SAMSUNG SDS
Realize your vision

Foresee

Techtonic 2019

Disrupt

Partner

2019.11.14 • SAMSUNG SDS Tower B1F
{ Magellan Hall / Pascal Hall }

Track 3 | Blockchain

DID(Decentralized Identity)
대세는 탈 중앙화! 신분 증명도 탈 중앙화?

김상현 프로 (블록체인 센터) / 삼성SDS
박철우 부장 (미래사업실/전략기획팀) / (주)드림시큐리티

AGENDA

1. DID – 블록체인, 등장
2. DID – 블록체인, 현재와 미래
3. 사업화 방안
4. 가치창출
5. 비즈니스 모델
6. 협력과 상생

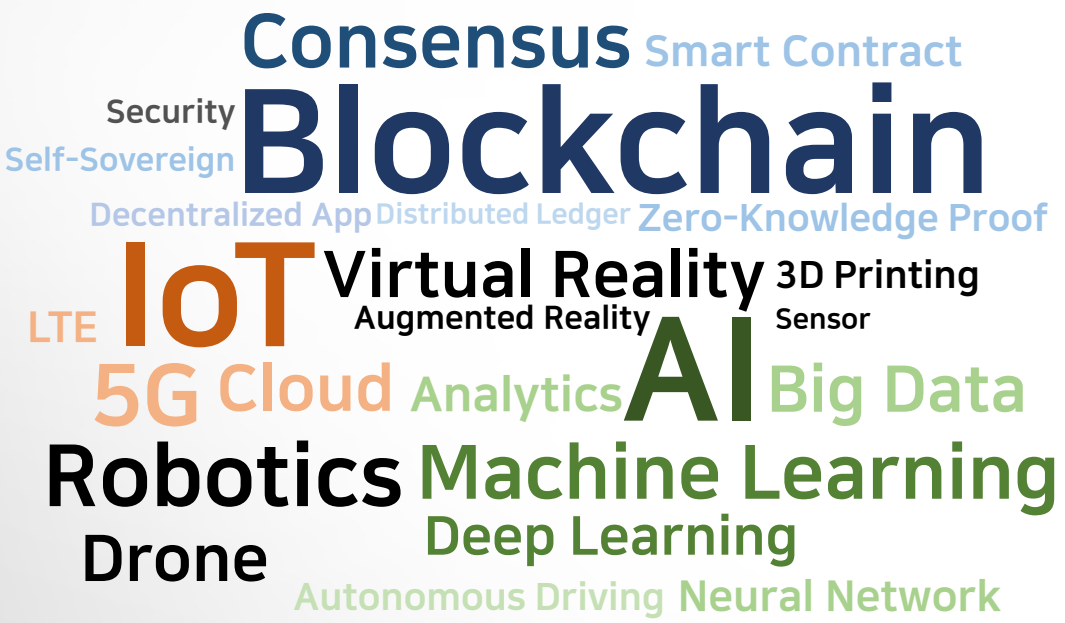
1

DID - 블록체인, 등장

2020 블록체인 ! 대세는 DID !

2020년 블록체인 상용화 핵심 전략, 탈 중앙화 신원 증명 (Decentralized Identity)

미래 산업 트렌드와 IT 기술



미래산업 트렌드와 IT 기술

- IoT[1], AI[2] 등과 함께 실용적인 블록체인(Practical Blockchain) 강조

블록체인 플랫폼의 발전 방향

- 완전한 엔터프라이즈 블록체인 플랫폼의 조건
  - 분산, 불변, 암호화, 토큰화, 탈 중앙화
- 상호 보완 기술과의 통합을 통한 발전
  - IoT, AI, SSI (Self-Sovereign Identity)

KBW[3] 2019 D.FINE 컨퍼런스

- DID 개념 및 관련 사업 소개

DID Alliance Korea 2019

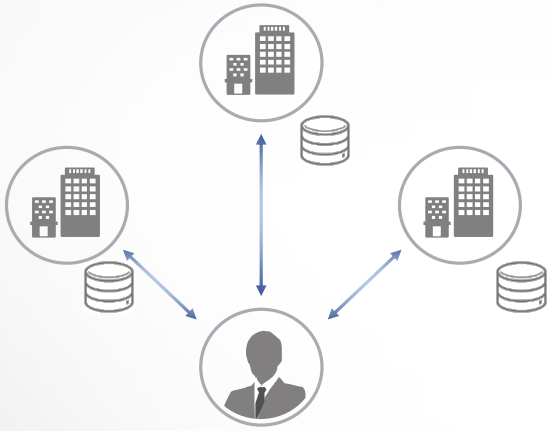
- DID 추진 전략 및 활용 사례 소개

1) IoT : Internet of Things, 2) AI : Artificial Intelligence, 3) KBW : Korea Blockchain Week

개인의 신원 증명은 개인의 몫으로, SSI 등장 !

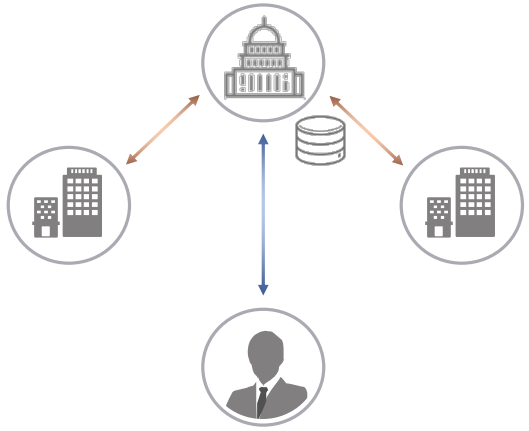
독립 / 연합 형태를 거쳐, 자기 주권 신원 증명 (Self-Sovereign Identity) 으로 전환

독립 / 중앙 집중



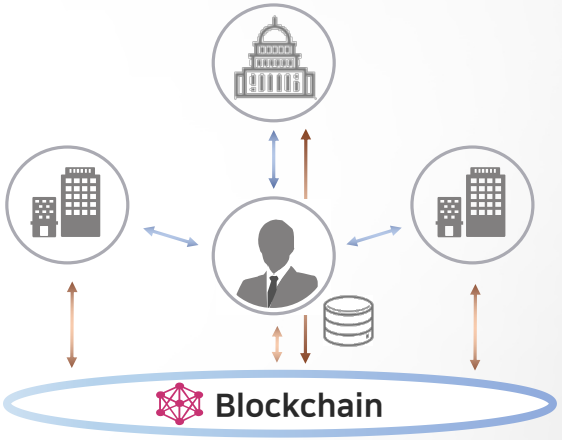
- 인터넷과 함께 등장
- ID/PW 형태의 신원 증명 발급
- 웹 사이트 별 ID/PW 등록 필요

연합 / 사용자 중심



- MS[1] 통합 ID, Open ID, OAuth
- 1개의 ID/PW 발급, 통합 사용
- 개인 동의에 의한 신원 증명 정보 제공

탈 중앙화 / 자기 주권



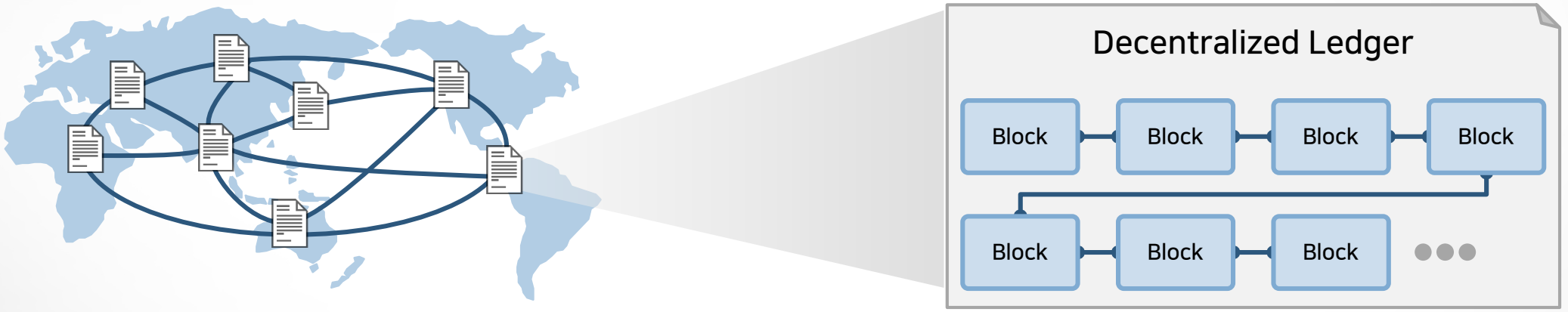
- 블록체인과 함께 등장
- 중앙 집중형 절차 및 데이터 저장소 배제
- 신원 증명에 대한 개인 권한 극대화

1) MS : Microsoft

DID, 불을 지핀 블록체인

탈 중앙화 원장 기술(Decentralized Ledger Technology) 블록체인, 탈 중앙화 서비스의 아이콘

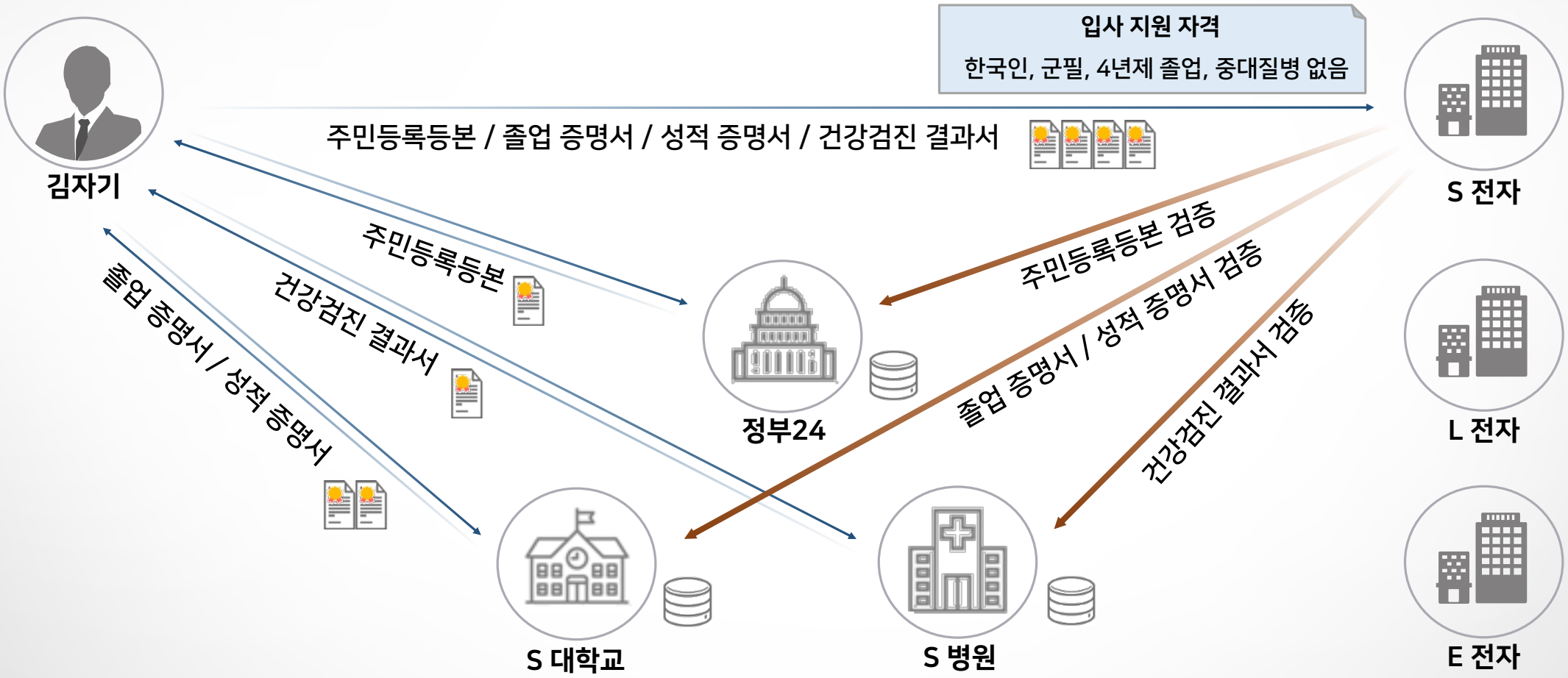
체인처럼 연결된 블록, 탈 중앙화 거래 장부



- 블록체인 네트워크의 모든 노드는 각각 탈 중앙화된 거래 장부 보관
- 모든 노드는 동일한 내용을 보관, 특정 내용에 대한 개별 위/변조 불가
- 개별 거래들을 블록이라는 단위로 묶음
- 거래 장부는 개별 블록들을 시간 순으로 체인처럼 연결하여 보관

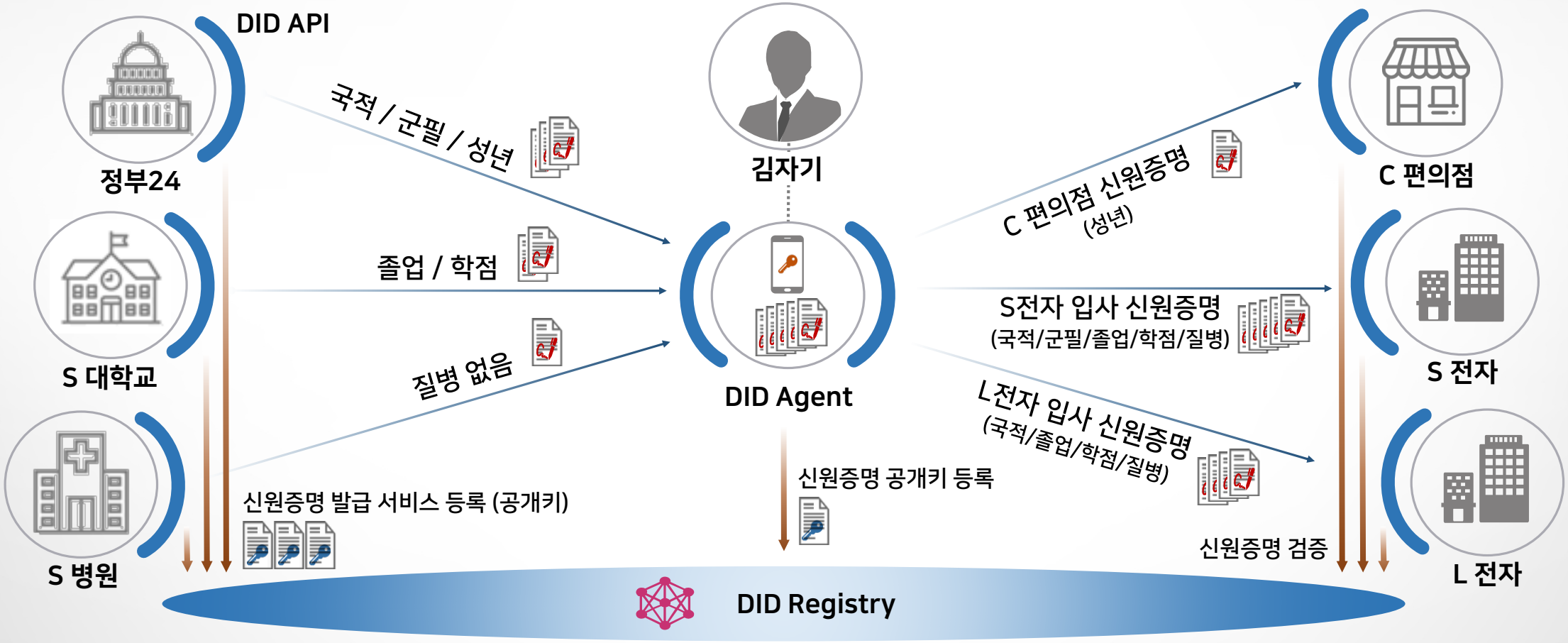
독립 / 개인 중심 신원 증명 (현재)

발급 기관별 신원증명 전자문서를 이용 기관에 제출, 이용 기관은 발급 기관을 통해 신원 증명 검증



탈 중앙화 / 자기 주권 신원 증명

DID Agent – 신원 증명 전자 지갑, DID API – 발급 / 증명 절차 자동화, DID Registry – 탈 중앙화 검증

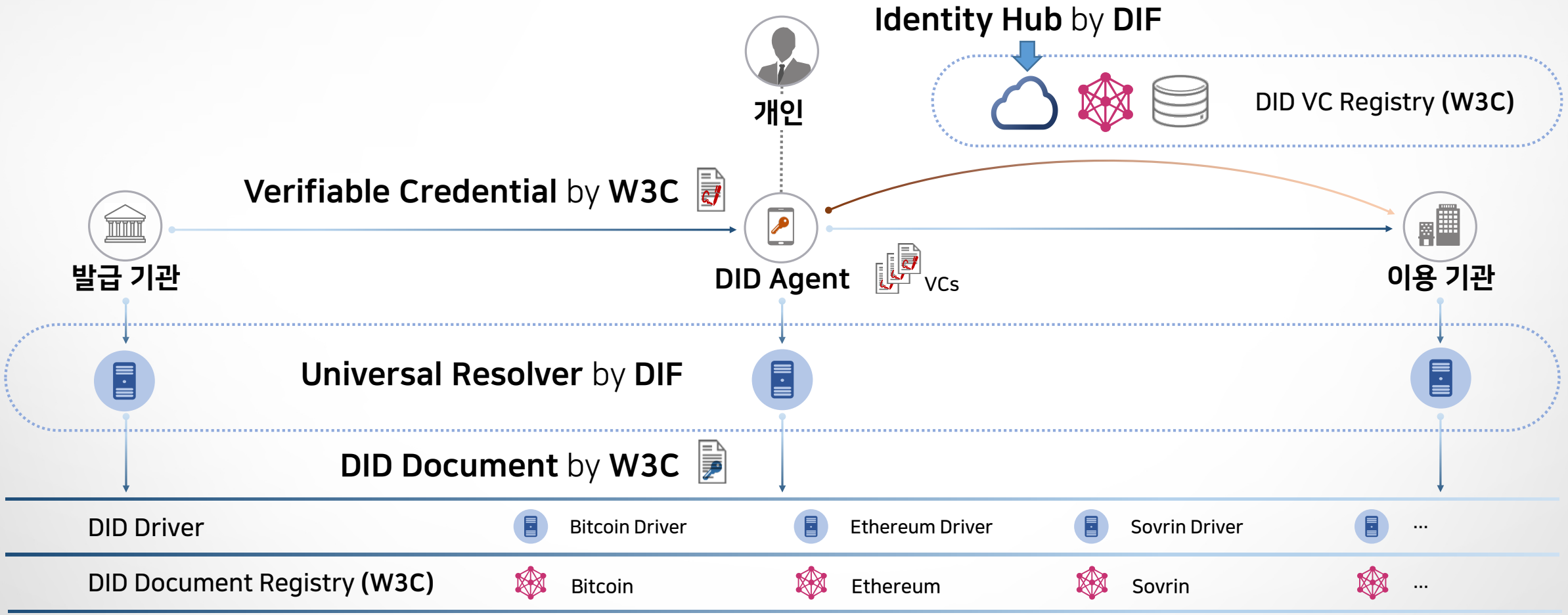


2

DID - 블록체인, 현재와 미래

DID 표준 개발을 위한 컨소시엄 등장

W3C[1] – DID 연계 표준 제정, DIF[2] – 개방형 DID 생태계 구축을 위한 공통 기술 개발



1) W3C : World Wide Web Consortium, 2) DIF : Decentralized Identity Foundation

개인 정보 보호 이슈

빅데이터 기술의 등장과 함께 데이터 가치 증가, 해킹에 따른 개인 정보 침해 피해 증가

W3C - 개인 정보 보호를 위한 고려사항

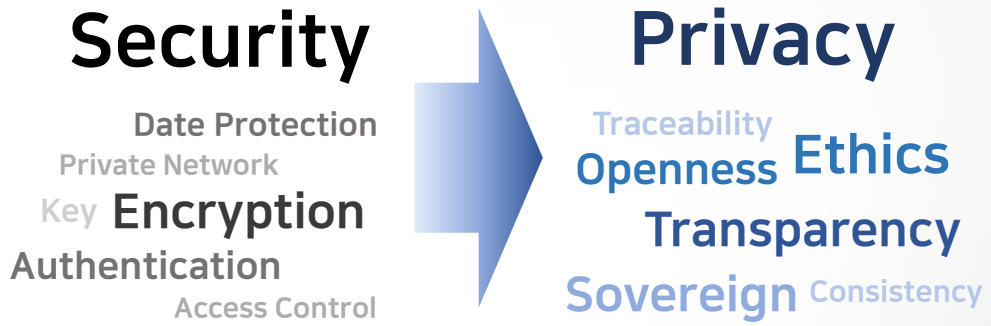
DID Document

- 분산 원장, 탈 중앙화 P2P 네트워크, 탈 중앙화 시스템
- DID Document는 어떠한 PII[1]도 미포함
- 사용 목적 별 별도의 DID 생성 및 사용
- DID는 익명성과 가명성 보장

Verifiable Confidential

- 사용 목적에 맞는 최소한의 신원 증명을 통한 개인 정보 최소화
  - 예) 성년을 증명하기 위해, "age" 필드가 아닌 "ageOver" 필드 사용
- 신원 증명 정보는 일회성으로 사용 혹은 사용 기간 최소화
- 서명 정보를 이용한 개인 식별을 방지하기 위해 **다중 서명** 적용
- 신원 증명 원본이 아닌 **영지식 증명**을 통한 검증 적용

개인 정보 보호의 관점 변화



디지털 윤리 관점의 개인 정보 보호

- 개인 정보의 가치에 대한 인식, 개인 정보의 사용 방식에 대한 관심 증대
- 정부 차원의 기업 규제 강화, 개인의 정보 보호 / 삭제 권한 강화

데이터 주권 관점의 투명성과 추적성

- 개인의 성장에 따라 조직의 데이터 저장 / 수집에 대한 책임 증가
- 신뢰 요소 강조 : 윤리, 청렴, 개방, 책임, 역량, 일관성

1) PII : Personally identifiable information

앞으로는 어떻게? – 권한과 책임

개인 모바일 기기 내 인증 수단 / 신원 증명 보관, 권한에는 반드시 책임이 수반된다.

개인 인식 변화

알 수 없는 출처 제한	• 출처가 불분명한 앱 설치 및 URL 접속 금지
보안 어플리케이션 사용	• 보안 어플리케이션 설치 및 최신 버전 유지

모바일 HW / SW 보안 강화

인증 기술	• 안면 인식, 정맥, 홍채 등 생체 인증 적용 • 인증 수단의 인식률 / 정확도 향상
보안 솔루션	• 모바일 보안 솔루션 적용 ▶ MDM[1)] • 보안 어플리케이션 연계
컴플라이언스	• 정부 차원의 정책 수립, 법령 제정 • 보안 가이드라인 준수

블록체인 보안 강화

전자서명	• 검증된 키 생성 알고리즘 사용
합의 알고리즘	• 51% 공격, 합의 가로채기 등 방지 • 랜덤 알고리즘 적용 • 노드 퍼미션 관리
스마트 컨트랙트	• 스마트 컨트랙트 취약점 모니터링 및 조치 • 소스 검증 체계 마련
네트워크	• 노드 / 클라이언트 검증 ▶ TLS[2)] • 비정상 거래 탐지
개인정보 보호	• **민감 데이터 배제** • **비공개 데이터 암호화** • **공개 / 비공개 데이터 별도 처리** • **비공개 데이터 라이프사이클 관리**

1) MDM : Mobile Device Management, 2) TLS : Transport Layer Security

앞으로는 어떻게? – 비공개 데이터 암호화, 민감 데이터 배제

비공개 데이터를 암호화하여 블록체인에 보관하거나, 비공개 데이터의 증명 자료만 보관

동적 그룹 암호화 (DGE[1])

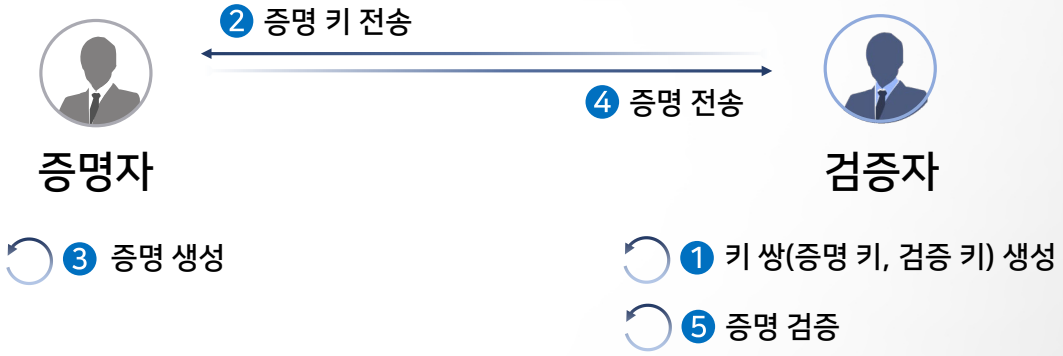
* 삼성SDS Nexledger 블록체인 플랫폼 - PoC 진행 중

Ex) DGE 거래 예시

```
{
  "Sender" : "A", "Receiver" : [ "B", "C" ] ,
  "Data" : {
    "Asymmetric Encrypted Symmetric-Key List" : [ "for B", "for C"],
    "Symmetric Encrypted Payload" : "A Payload"
  }
}
```

영지식 증명 (ZKP[2])

* 삼성SDS Nexledger 블록체인 플랫폼 - PoC 진행 중



$$G(proving\ program, random) = (proving\ key\ , verifying\ key\ )$$

$$P(proving\ key, witness, hash\ of\ witness) = proof$$

$$V(verifying\ key, hash\ of\ witness, proof) = true/false$$

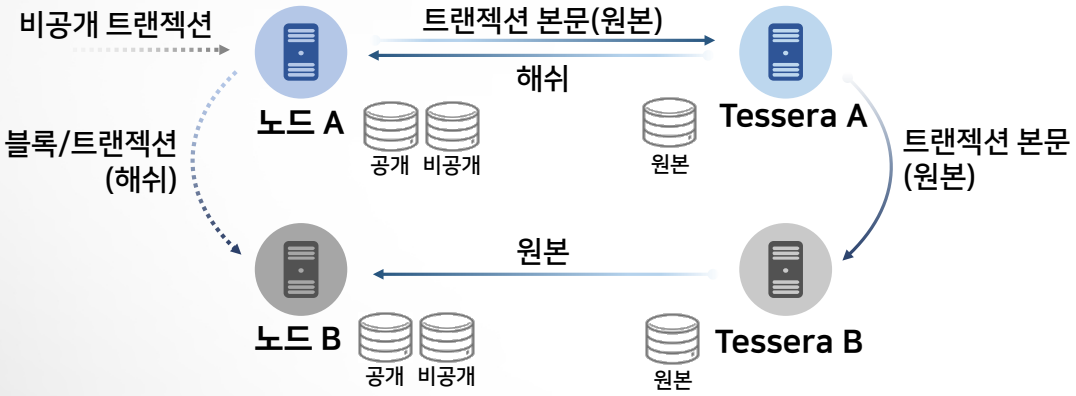
1) DGE : Dynamic Grouping Encryption, 2) ZKP : Zero-Knowledge Proof

앞으로는 어떻게? – 비공개 데이터 별도 처리

트랜젝션 / 스마트컨트랙트 단위 비공개 데이터 공유 범위 지정, 비공개 데이터용 별도 저장소 사용

비공개 트랜젝션 - Quorum

* 삼성SDS 물류 블록체인 플랫폼 - PoC 진행 중

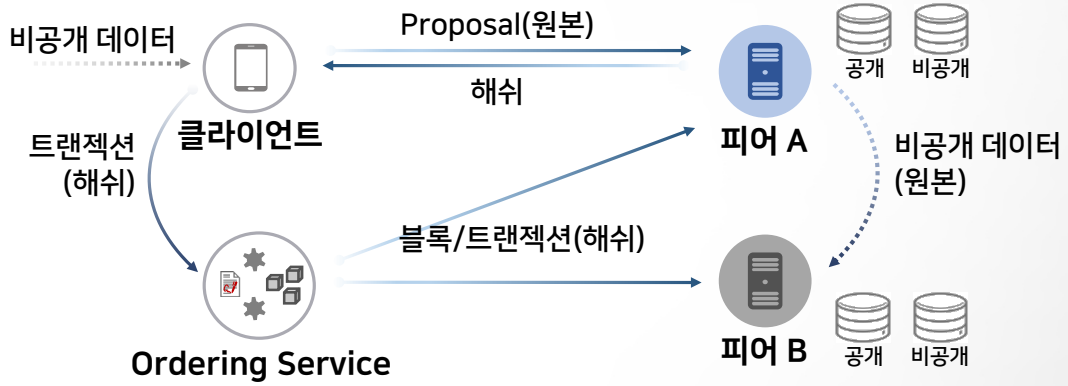


Ex) 비공개 트랜젝션 예시

```
{
  "jsonrpc" : "2.0",
  "method" : "eth_sendTransaction"
  "params" : [{ "from" : "0x01", "to" : "0x02", ··· ,
      "privateFor" : [ "Pubkey1", "Pubkey2" ]
  }],
  "id" : 1
}
```

※ Source : https://github.com/jpmorganchase/tessera/wiki/How-Tessera-works

비공개 데이터 컬렉션 – Hyperledger Fabric



Ex) 비공개 데이터 컬렉션 정의 파일 예시

```
{
  "name" : "collection1",
  "policy" : "OR( 'organization1' )"
  "requiredPeerCount" : 1,
  "maxPeerCount" : 10,
  "blockToLive" : 10,
  "memberOnlyRead" : true
}
```

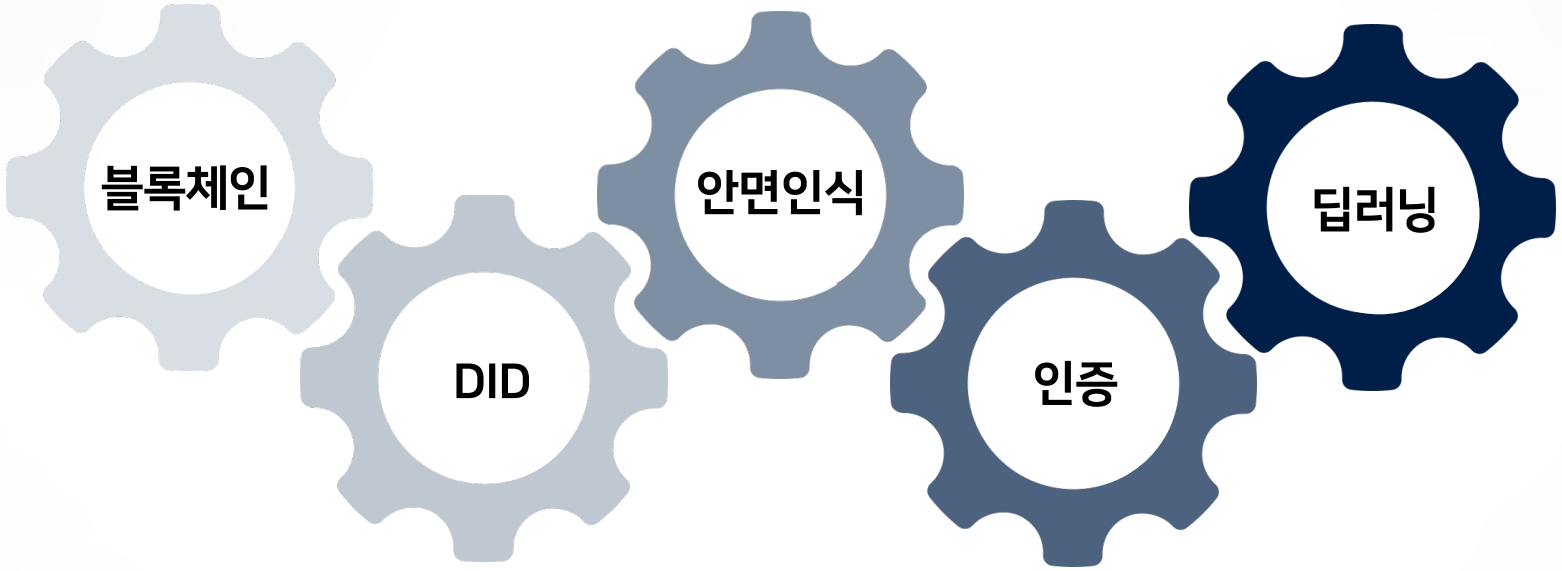
※ Source : https://hyperledger-fabric.readthedocs.io/en/latest/private-data-arch.html

3

사업화 방안

구슬이 서 말이라도 꿰어야 보배

"아무리 훌륭하고 좋은 것이라도 다듬고 정리하여 쓸모 있게 만들어 놓아야 값어치가 있음을 비유적으로 이르는 말"



시장 동향 → 새로운 가치 → 비즈니스 모델

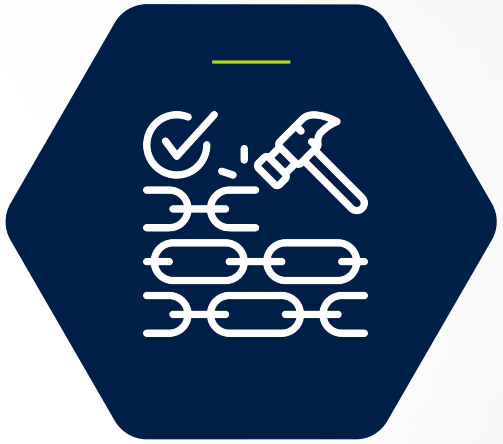
규제 완화에 따른 사업 활성화

규제자유특구를 중심으로 블록체인 사업 및 공공 선도사업 활성화, DID 연합체 출범

특구(부산) 중심
사업 활성화

- 특구(부산)를 중심으로 블록체인 사업 활성화
- 중소벤처기업부에서 신산업 육성을 위해 부산을 블록체인 규제자유특구로 지정(2019.08)

- 규제자유특구에서는 201개 메뉴판식 규제 특례 적용
- 규제 샌드박스 활용, 신사업 검증 또는 제품 출시 가능
- 개인정보 보호법 규제특례 포괄적 적용



블록체인 관련
규제 완화

- 과학기술정보통신부 : 2019년 정부 공공기관 블록체인 공공 선도사업 6개에서 12개로 증가
- 이니셜 DID 컨소시엄, DID 얼라이언스 코리아, My ID 얼라이언스 등 DID 연합체 출범

4

가치창출

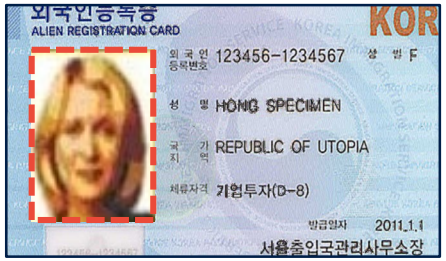
DID - 가치를 더하기 위한 고민

손쉽게 DID를 사용하기 위한 방법에는 무엇이 있을까?

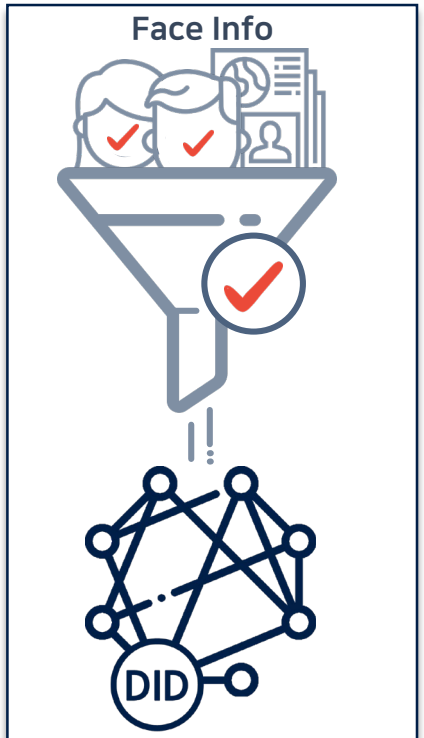
주민등록증

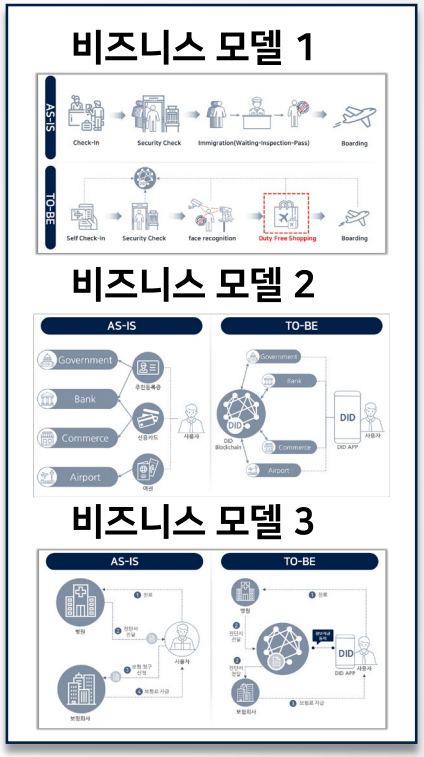
운전면허증

여권



외국인등록증



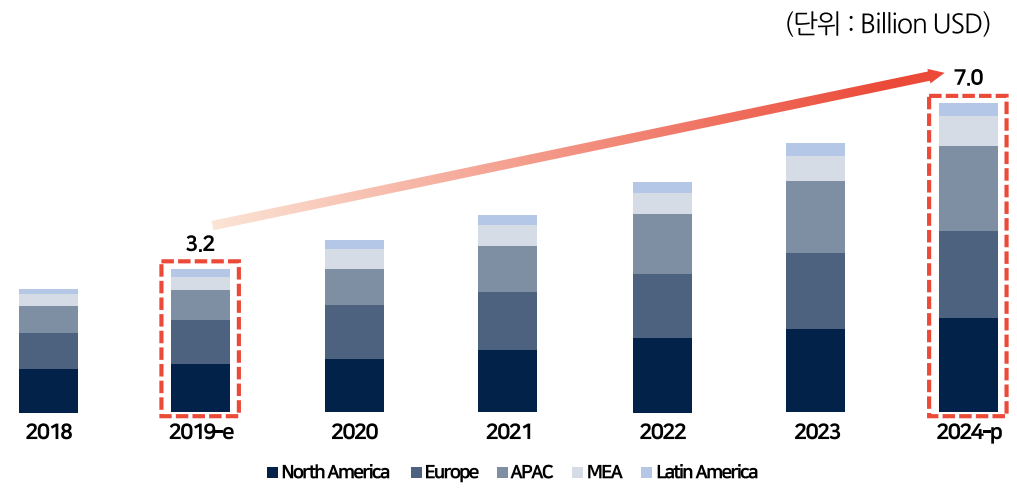


안면정보를 이용하여 사용자를 빠르고 쉽게 식별, DID에 안면인식을 적용하여 다양한 비즈니스 모델 창출

글로벌 안면인식 시장

연평균 16.6% 성장 예상, 편의성이 높아 다양한 분야에서 활용 기대

안면인식 시장 규모



- ‘19년 32억달러에서 ‘24년 70억달러로 성장 예상
- 연평균 16.6%의 성장 달성 예상

※ Source : https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html

다양한 산업에 적용

[Retail]
- 고객이 얼굴을 카메라에 인식하는 방식으로 결제 수행

[Finance]
- 고객 안면인식으로 신분증, PW 대체
- 계좌개설, 이체·결제·송금 등 서비스

[Safety]
- CCTV등 매체를 통해 범죄자 색출 및 테러범 경계

[Transportation]
- 고객 안면인식으로 다양한 교통편 이용
- 입·출국시 안면인식으로 신원확인

위치정보 기반 안면인식

비콘 연동 안면인식 출입통제 시스템, 대형 물류센터 일용직 근로자의 출입환경 개선

사용자 편의성 확보


물류센터


건설 현장


택배

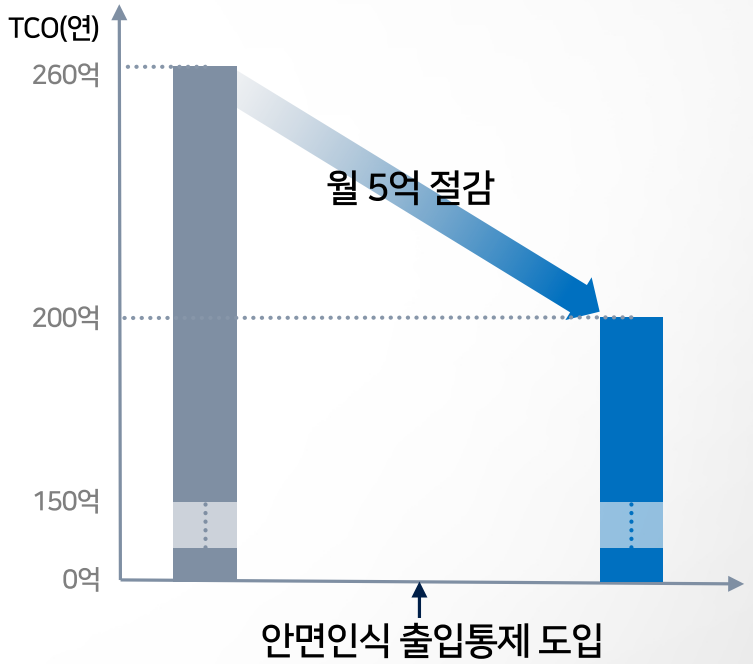
프랜차이즈 매장

근태 관리	출입통제	시스템 인증	전자식권	전자사물함	건강관리
					
• 출퇴근 관리 • 근무 시간, 근태, 급여 정산, 직원 고용 및 계약 등 통합 직원 관리 서비스 제공	• 스피드 게이트 등과 연계하여 외부인 출입통제 • 일회용바코드 등 활용	• 사내 그룹웨어 등 로그인 및 인증 제공 • 온라인 강의 등에 출결 관리로 활용	• 키오스크 등의 단말기와 연계하여 바코드 등을 활용하여 전자식권 발급	• 전자사물함과 연계하여 바코드 등을 활용하여 사물함 개폐	• 출근시 혈압 등의 건강 기록 및 관리

(*일 평균 출근 등록인원 5,000여명 기준)

- 비콘 연동 안면인식 출입통제를 통해 일용직 근로자 출근등록시간 2시간→20분으로 단축
- 근로계약서 작성, 근로자 식권 지급 등 부가서비스 연계 적용

TCO 절감

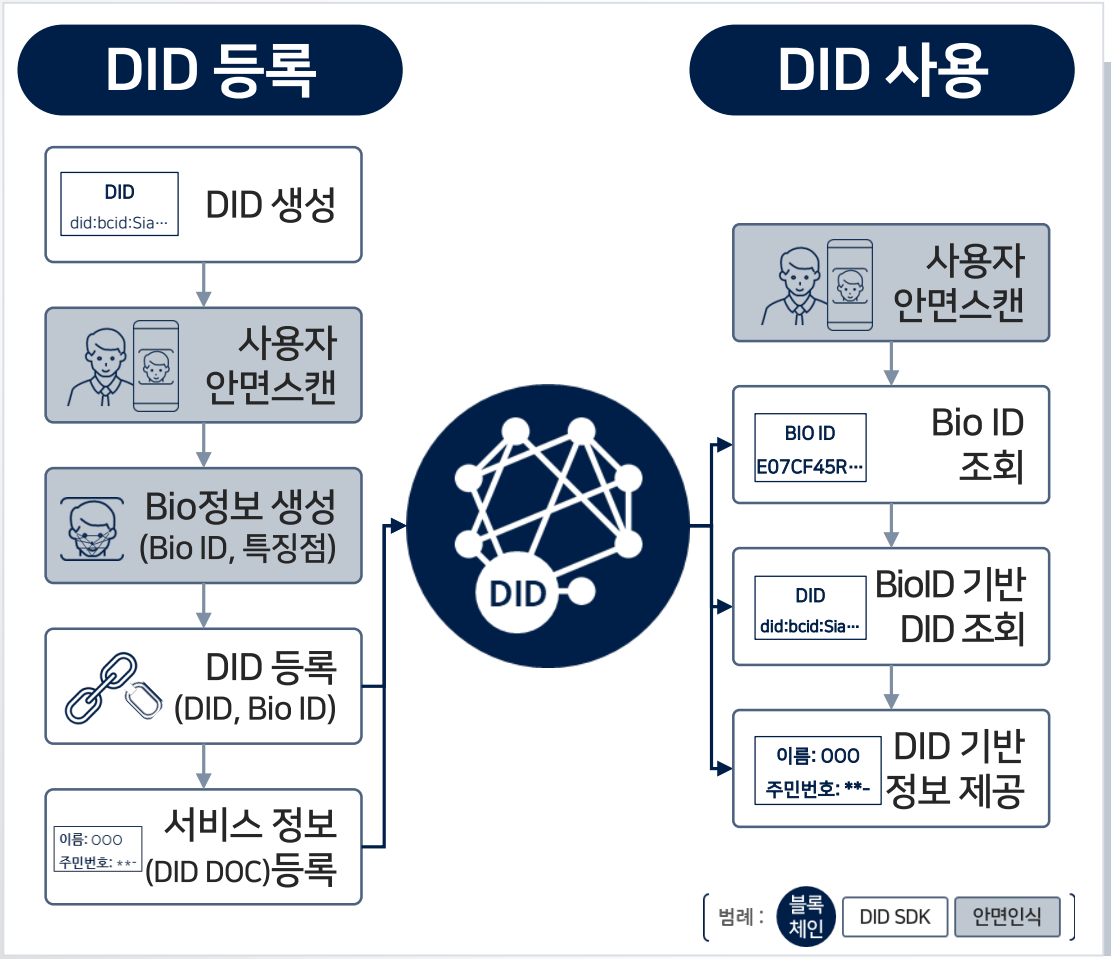


- 출입절차 간소화를 통해 연간 약 60억원 절감

※ TCO : 총소유비용(Total Cost of Ownership)

DID – 보안성과 편의성의 결합

보안성과 사용자 편의성을 동시에 만족할 수 있도록, DID와 안면인식 기술 콜라보레이션
안면인식 기술을 활용한 DID 서비스 상용화 추진



표준

- Verifiable Credentials Data Model 1.0
- Decentralized Identifiers (DIDs) v0.13

DID

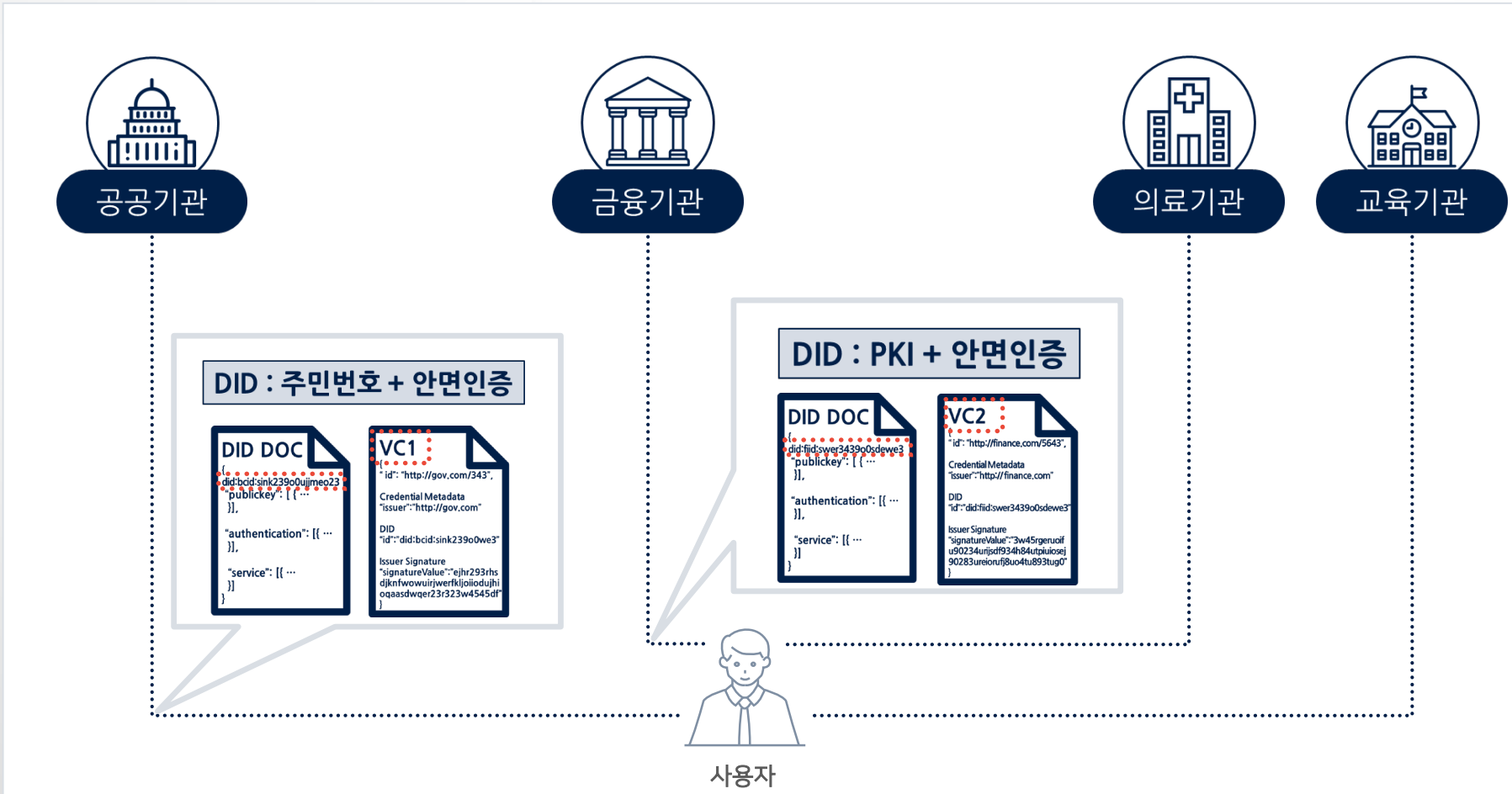
- [Schema:DID Method:DID OIdentifier] 형식
- 키 쌍의 Public Key로 Identifier 생성
- '주민등록번호'의 개념

DID Document(상세정보)

- DID에 상응하는 객체와 암호인증 가능 정보의 집합
- 구성정보 :
  - Public Key (기본)
  - 서비스에 필요한 정보
    (예: 결제서비스에 필요한 Credit ID 등)
  - 정보의 중요도에 따라 off-chain에 저장

DID – 발급 기관 별 다양한 DID 보유 가능

발급기관의 블록체인에 따라 사용자는 다양한 DID 보유 가능
DID에 상응하는 VC(Verifiable Credential) 또한 기관이 제공하는 서비스에 필요한 정보 보유



VC(Verifiable Credential)

- 현실 세계에서의 Credential이 제공하는 정보 전부 포함 (SSI의 주요 요소 중의 하나)
- 즉, 디지털 서명을 통해 정보 변경을 쉽게 확인하고, 신뢰 할 수 있는 체계를 의미함

Credential 구성

- 인증 주체에 대한 정보 (사진, 이름, 주민등록번호 등)
- 발행 주체에 대한 정보 (정부, 국가기관 등)
- Credential 유효기간

5

비즈니스 모델

DID 비즈니스 모델(1/3)

내·외국인 출입국 관리 : 전국 공항,항만 등 내 · 외국인 출입국 절차 간소화 및 내수경제 활성화

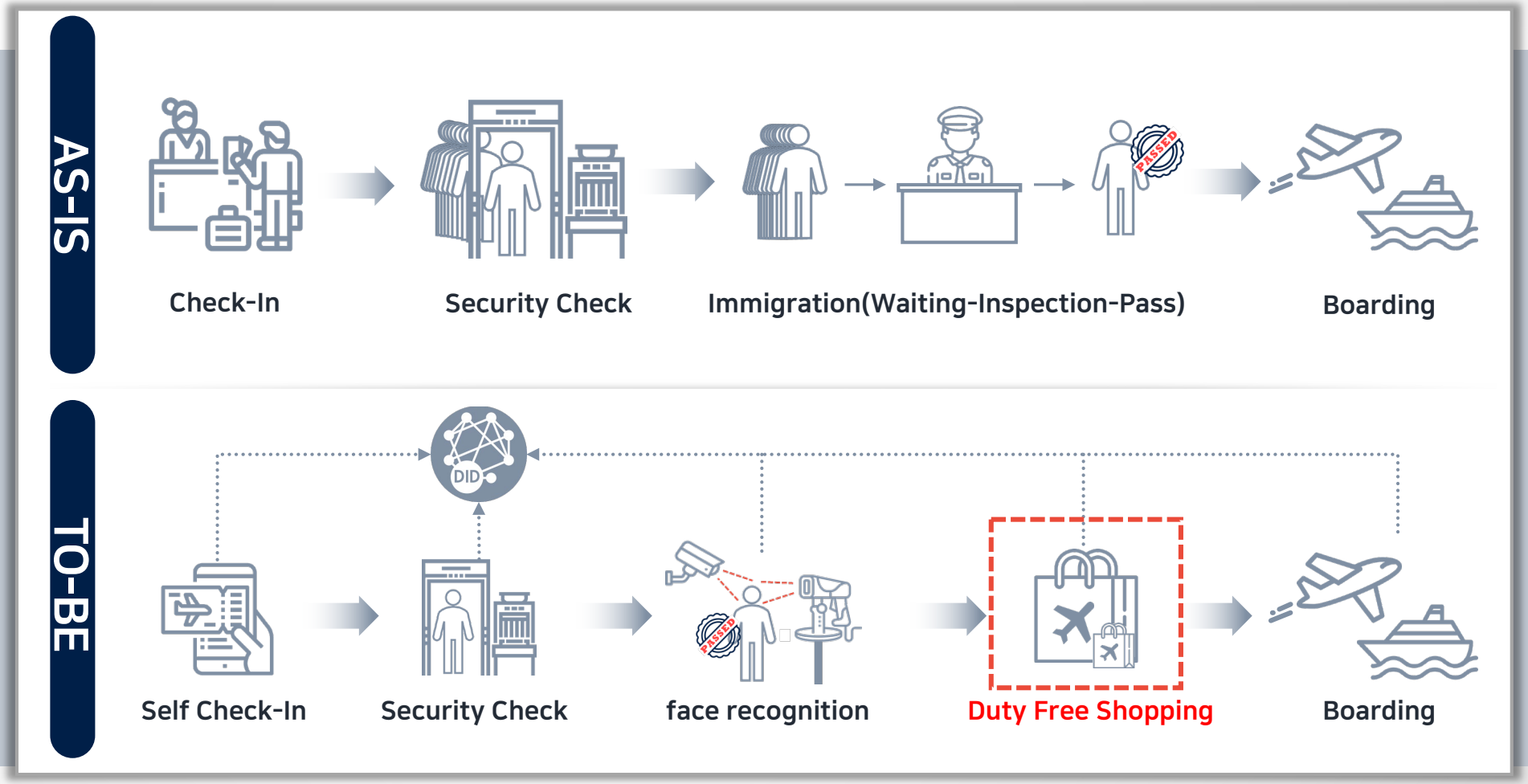
내 외국인 출입국 관리

목적

- 번거로움 없이 신속·정확·안전한 차세대 출입국 수속 실현

기대효과

- 출입국 절차 간소화
- 면세구매 활성화를 통한 내수 경제 활성화



DID 비즈니스 모델(2/3)

신원인증 일원화 : 공공/금융/의료/유통 등 실 생활에 필요한 대민 서비스 인증 통합

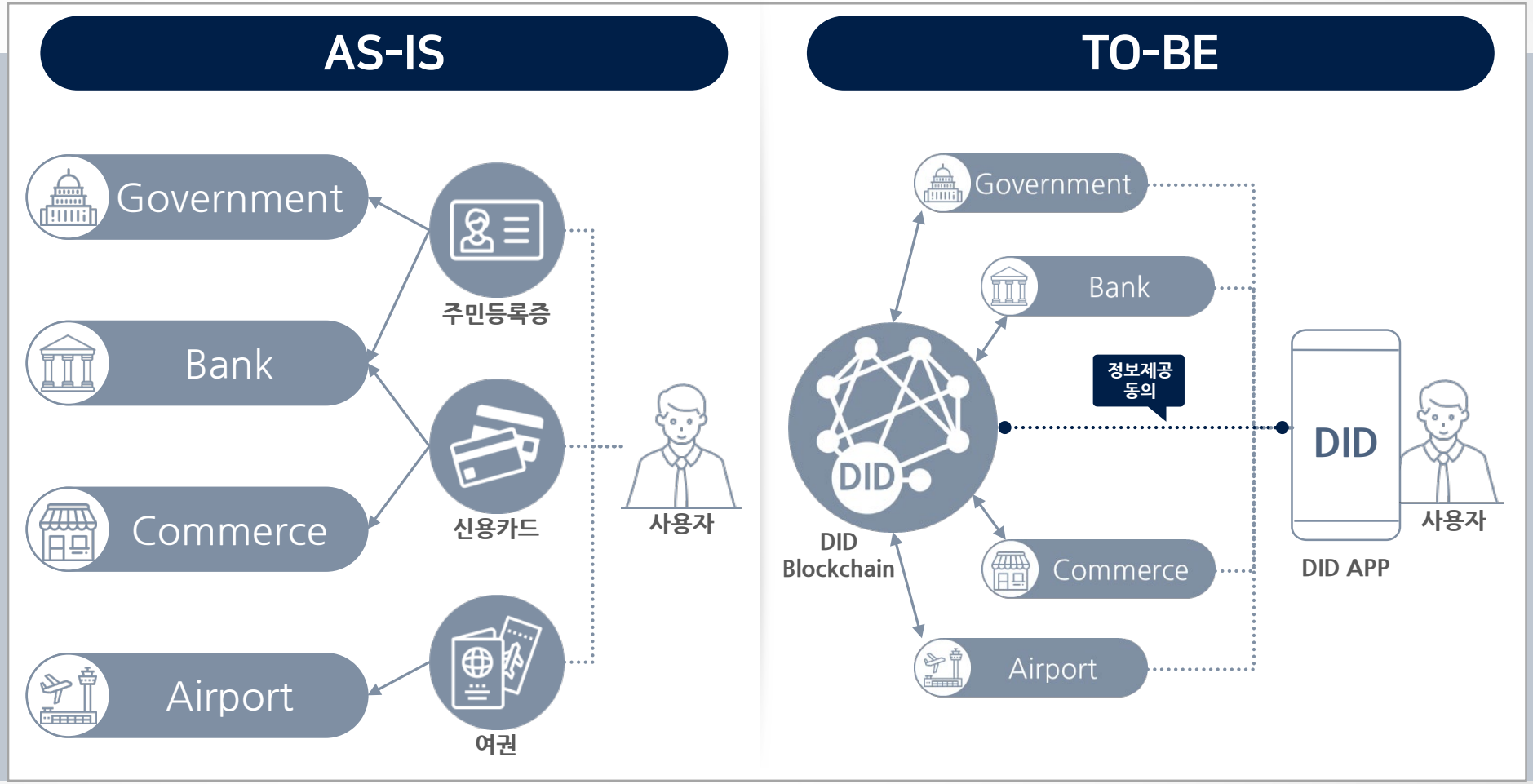
신원인증 일원화

목적

- 실생활에 필요한 대민 서비스의 인증 통합 (자기주권 신원인증)

기대효과

- 개인정보 오남용 방지
- 자기주권형 인증환경 마련
- 사용자 인증 간소화

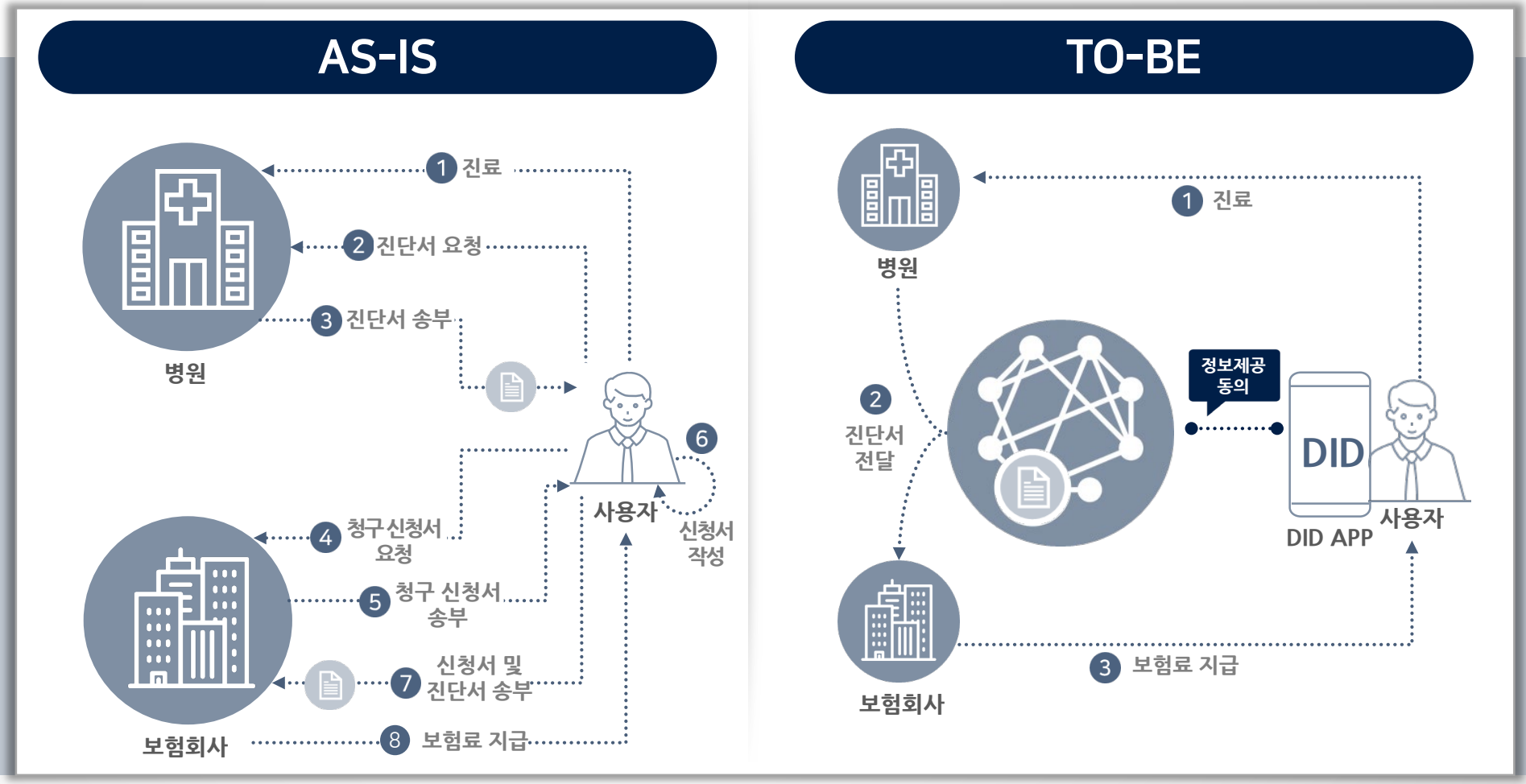


DID 비즈니스 모델(3/3)

의료 서비스 : 병·의원 간 진료정보 연계, 보험금 청구 자동화 서비스

의료 서비스

- 목적
  - 보험금 청구업무 효율화
  - 환자,진료자 편익 제고
- 기대효과
  - 보험금 청구업무 간소화에 따른 업무처리시간 단축
  - 실시간 정보연계를 통한 페이퍼리스 실현

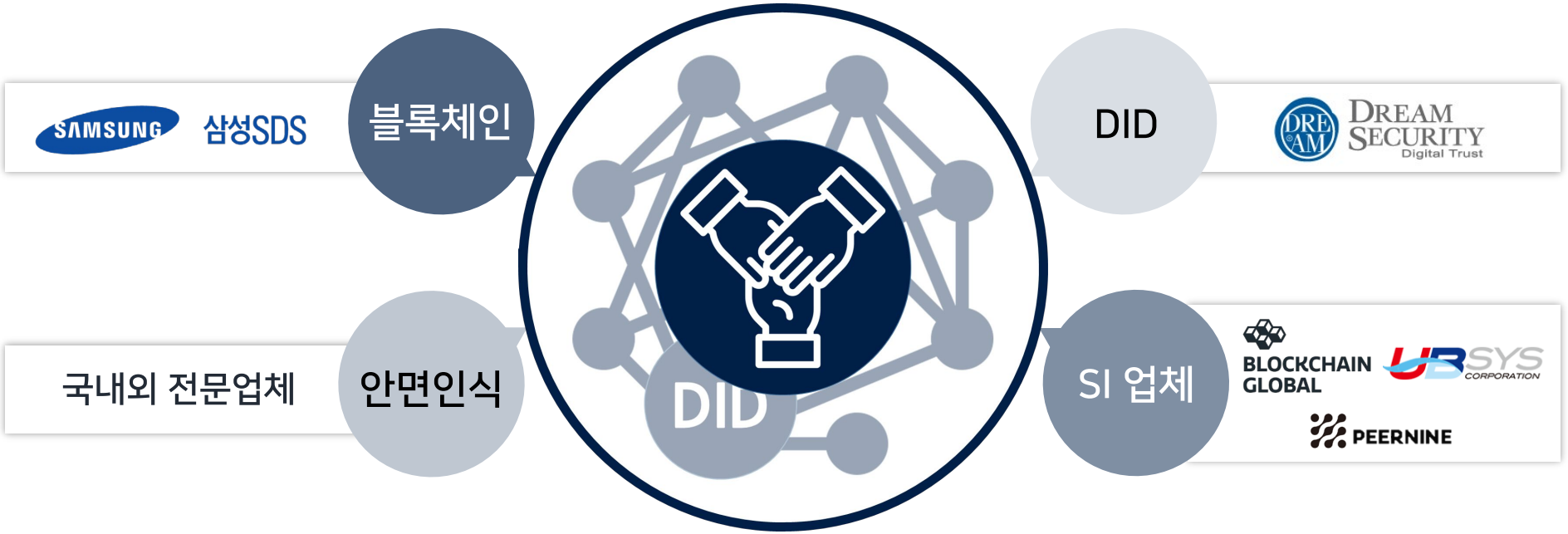


6

협력과 상생

협력과 상생

DID 적용이 가능한 생태계를 중심으로, 각 분야의 전문 기업들 간 협업이 필수



블록체인+DID+안면인식+SI 등 각 분야 전문 업체의 협력 및 상생도모

기대효과

블록체인의 새로운 가치를 창출하고 사용자 주도의 분산ID를 실현하여 다양한 산업에 적용

New-Value

블록체인의
새로운 가치 창출

- 블록체인 기술의 본질에 충실
- 디지털 트랜스포메이션

Decentralized ID

사용자 주도의
분산ID 실현

- 개인정보 오남용 방지
- 생활속의 무자각 분산인증 실현

Various Industries

DID 기술을
다양한 산업에 적용

- 공공/대민, 금융, 의료 서비스 등 다양한 산업에 적용

Thank You

Q & A

Partner Disrupt Foresee