우수사례 소개 등이 진행되었음.

- 이어 행안부는 '고향사랑 상품권 지원 방안'을 설명하였는데, 방안에 따르면 은누리 상품권 뿐 아니라 고향사랑 상품권으로 지방공무원 복지 포인트를 30%까지 지급할 수 있도록 「지방공무원 맞춤형 복지제도 운영기준」을 개정하는 한편, 지자체 재량에 따라 '아동수당' 등 신규 도입 복지수당을 고향사랑 상품권으로 지급할 수 있도록 지원할 계획임.

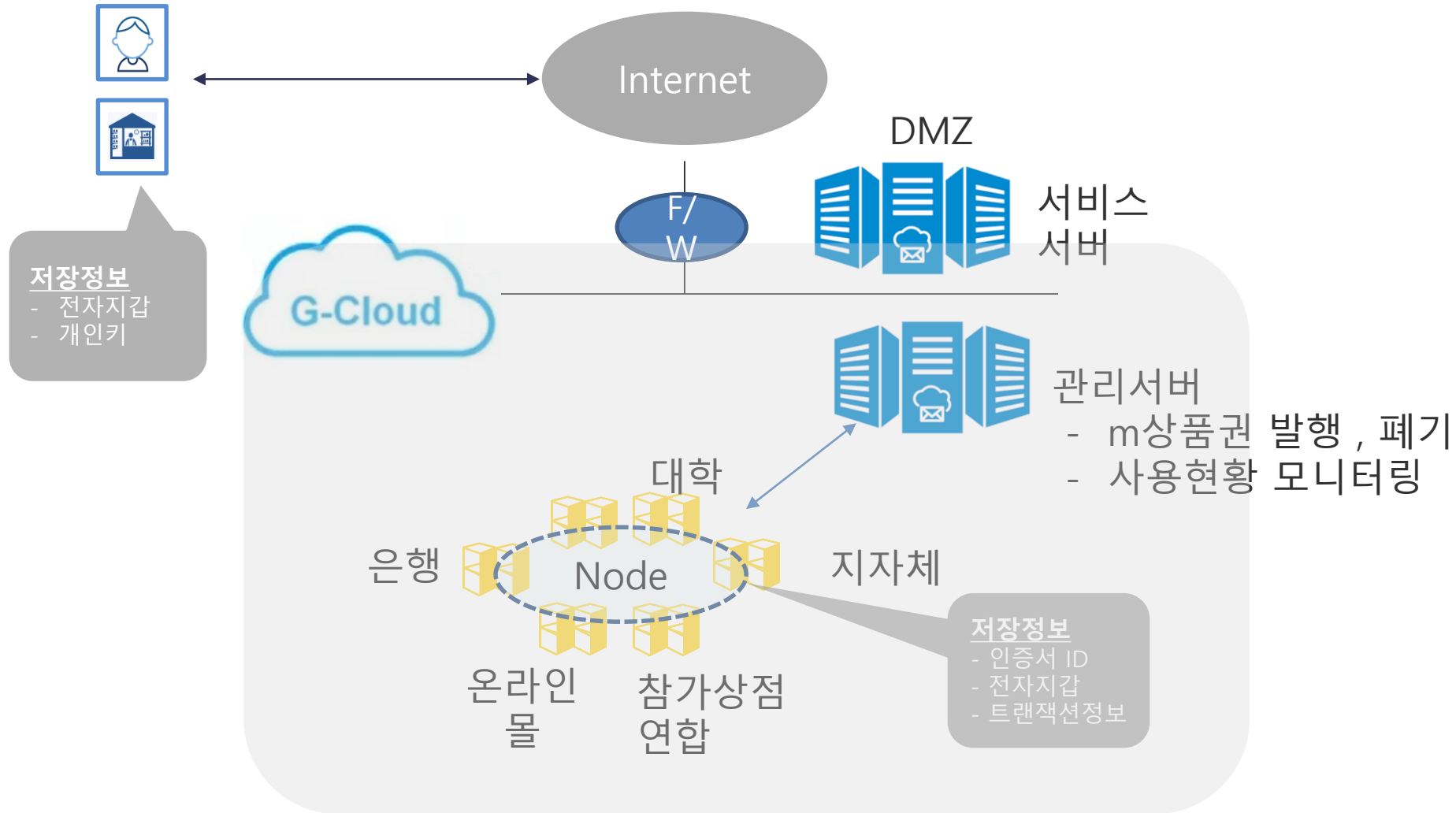
고향사랑 상품권

발행 및 운영 안내서

2017. 9.



지자체 모바일상품권 시스템 구성도



혜택



지역경제활성화

- 자금의 관외유출 방지
- Commerce platform 연계 시 시너지 극대화



모바일 결제 - 편리성, 보안성, 보너스

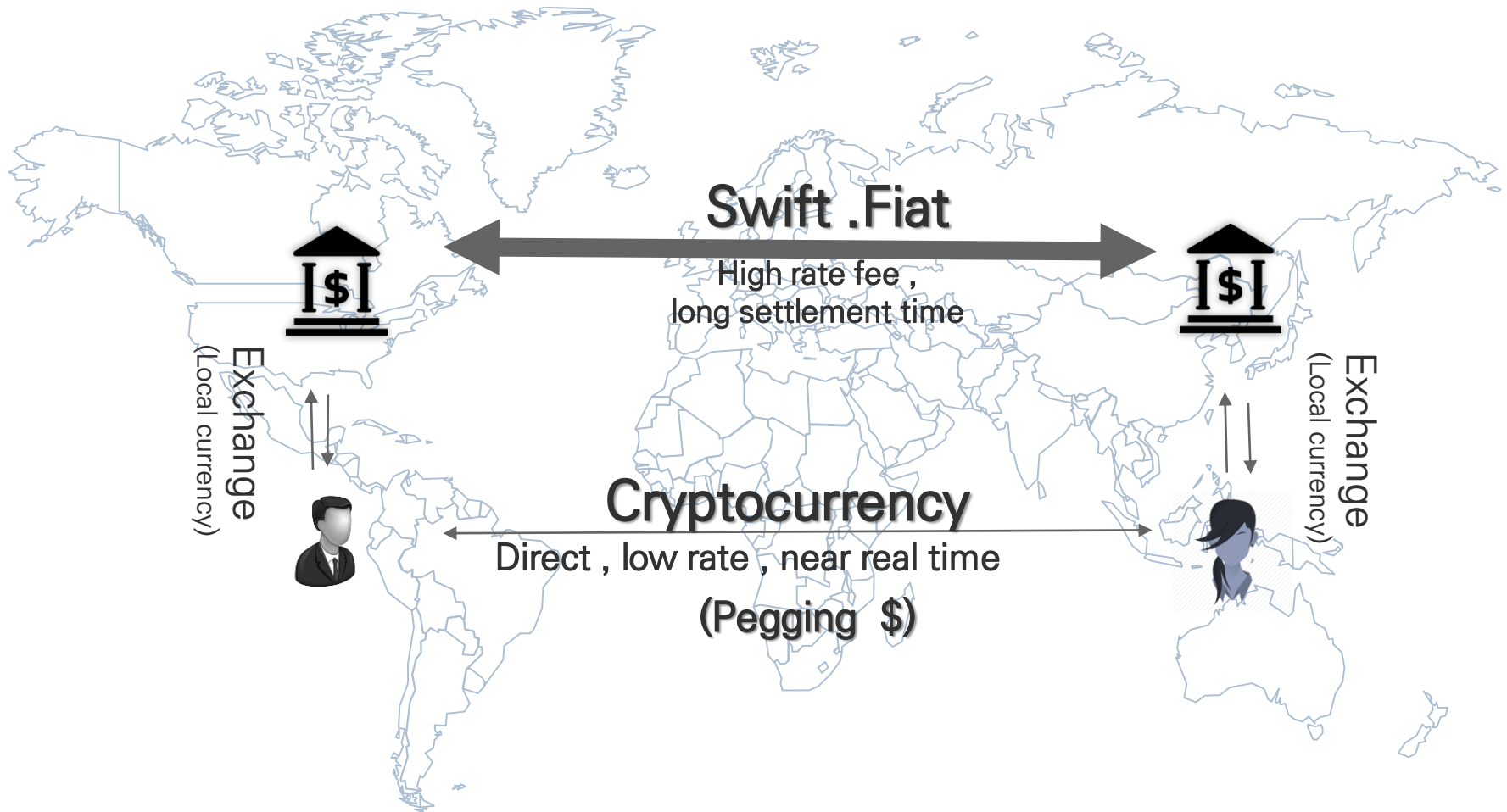


수익률 상승 - 지금결제에 대한 수수료 '0'에 수렴' Daily settlement - 운전자금 감소효과



안정적 수신고 - 이탈률이 낮은 자금확보 계좌증가 - 가맹점 확대 (VAN less) 상품개발 - micro credit상품 (50만원이하)

Swift 대체

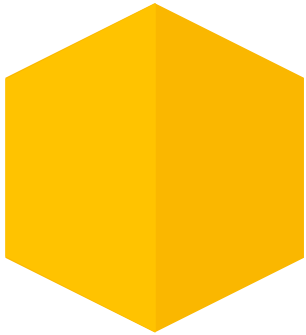


Case : 지불

■ 미래발전모델

- ❖ 모바일폰을 이용한 간편결제 확산
- ❖ '지불결제 중간자 대체 (카드, VAN, POS system 등)
- ❖ 복합결제 (포인터 지불 → 잔금결제 →포인터적립)
- ❖ 특정영역에서 블록체인기반 Private Coin 사용활성화
ex. 지역화폐, 복지코인, 교통코인 등
- ❖ 법정화폐는 Private Coin 의 정산에 활용

Use Case



- I. 금융투자업권 공인인증서 대체 ‘블록체인 공동인증서’
- II. K생명, SmartContract를 이용한 자동청구시스템
- III. 계약플랫폼 : Chain Sign (SmartContract 기반 -은행 약정서)
- IV. 지불결제 시스템 ‘uCoin, 위비코인’, 지방자치 단체- 모바일 상품권
- V. 기타 – 물류시스템 & 투표시스템

Pain Point : 물류

파손·분실·지연 추석선물 택배, 보상받으려면...

30일부터 민원제기 가능...택배회사 "고객요구 대부분 수용"

(서울=뉴스1) 양종권 기자 | 2015-09-27 10:00 송고

☰ 중앙일보

[단독]인천공항에 밀린 해외소포 3만개..."인력 없다" 통관 지연

[뉴스1] 입력 2017.12.30 12:12

되풀이 되는 학교 급식 식중독 사고

-철저한 원인 규명과 추적으로 책임소재 밝히고 처벌해야

데스크 webmaster@kado.net 2018년 04월 04일 수요일

☰ ☱ ☲ ☳ ☴ ☵ ☶ ☷

◆ 신뢰가 부족한 부분

◆ 복잡한 서류 절차

◆ 다수의 참가자 (Cross-board)

❖ 변질가능한 제품의 이동시 변질 (식자재, 단체급식-병원, 학교 등)

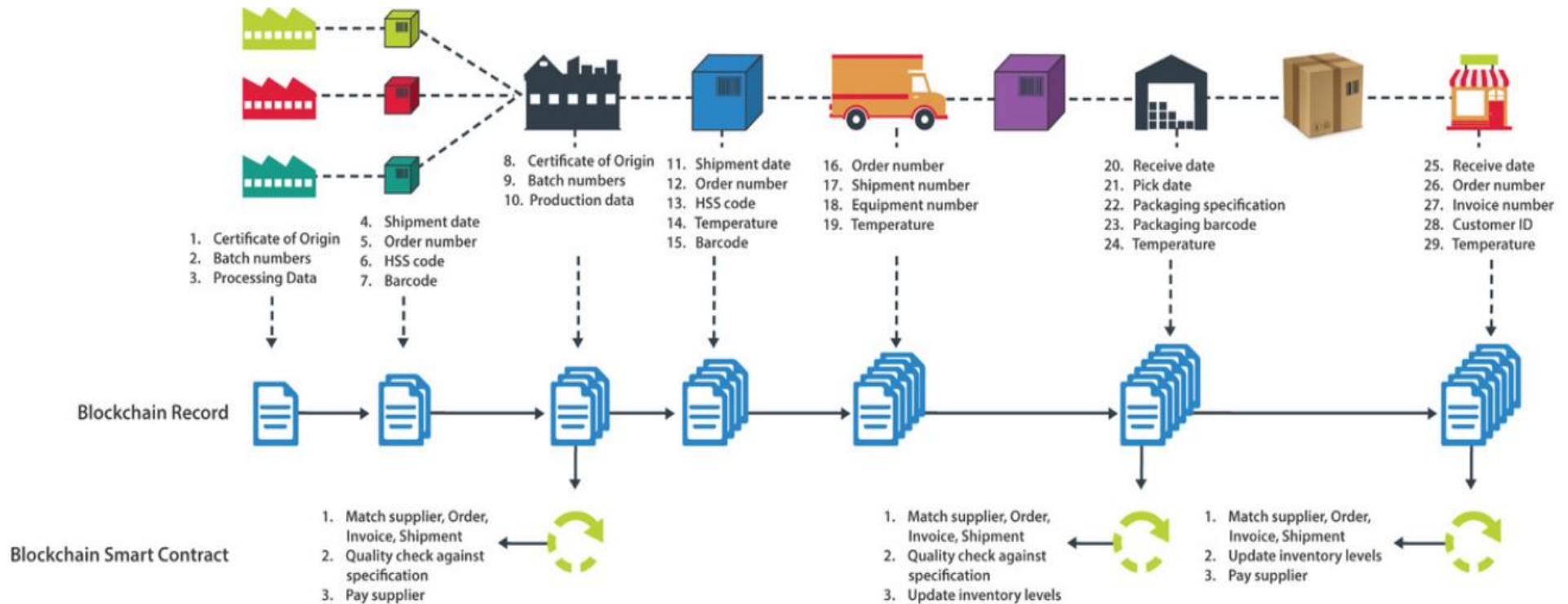
❖ 고가제품의 물류상의 파손 (미술품, 혈액, 장기, 의약품 등)

❖ 프로세싱 시간 지연

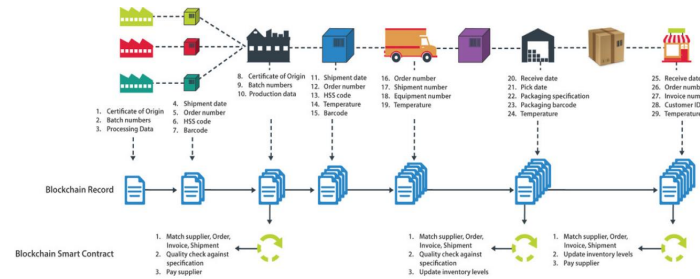
❖ 파편화된 정보, 처리시간 과 비용증가

물류 & Blockchain

Blockchain in the SCM & Logistics



물류 & Blockchain



❖ 변질가능한 제품의 이동시 변질
(식자재, 단체급식 -병원, 학교 등)

❖ 고가제품의 물류상의 파손
(미술품, 혈액, 장기, 의약품 등)

❖ 프로세싱 시간 지연

❖ 파편화된 정보, 처리시간 과 비용증가

❖ Cold Chain 정보공유 (온도/습도)

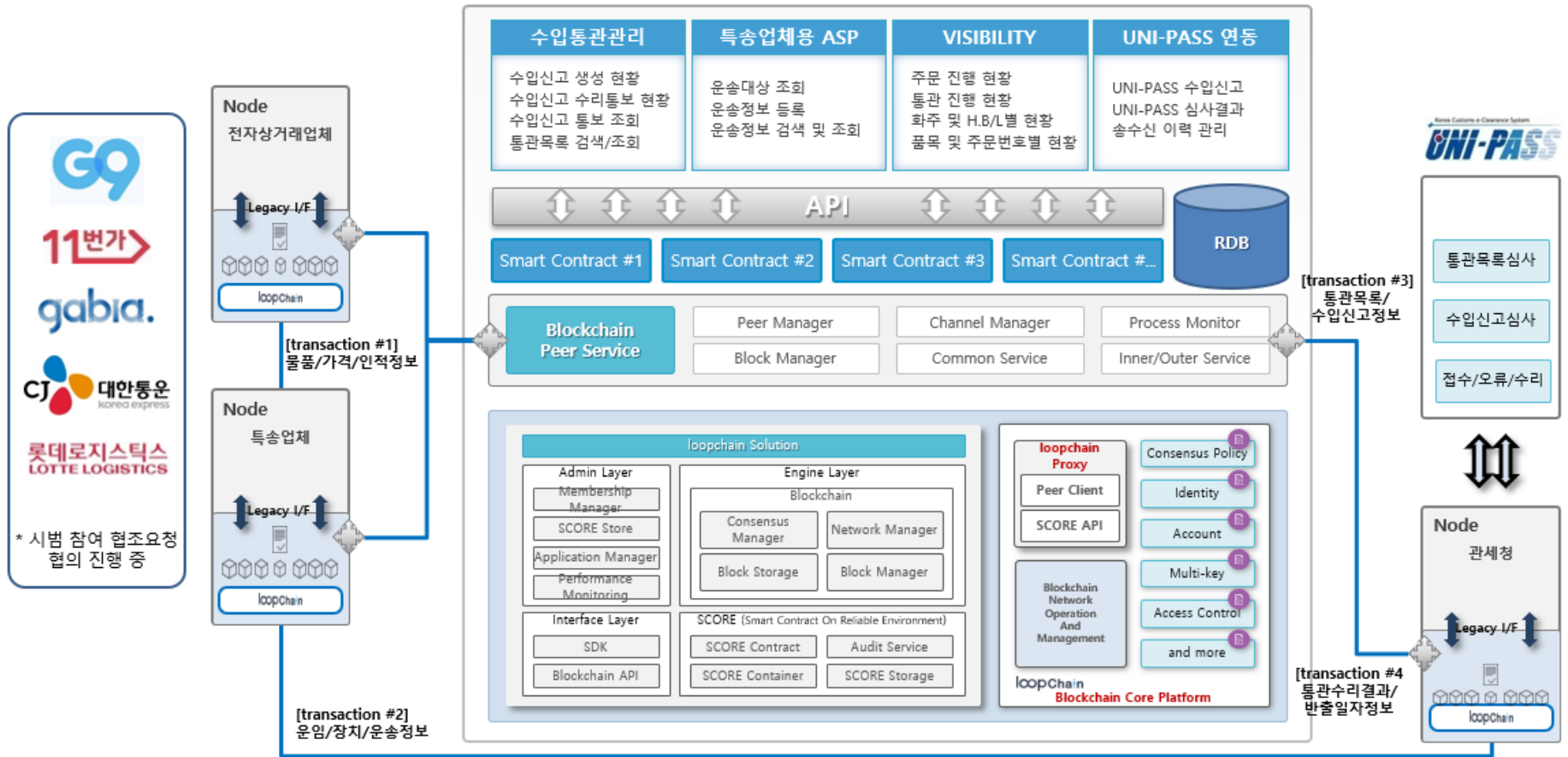
❖ 진동센스 정보공유 (진동/조도/GPS)

❖ Smart Contract 를 통한
업무 자동화 (RPA 기능)



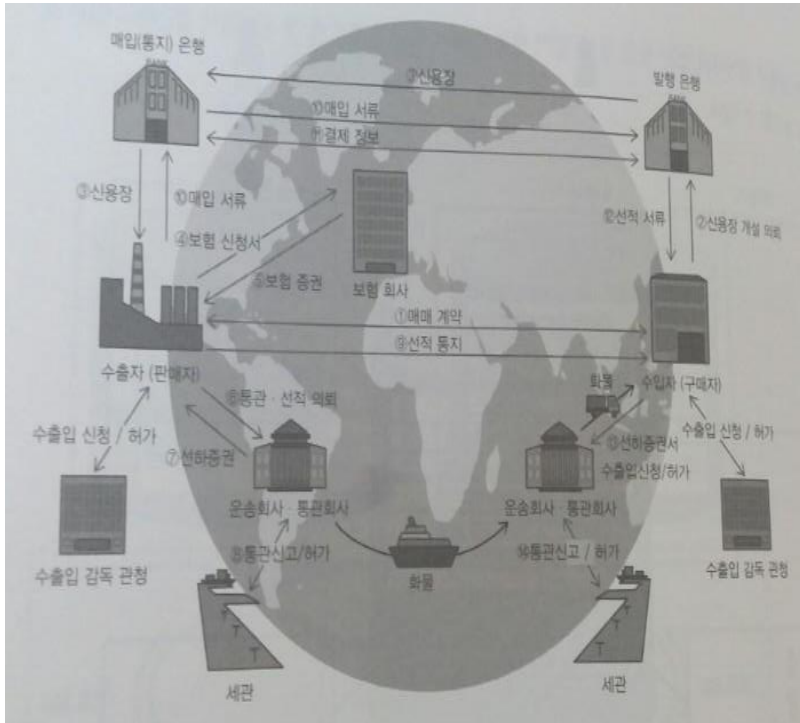
물류 & Blockchain (다품종 소량 화물)

관세청 “지능형 개인통관서비스 구축 플랫폼 시범사업”

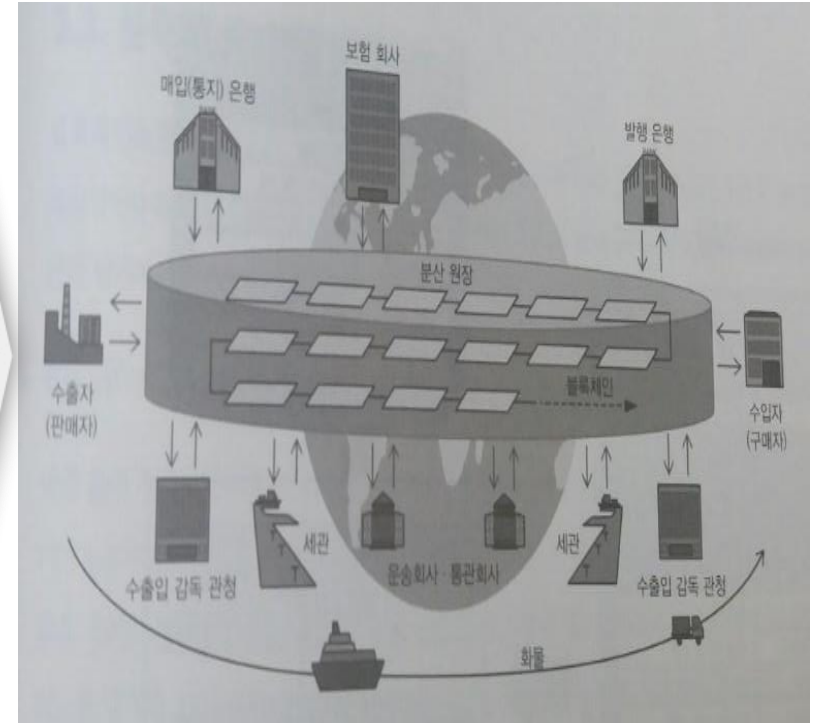


물류 & Blockchain (투명성, 추적가능성 확보)

As Is



To Be

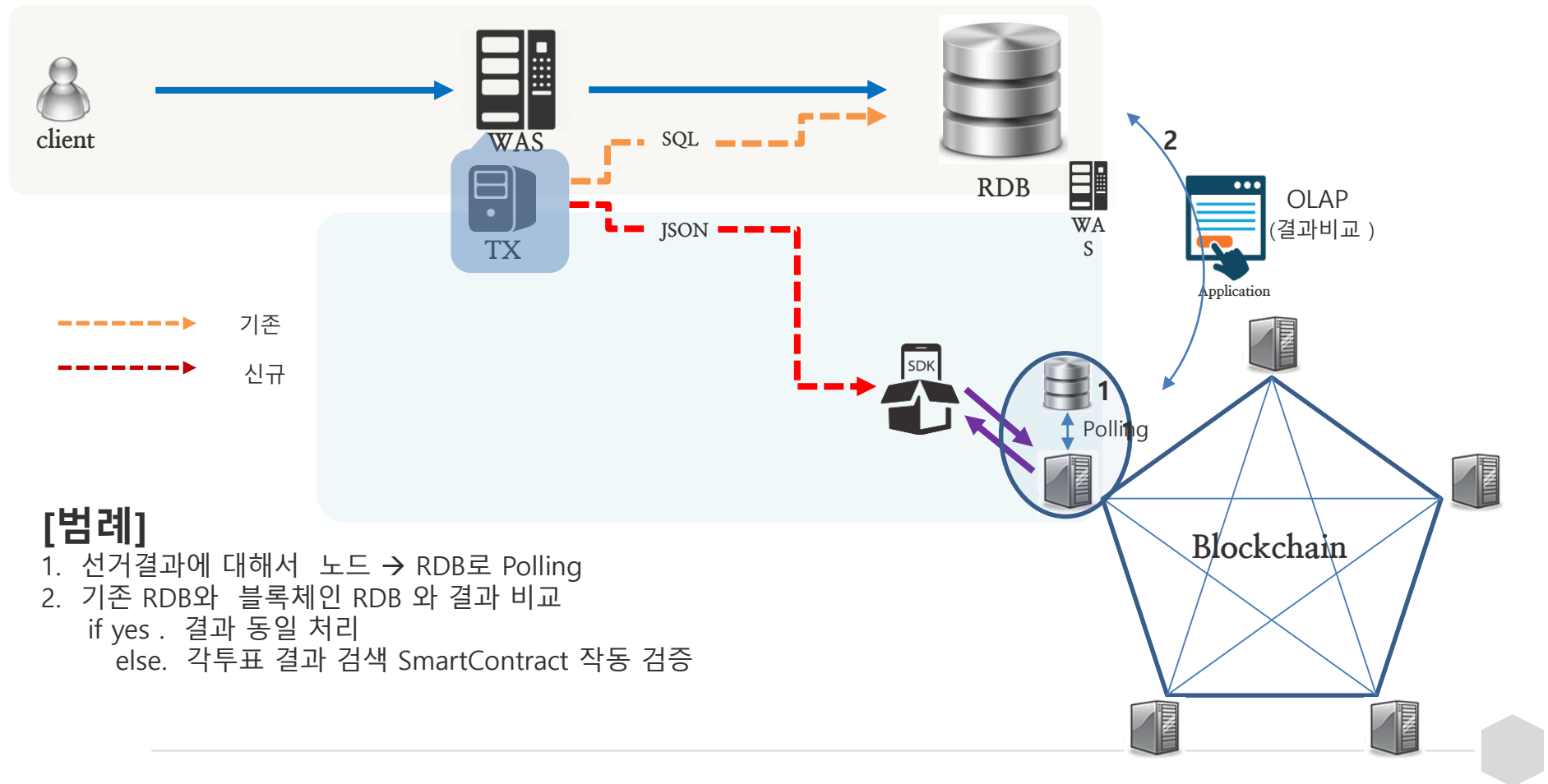


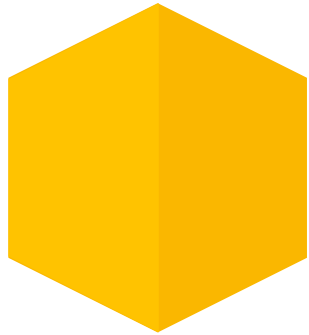
Blockchain

기존 투표시스템에 '블록체인'을 더하다

Pain Point : 투표에 대한 '공정성'과 '투명성'이 누락되어 있음

요구사항 : 기존의 시스템을 그대로 두고 블록체인을 이용한 공정성 부분만 추가





Contents

- I. Blockchain 에 대한 오해
- II. How Blockchain
- III. Case Study
- IV. loopchain™ & ICON™**
- V. Q & A

— Key Feature

- Loopchain
- 타사비교
- Legacy system 상호운용성
- 네트워크상호운용성



[참고] Public Blockchain vs Enterprise Blockchain (상세)

특성 항목		Enterprise Blockchain	Public Blockchain	
		loopchain	Bitcoin	Ethereum
시멘틱 데이터 구조		바로 이전 블록의 해시값, 트랜잭션 리스트, 블록 생성 노드 ID, 블록 검증 피어의 서명, 블록 생성 노드의 서명 등	바로 이전 블록의 해시값, 트랜잭션 리스트, 기타 데이터를 포함하는 헤더	바로 이전 블록의 해시값, 트랜잭션 리스트, uncle 블록 리스트를 포함하는 헤더
네트워크 타입		프라이빗, 컨소시엄	퍼블릭	노드의 배치에 따라 프라이빗, 컨소시엄, 퍼블릭 형태 지원
참여자		신원이 판명된 참여자	불특정 다수 (신뢰할 수 없는 사용자 포함)	노드의 배치에 따라 상이 (불특정 다수 / 신원이 판명된 참여자)
합의	알고리즘	PBFT (Practical Byzantine Fault Tolerance)	작업증명(PoW: Proof of work)	작업증명(PoW: Proof of work) / 지분증명(PoS: Proof of Stake)
	완결성	BFT 알고리즘으로 분기가 존재하지 않음. 하나의 블록 검증시 즉시 완결	시간의 흐름에 따라 새 블록의 유효성 검증 시 거래 역분개의 가능성 존재	시간의 흐름에 따라 새 블록의 유효성 검증 시 거래 역분개의 가능성 존재
계약	계산력	튜링 완전성 지원	스택 기반 언어 (단순한 인스트럭션만 제공)	튜링 완전성 지원
	프로그래밍 언어	Python	스크립트(Script)	Solidity, Serpent, LLL 등 EVM에서 처리되는 다양한 언어 지원
지연시간	블록 확정 시간	1초 미만	10분당 1블록	14초당 1블록
최대 트랜잭션/계약 크기		어플리케이션에 따라 유동적	100KB	Gas 사용량에 따라 유동적
확장성/트랜잭션 처리량		1000TPS 이상	7TPS	15TPS
프라이버시		서비스 채널 암호화를 통해 프라이버시 보호	개방	개방

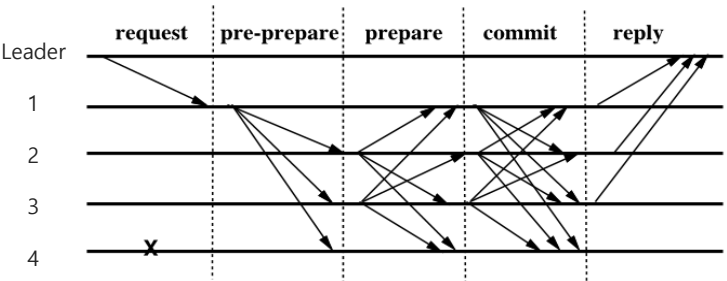
Feature #1: 고성능 합의 알고리즘

Description

- 외부 공격에 의해 침입이나 일시적 운영 시스템 실패 가능성을 고려
- 오로지 중개자의 개입 없이 당사자들 간의 메시지 전달에 기반한 합의

Byzantine Fault Tolerance (BFT)

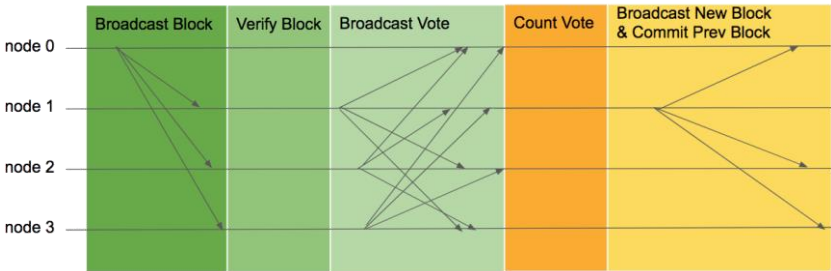
- 3단계로 나뉘어 구성
- 메시지 전달을 통해 "pre-prepare"에서 "prepare" 그리고 "commit" 순으로 진행



최적화 과정

loopchain Fault Tolerance (LFT)

- 3단계에서 2단계로 축소
- 블록 생성 전파를 위한 제한된 노드 수 (오직 남아있는 노드만이 투표과정에 참여)

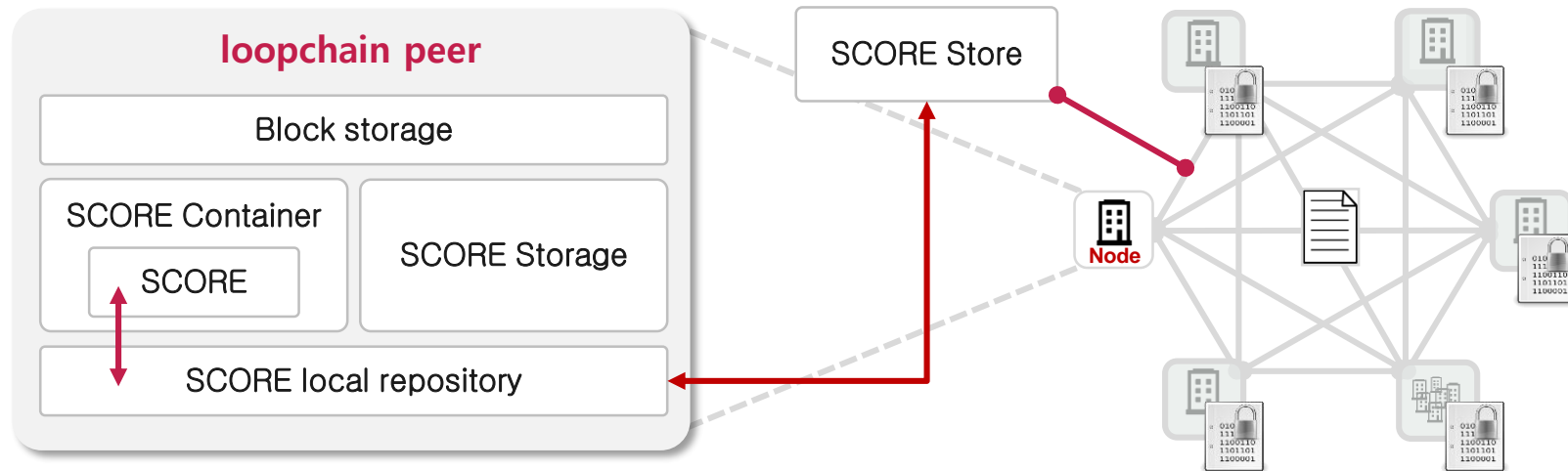


Note: Patent filed and currently under review.

Feature #2: SCORE(Smart Contract On Reliable Environment)

Description

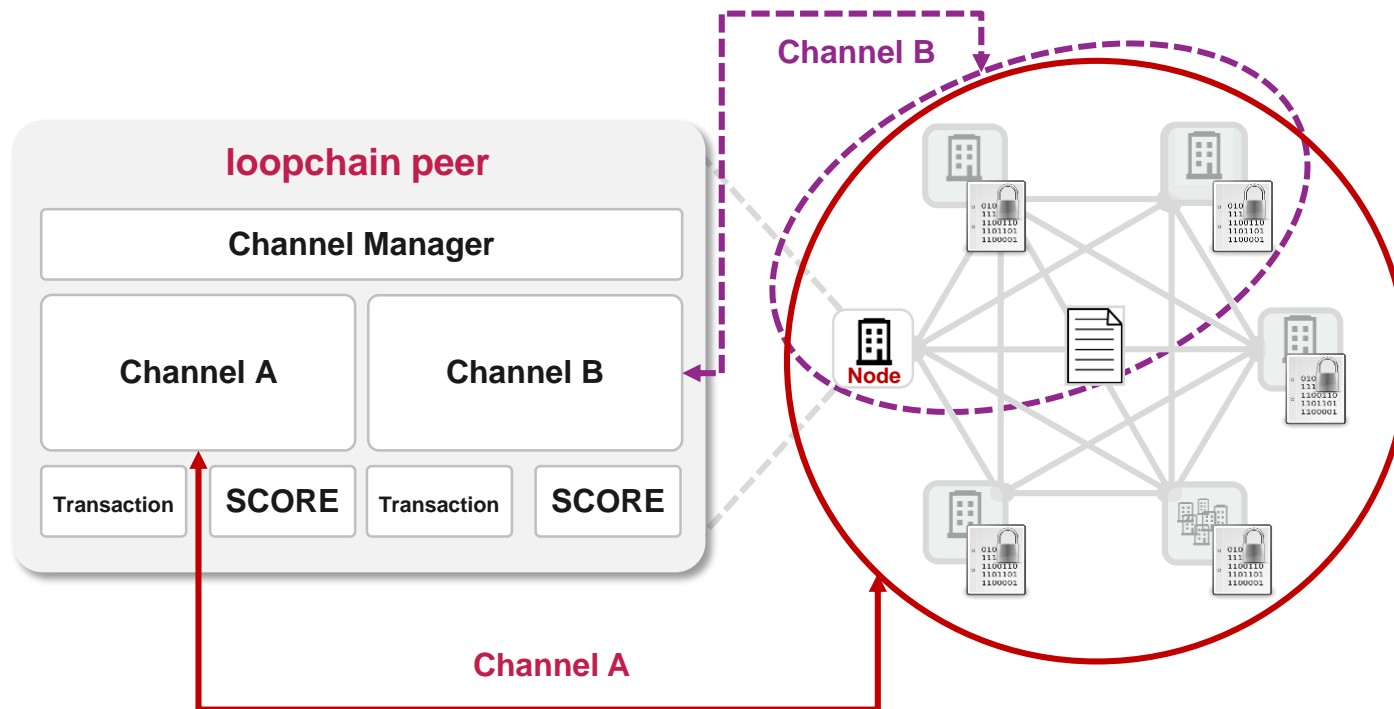
- 효율성을 높이기 위해 기본 블록체인 프로세스와는 별도로 컨테이너 기반 런타임 동안 루프체인에서 실행되는 강화된 버전의 스마트 컨트랙트
- SCORE 스토어는 스마트 컨트랙트의 효율적이고 간편한 등록과 사용, 버전닝을 지원
- 별도의 컨테이너 기반 가상 기계 (VM) 안에서가 아닌, 노드 실행 환경 안에서 바로 작동되는 SCORE는 효율성을 극대화하고 스마트 컨트랙트 상의 오류로부터 전체 블록체인 프로세스를 보호



Feature #3: Multi-Channel

Description

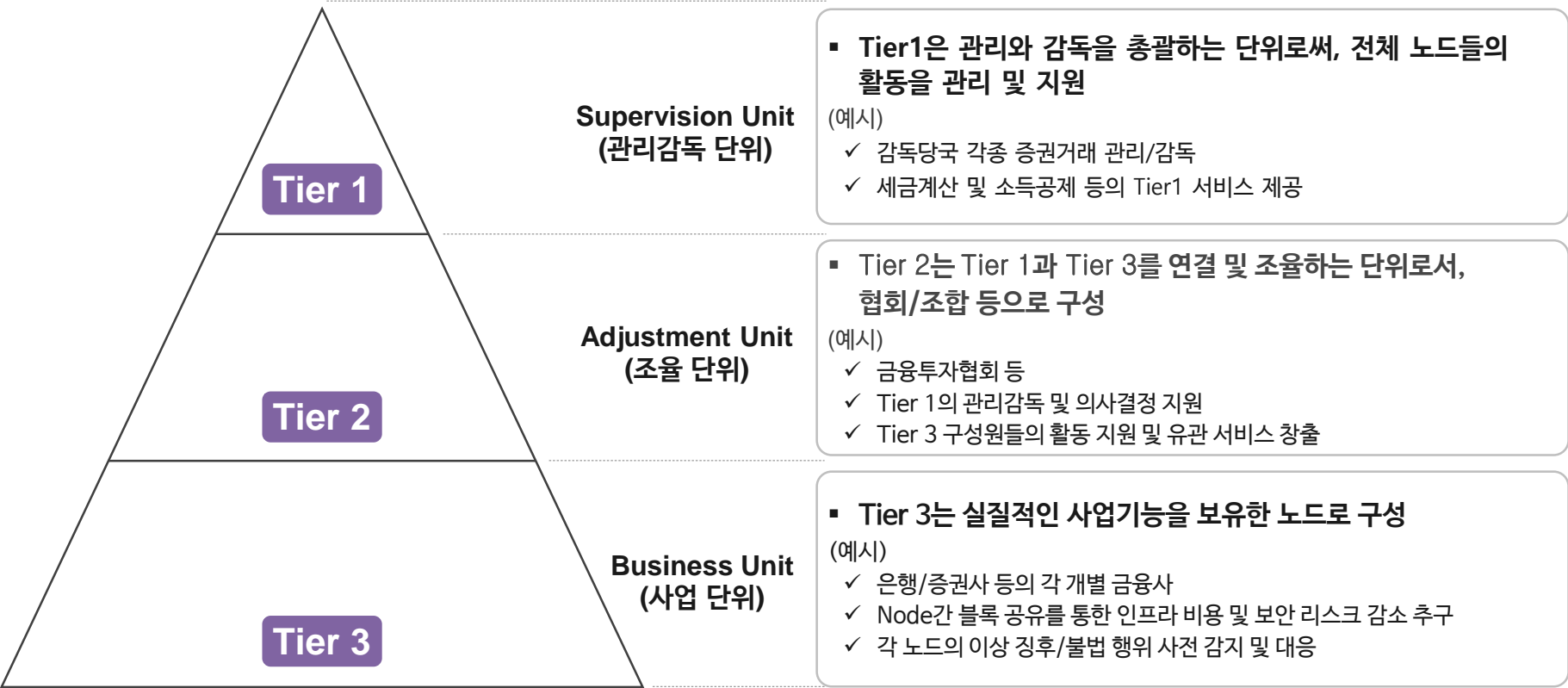
- Multi-Channel 기능은 채널들 혹은 네트워크들이 같은 블록체인 네트워크 내에서 별개의 블록체인 네트워크를 만들지 않아도 되도록 선별된 피어들과 다중 채널을 구성할 수 있도록 함
- 허용된 당사자들만 거래 데이터에 접근할 수 있도록 하기 때문에 정보 보호 등 규제를 충족시킴



Feature #4: Tiered System

Description

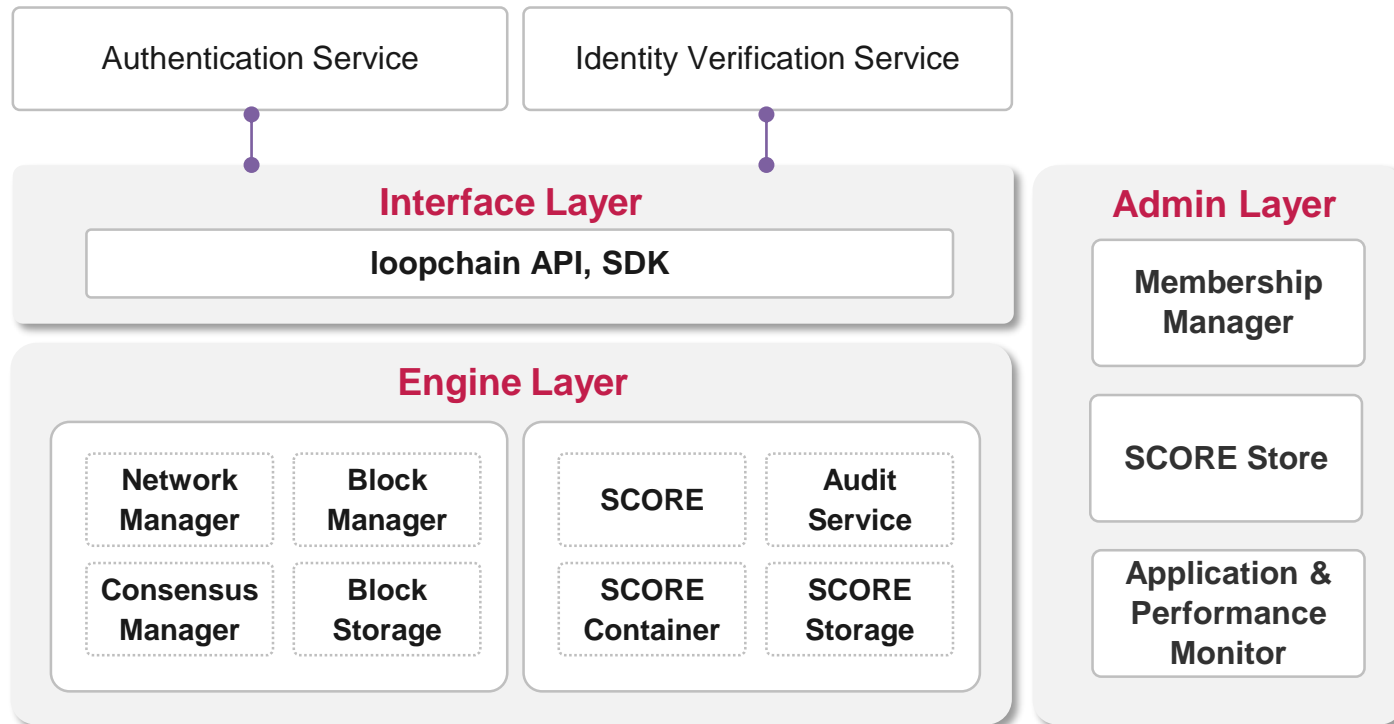
loopchain은 각 참여자들이 접속, 관리, 감독할 수 있는 정보의 등급을 조정함



Feature #5: Modular Architecture

Description

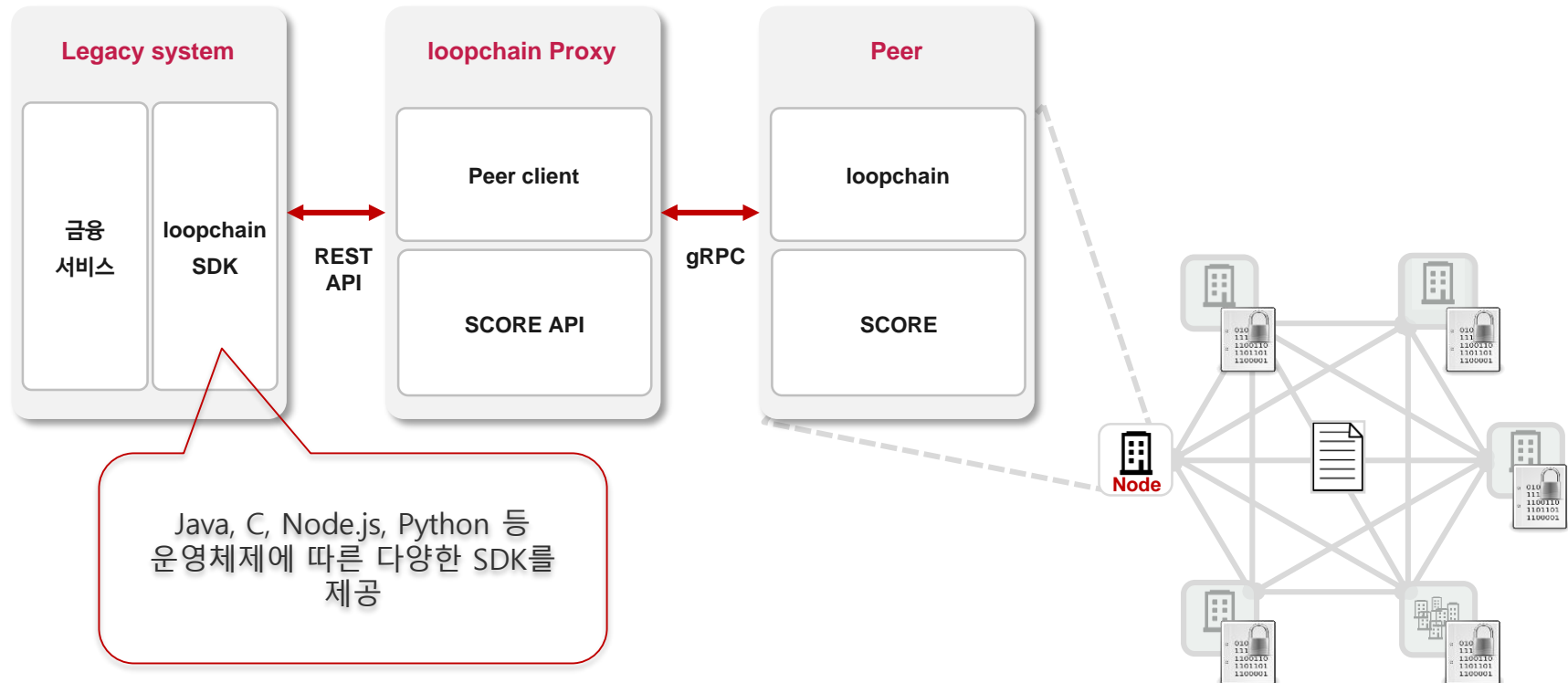
loopchain의 모듈화 구조는 노드 검증, 합의 알고리즘, 스마트컨트랙트 등을 위한 모듈의 커스터마이징을 필요할 때 언제든지 가능케 한다.



Legacy System의 상호운용성

Description

클라이언트 또는 인증된 기관에는 Rest API를 통해 loopchain 프록시에 접근하고
블록체인 피어에 연결하기 위해 loopchain SDK가 제공됨



















Top 100 Cryptocurrencies By Market Capitalization

Public Coin 들

www.coinmarketcap.com

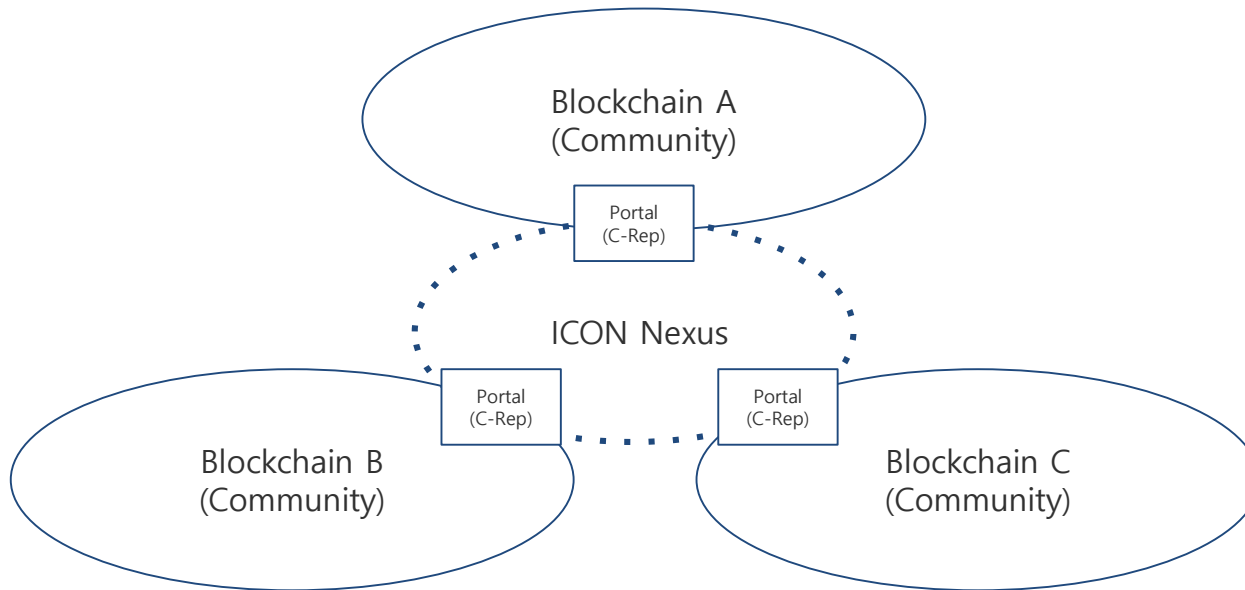
31	 DigiByte	\$240,180,691	\$0.022536	\$3,599,035	10,657,699,160 DGB	-16.67%		...
32	 Steem	\$228,929,852	\$0.838952	\$9,383,395	272,876,023 STEEM *	-14.65%		...
33	 MOAC	\$217,478,553	\$3.48	\$263,290	62,463,334 MOAC *	-12.10%		...
34	 Aeternity	\$205,273,178	\$0.880923	\$21,331,772	233,020,472 AE *	-23.04%		...
35	 ICON	\$203,765,670	\$0.525940	\$22,977,322	387,431,340 ICX *	-25.51%		...
36	 Zilliqa	\$201,914,277	\$0.026682	\$19,674,017	7,567,552,268 ZIL *	-25.66%		...
37	 Waves	\$191,614,128	\$1.92	\$7,029,300	100,000,000 WAVES *	-10.96%		...



Introduction

ICON: 블록체인으로 구성된 다양한 독립적인 Community들을 각 Community를 대표하는 C-Rep(Community Representative)을 통해 연결하여 Nexus라는 네트워크를 구성하는 프로토콜과 그 형상
하나의 Nexus는 또다른 Nexus와 연결이 가능하며 이를 통해 블록체인 네트워크가 다양하게 확대 가능

Architecture



Comments

loopchain – Nexus는 loopchain 기반으로 구현

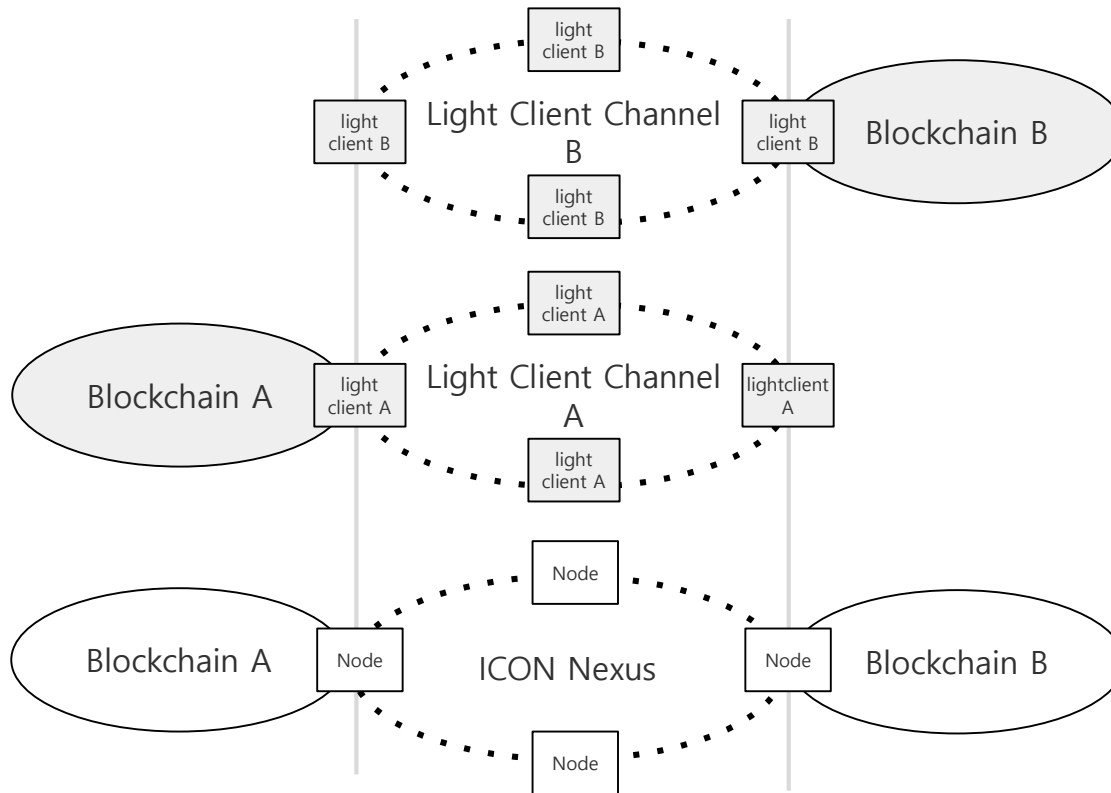
Nexus – Nexus 중심으로 다양한 블록체인이 Portal을 통해 연결

BTP – Portal을 통해 BTP를 기반으로 다양한 블록체인간 거래 연동이 가능

Governance – 다른 블록체인을 연결하는 Portal 및 여러 노드가 참여하여 탈중앙화된 거버넌스 구현

Blockchain Transmission Protocol (BTP)

Blockchain Transmission Protocol (BTP)

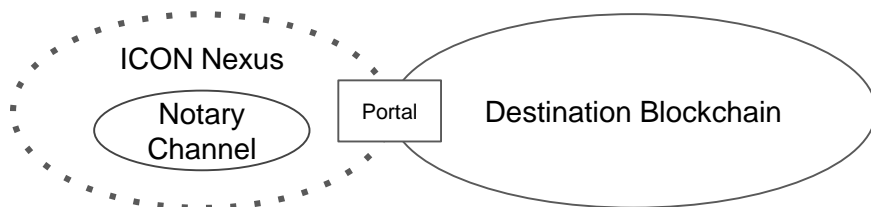


Comments

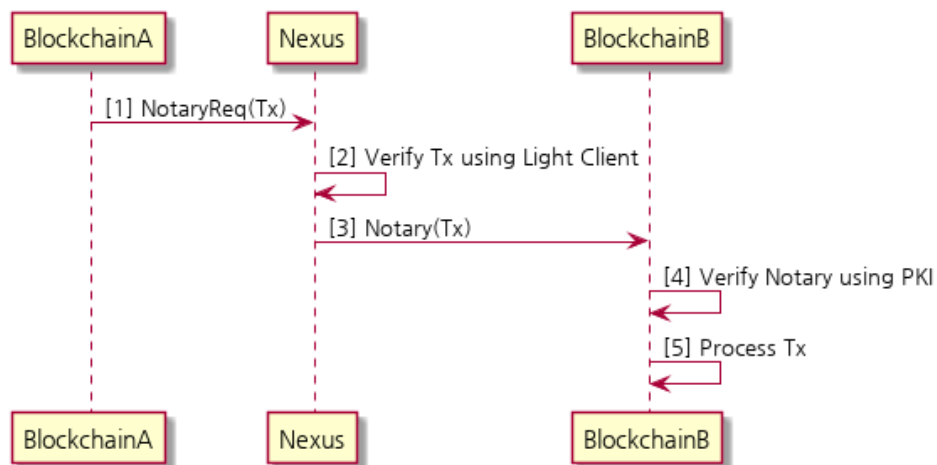
- Nexus와 연결된 블록체인 간 거래를 연계하기 위한 프로토콜
- Nexus에 구성된 Notary channel을 통해 송신 블록체인의 거래가 수신 블록체인으로 전달
- Nexus 구성 노드 중 Notary channel의 투표권한이 있는 노드는 Nexus에 연결된 각 블록체인의 Light Client를 하나의 채널로 한 다수의 채널 보유
- Notary channel은 loopchain의 Multi-channel 지원 기능을 기반으로 구현
- Nexus에 연결된 블록체인의 Light Client를 통해 해당 블록체인에서 합의된 거래를 Nexus에서 확인

Blockchain Transmission Protocol (BTP) – (continued)

Notary Channel



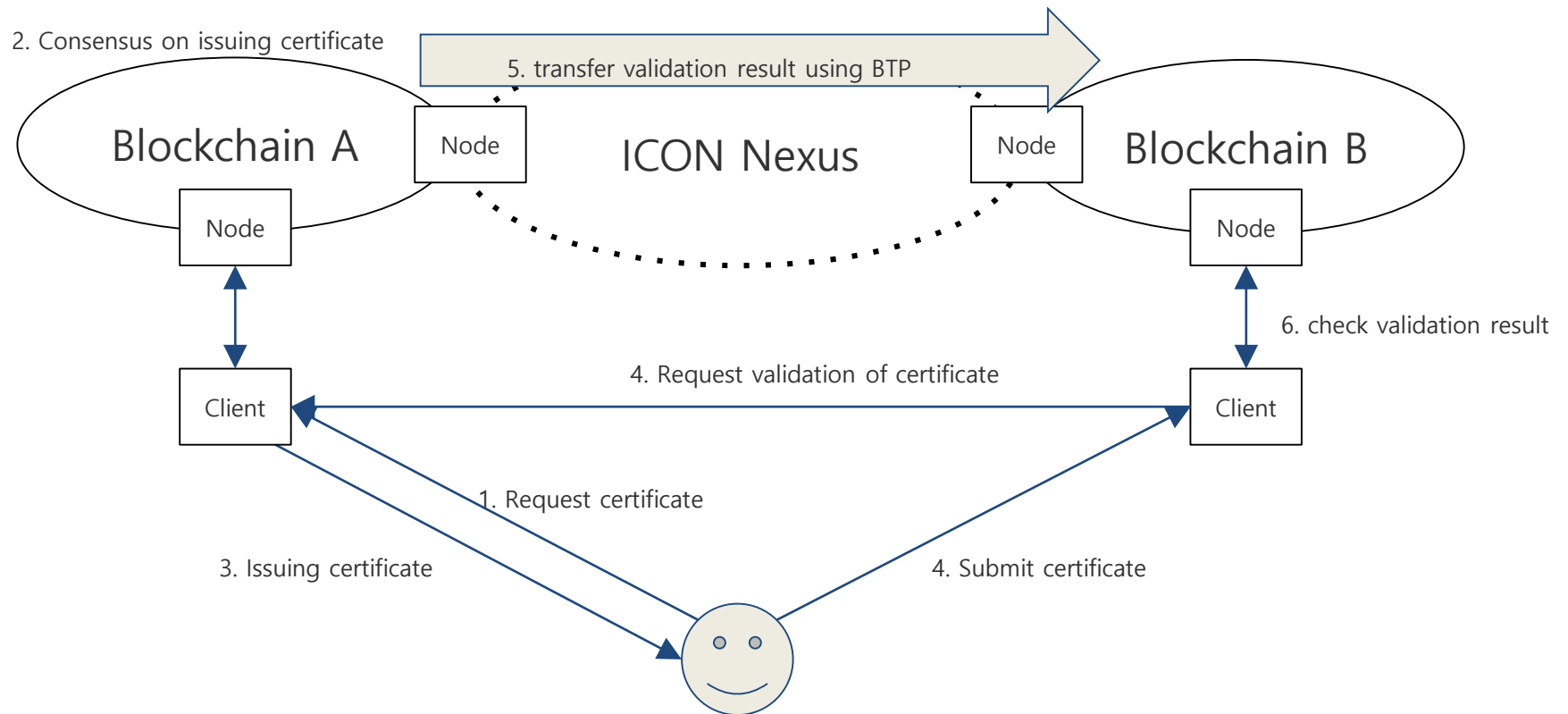
Notary Channel Transaction Flow



Comments

- Notary 등록 요청 거래에 대해 투표권이 있는 노드들의 복수의 서명이 블록에 포함되어 Notary channel의 블록체인을 형성
- Notary channel에 등록된 거래가 포함된 블록데이터는 Portal을 통해 수신 블록체인으로 전달
- 수신 블록체인에서 해당 블록데이터를 검증할 때는 Nexus의 Notary channel을 구성하는 노드들의 인증서를 기반으로 각 노드의 서명 검증
- LFT 기반의 합의를 따르는 Notary channel 규격에 따라 2/3 이상의 서명이 확인되면 해당 거래의 합의 여부가 확인되어 거래 진행

BTP Example – Certification Transfer



Decentralized Exchange (DEX)

ICON 네트워크 시작 시점부터 별도의 거래소 없이 스마트컨트랙트 기반의 분산 거래소 제공

Formula for Price

$$ReserveBalance = ReserveRate \times ICXVolume \times ICXPrice$$

$$ICXPrice = \frac{ReserveBalance}{ReserveRate \times ICXVolume}$$

- ETH로 ICX 구매할 경우
 - ETH Reserve Balance 늘어남
 - ICX Volume 줄어듦
 - ICX Price 올라감
- ICX로 ETH를 구매할 경우
 - ETH Reserve Balance 줄어듦
 - ICX Volume 늘어남
 - ICX Price가 내려감

Comments

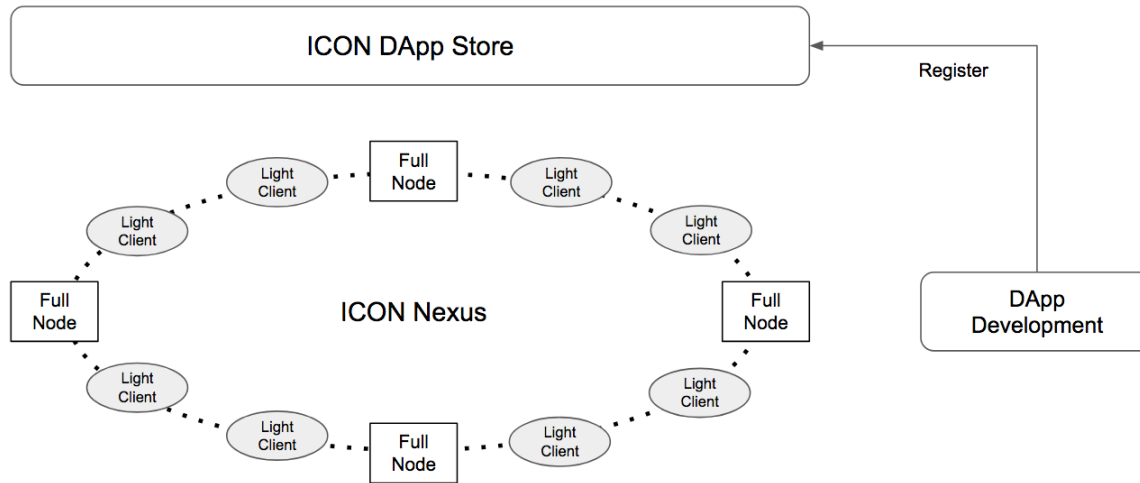
- **DEX** – 일반적인 가상화폐 거래소처럼 third party를 통해 거래하는 centralized exchange가 아닌 블록체인 상에서 자동으로 거래를 처리해주는 시장
- Bancor Protocol 을 기반으로 Reserve를 통한 거래 가격을 산정하여 가상화폐간 실시간 거래 제공
- 기본적으로 ETH/ICX DEX 제공
- Ethereum내 Reserve 스마트컨트랙트와 ICON내 Reserve 스마트컨트랙트에 투표권이 있는 노드로 DEX 구성

Source: https://bancor.network/static/Bancor_Protocol_Whitepaper_en.pdf

Nexus Public Channel

Nexus에는 모든 사람에게 공개된 Public channel이 포함되어 있어 누구나 ICX 거래 및 DApp을 만들고 이용할 수 있음

Public Channel



Comments

- **Ethereum DApp** – 거래 데이터에 컴파일한 DApp 코드를 포함시키고 VM(Virtual Machine)으로 해당 코드를 실행
- **ICON DApp** – 사전에 DApp을 개발하여 DApp Store에 등록하고 해당 거래에 참여할 노드는 DApp Store로부터 DApp을 받아서 설치한 후 이용
- 거래를 등록하고 확인할 수 있는 Light Client 기반의 노드와 거래에 대한 합의를 이루는 Full Node로 구성
- Light Client, Full Node 모두 ICON 네트워크 유지 및 활성화 기여도에 따라 Incentive 받음

Source: https://bancor.network/static/Bancor_Protocol_Whitepaper_en.pdf

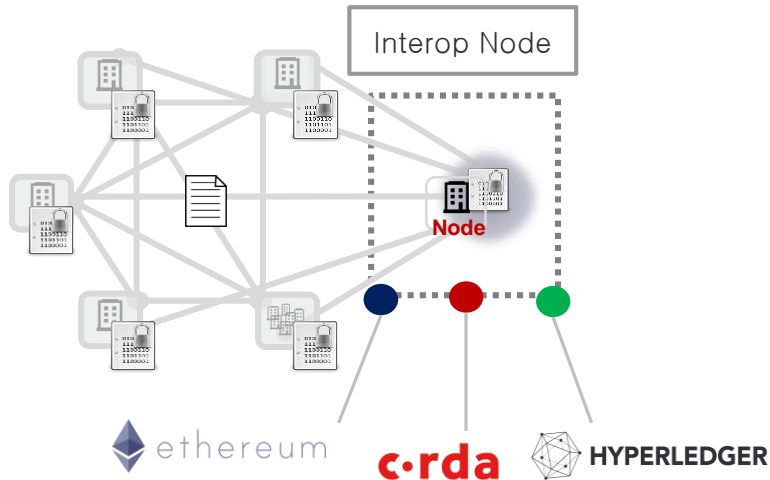
네트워크 상호운용성 방법 (블록체인간 정보 전달과 교환)

Description

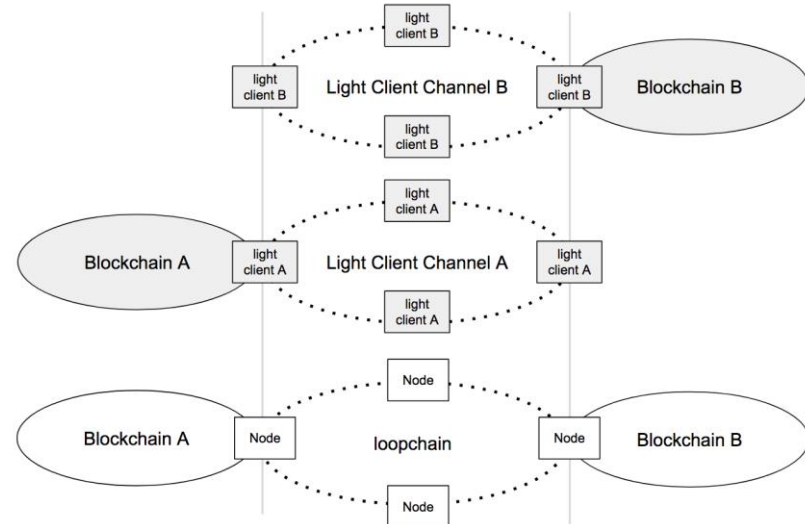
Loopchain이 허가, 공개 여부에 관계없이 제3의 블록체인에 연결할 수 있는 방법:

- 상호운용성을 위해 설계된 특수 노트 추가 – **“Interop Node”**
- 독립적인 블록체인간 transaction을 용이하게 하는 **Blockchain Transfer Protocol (BTP)**을 통해 연결

Interop Node



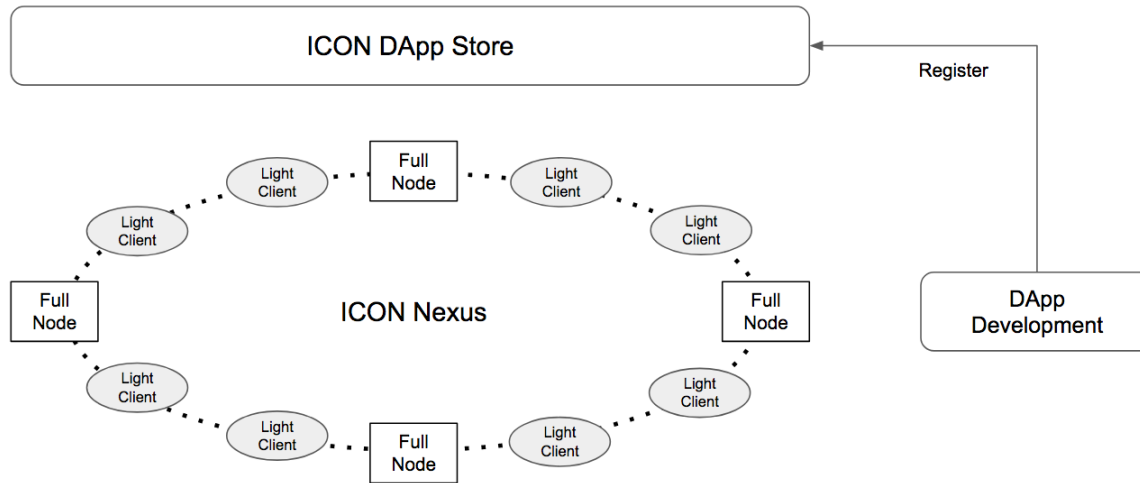
Blockchain Transfer Protocol (BTP)



Nexus Public Channel

Nexus에는 모든 사람에게 공개된 Public channel이 포함되어 있어 누구나 ICX 거래 및 DApp을 만들고 이용할 수 있음

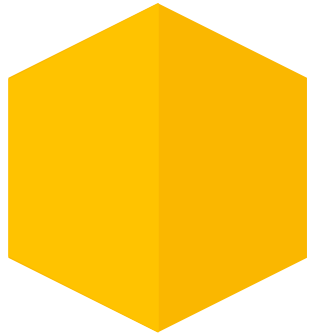
Public Channel



Comments

- **Ethereum DApp** – 거래 데이터에 컴파일한 DApp 코드를 포함시키고 VM(Virtual Machine)으로 해당 코드를 실행
- **ICON DApp** – 사전에 DApp을 개발하여 DApp Store에 등록하고 해당 거래에 참여할 노드는 DApp Store로부터 DApp을 받아서 설치한 후 이용
- 거래를 등록하고 확인할 수 있는 Light Client 기반의 노드와 거래에 대한 합의를 이루는 Full Node로 구성
- Light Client, Full Node 모두 ICON 네트워크 유지 및 활성화 기여도에 따라 Incentive 받음

Source: https://bancor.network/static/Bancor_Protocol_Whitepaper_en.pdf



Contents

- I. Blockchain 에 대한 오해
- II. How Blockchain
- III. Case Study
- IV. loopchain™ & ICON™
- V. Q & A

참조문헌

1. “Bitcoin: A Peer-to-Peer Electronic Cash System” , Satoshi Nakamoto
2. “Mastering Bitcoin” , Andreas M
3. “Blockchain Revolution “ , Don Tapscott
4. “Business Blockchain “ , William Mougayar
5. “Blockchain Basics “ , Daniel Drescher
6. “The age of Crypto currency “ , Paul Vigna & Micheal J. Casey
7. “블록체인의 구조와 이론”, 아카하네 요시하루 , 아이케이 마나부



—
Thank you

'Closed Question'
('예,아니오'로 답할 수 있는 질문)
으로 부탁드립니다. ^^

Presenter

블록체인사업본부
김항진 이사 / 사업개발
2727@theloop.co.kr

the**loop**

theloop www.theloop.co.kr

L 서울시 중구 삼일대로 343 , 12층

T +82. 2 6105. 8100

F +82. 2 6105. 8122

