GISC2020
Global ICT Standards Conference

뉴노멀시대 선도를 위한
ICT 표준의 역할

초연결·비대면 신뢰 사회를 위한 분산원장기술 보안표준화 현황

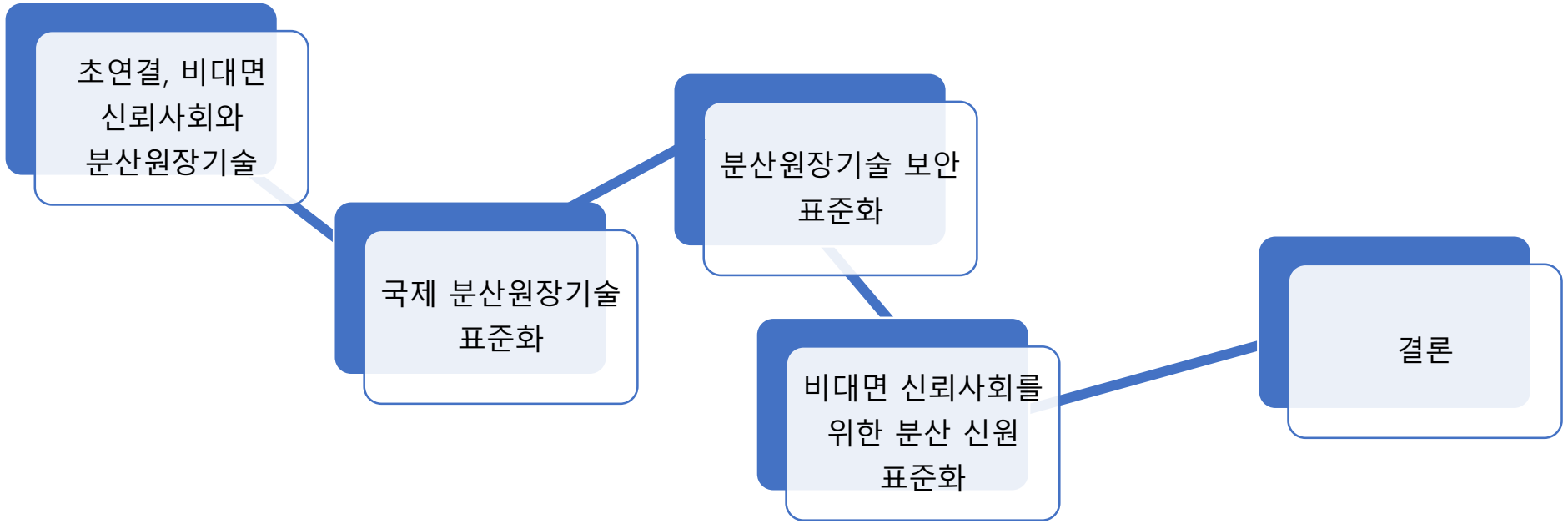
TCA서비스 오경희

khoh@tcaservices.kr
ITU-T SG 17 Q14 Co-Rapporteur
ISO TC 307 IS 23257 Project Leader

GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

목차

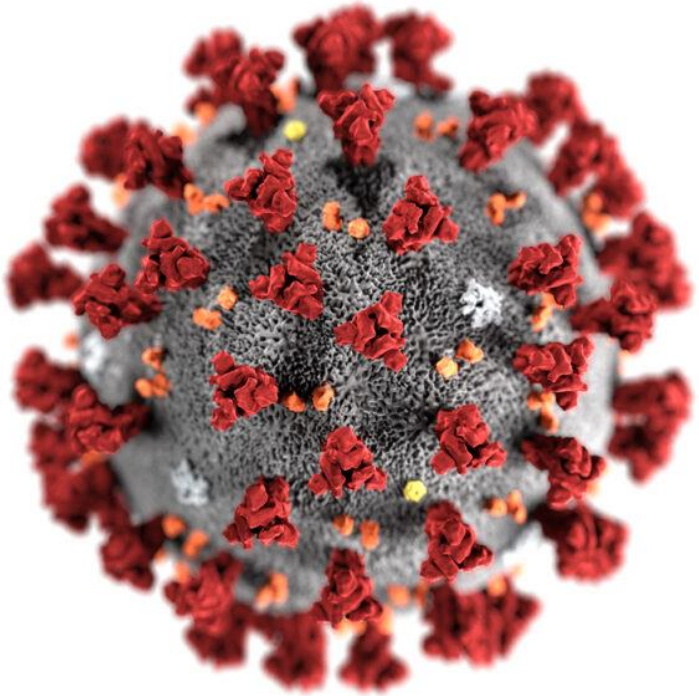


GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

COVID-19

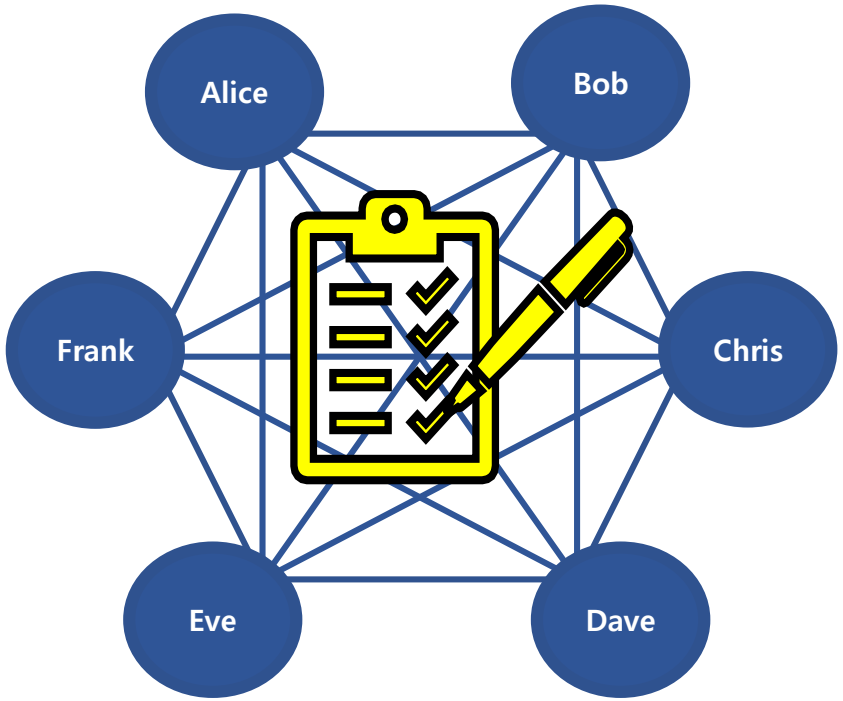
- ✓ 경제사회 전반의 디지털화·비대면화 촉진
- ✓ 온라인 연결성 강화
- ✓ 온라인 상의 상대에 대한 신뢰 방안



분산원장기술

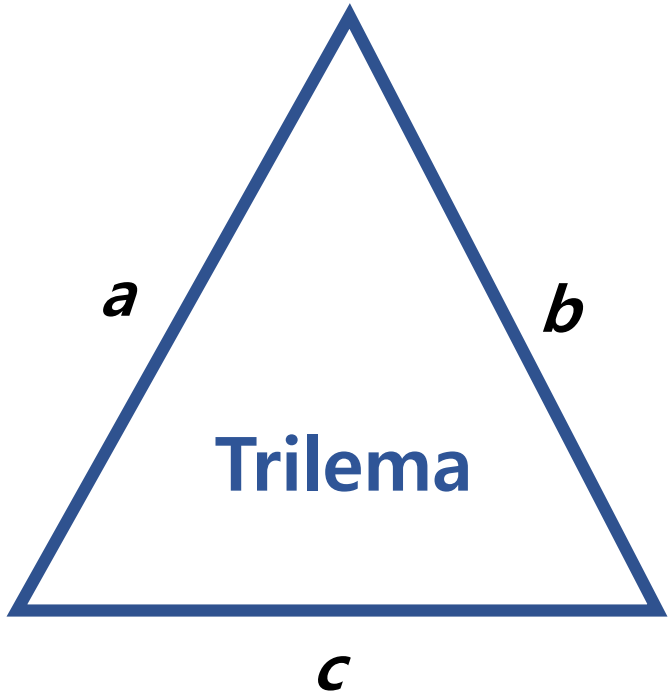
- ✓ 원장(Ledger): 최종적으로 결정된, 변경 불가능한 거래 기록을 유지하는 정보 저장소

- ✓ 제3자 및 상대에 대한 의존 없이
- ✓ 공통의 원장 생성 유지
- ✓ 기술에 대한 신뢰
  - 암호 알고리즘에 의한 보호
  - 분산 합의



기술에 대한 이해

- ✓ 기술에 대한 환상
  - 투명성
  - 불변성
  - 가용성
- ✓ 소통
  - 용어
  - 블록체인?
  - 분산원장?



표준화와 보안

- ✓ 확장성, 상호운영성 필요
  - 플랫폼과 응용 분리 미흡
  - 개발사 및 적용 기술에 따라 분절적으로 구현
  - 확장 및 연동에 한계
- ✓ 운영 안전성
  - 연결성을 위한 신뢰요소 확보

GISC2020
Global ICT Standards Conference

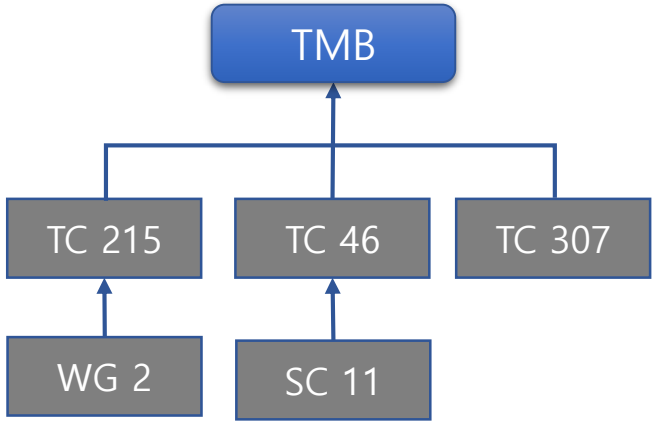
뉴 노멀 시대
선도를 위한
ICT 표준의
역할

분산원장기술 국제 표준화

분류	기구	특징	비고
공식표준화	ISO	민간/전분야	개념/구조/ 상호운용성
	ITU	국가/전분야	
	UN/CEFACT	국가간/무역	
사설표준화	W3C	민간/자기주권ID	기술개발
	IEEE	민간/전분야	
사실표준	EEA	가입형/서비스연계/코인	구현
	Hyperledger	가입형/플랫폼 및 연계	
	EC	유럽 역내외 국가간/구현	

ISO TC 307 – Blockchain and DLT

- ✓ IS 1건, TR 2건 발표
  - IS 22739:2020 Vocabulary
  - TR 23244 Privacy and PII considerations
  - TR 23455 Overview of and interactions between smart contracts ..
- ✓ IS 1건, TS 3건, TR 4건 개발 중
  - IS 23257 Reference architecture
  - TS 23258 Taxonomy and ontology
  - TS 23259 Legally binding smart contracts
  - TS 23635 Guidelines for governance



ISO TC 307 – Blockchain and DLT

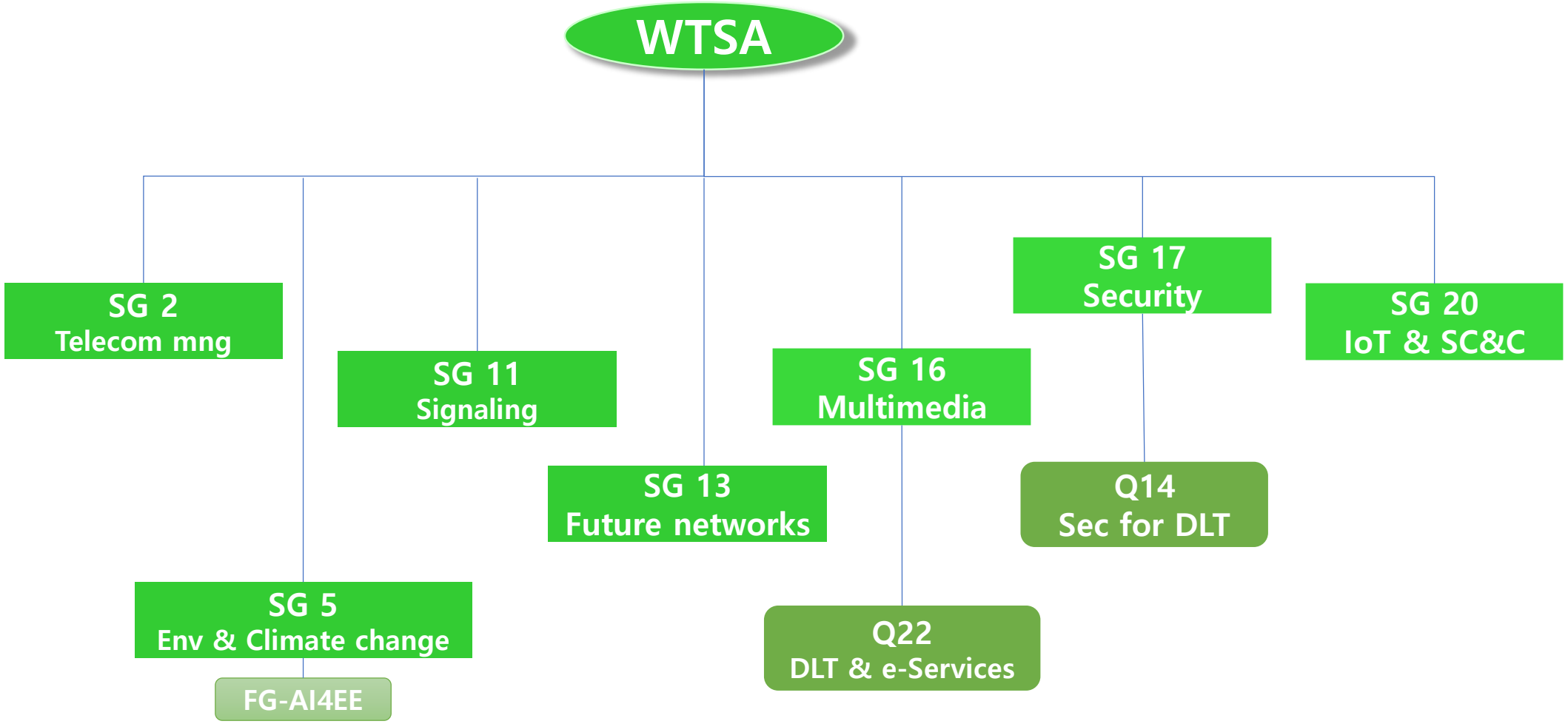
- ✓ IS 1건, TS 3건, TR 4건 개발 중
  - TR 3242 Use cases
  - TR 23245 Security risks, threats and vulnerabilities
  - TR 23249 Overview of existing DLT systems for id management
  - TR 23567 Security management of digital asset custodians

WG 1	WG 2	WG 3	JWG 4	WG 5	WG 6	SG 7	AHG X
Foundations	Security, privacy and identity	Smart contracts and their applications	Joint with JTC 1/SC 27	Governance	Use cases	Interoper-ability	Guidance for auditing..
Geoff Goodell (UK)	Julien Bringer (France)	Volker Skwark (German)	Julien Bringer (France) Sal Francomacaro (US)	Roman Beck (Denmark)	Caroline Thomas (UK)	Gilbert Verdian (UK)	Siddharth Durbha (India)

GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

ITU-T SGs



GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

ITU-T SGs

SGs	Rec #	Title
SG 2	M.rmbs	Requirements for management of blockchain system
	M.immbs	Information model for management of blockchain system
SG 11	O.BaaS-iop-reqts	Interoperability testing requirements of blockchain as a service
SG 13	Y.2342	Cloud computing - Functional requirements for blockchain as a service
	Y.3550	Scenarios and capability requirements of blockchain in next generation network evolution
	Y.SCid-fr	Requirements and Converged Framework of Self-Controlled Identity based on Blockchain
	Y.NRS-DLT-reqts	Scenarios and requirements of network resource sharing based on distributed ledger technology

GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

ITU-T SG 16

SGs	Rec #	Title
SG 16	F.751.0	Requirements for Distributed Ledger Systems
	F. 751.1	Assessment criteria for DLT
	F.751.2	Reference framework for distributed ledger technology
	H.DLT-DEDE	Digital evidence services base on DLT
	F.BVSSI	Scenarios and requirements for blockchain in visual surveillance system interworking
	F.DLT.HC	Requirements of distributed ledger technologies (DLT) for human-care services
	F.DLT.PHR	Service models of distributed ledger technologies (DLT) for personal health records (PHRs)
	F.HFS-BC	Requirements and framework for blockchain-based human factor service models
	F.Supp-OCAIB	Overview of convergence of artificial intelligence and blockchain
	F.DLT-FIN	Financial distributed ledger technology application guideline
	HSTP.DLT-RF	Distributed ledger technology: Regulatory framework
	HSTP.DLT-UC	Distributed ledger technology: Use cases
	HSTP.DLT-GTI	DLT governance and technical interoperability framework
	HSTP.DLT-TFR	Technical framework for DLT regulation
	HSTP.DLT-VERI	Formal verification framework for smart contract
	HSTP.DLT-Risk	DLT-based application development risks and their mitigations
	F.DLIM-AHFS	Requirements of the distributed ledger incentive model for agricultural human factor services
	F.DLS-SHFS	Requirements of distributed ledger systems (DLS) for secure human factor services
	F.Med-VHN	Framework of telemedicine service based on distributed virtual healthcare network

GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

ITU-T SG 17

SGs	Rec #	Title
SG 17	X.1400	Terms and definitions for distributed ledger technology
	X.1401	Security threats of Distributed Ledger Technology
	X.1403	Security considerations for using DLT data in Identity Management
	X.1404	Security assurance for Distributed Ledger Technology
	X.str-dlt	The security threats and requirements for digital payment services based on distributed ledger technology
	X.sct-dlt	Security capabilities and threats of Distributed Ledger Technology
	X.ss-dlt	Security Services based on Distributed Ledger Technology
	X.dlt-sec	Security considerations for using DLT data in Identity Management
	X.sa-dlt	Security assurance for Distributed Ledger Technology
	X.stov	Security threats to online voting using distributed ledger technology
	X.das-mgt	Security framework for the data access and sharing management system based on the distributed ledger technology
	X.tf-spd-dlt	Technical framework for secure software programme distribution mechanism based on distributed ledger technology
	X.srip-dlt	Security requirements for intellectual property management based on distributed ledger technology
	X.srscm-dlt	Security requirements for smart contract management based on DLT
	X.sa-dsm	Security architecture of data sharing management based on DLT
	TR.qs-dlt	Guidelines for quantum-safe DLT system

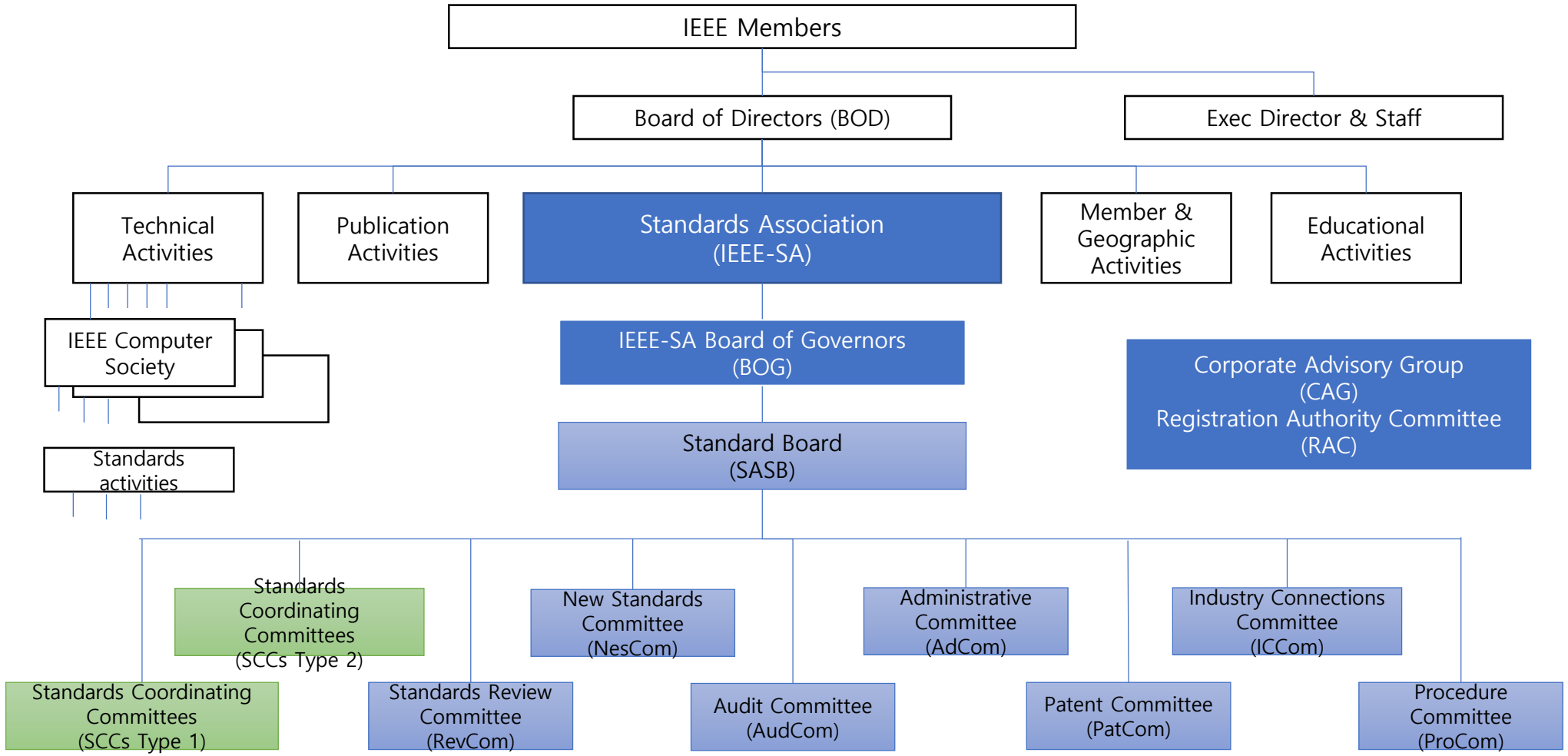
GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

ITU-T SG 20

SGs	Rec #	Title
SG 20	Y. 4464	Framework of blockchain of things as decentralized service platform
	Y.4560	Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities
	Y.4561	Blockchain-based Data Management for supporting Internet of things and smart cities and communities
	Y.4907	Reference architecture of blockchain-based unified KPI data management for smart sustainable cities
	Y.dec-IoT-arch	Decentralized IoT communication architecture based on information centric networking and blockchain
	Y.IoT-rf-dlt	OID - based Resolution framework for transaction of distributed ledger assigned to IoT resources
	Y.BC-SON	Framework of blockchain-based self-organization networking in IoT environments
	Y.blockchain-terms	Vocabulary for blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects
	Y.Suppl.62	Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects

IEEE


IEEE Members
Board of Directors (BOD)
Exec Director & Staff
Technical Activities
Publication Activities
Standards Association (IEEE-SA)
Member & Geographic Activities
Educational Activities
IEEE Computer Society
Standards activities
IEEE-SA Board of Governors (BOG)
Standard Board (SASB)
Corporate Advisory Group (CAG)
Registration Authority Committee (RAC)
Standards Coordinating Committees (SCCs Type 2)
New Standards Committee (NesCom)
Administrative Committee (AdCom)
Industry Connections Committee (ICCom)
Standards Coordinating Committees (SCCs Type 1)
Standards Review Committee (RevCom)
Audit Committee (AudCom)
Patent Committee (PatCom)
Procedure Committee (ProCom)

IEEE

WGs	#	Title
BACWG – Blockchain Against Corruption Working Group	P2141.1	Standard for the Use of Blockchain in Anti-Corruption Applications for Centralized Organizations
	P2141.2	Standard for Transforming Enterprise Information Systems from Centralized Architecture into Blockchain-based Decentralized Architecture
	P2141.3	Standard for Transforming Enterprise Information Systems from Distributed Architecture into Blockchain-based Decentralized Architecture
EIBCTWG – E-Invoice Business Using Blockchain Technology Working Group	P2142.1	Recommended Practice for E-Invoice Business Using Blockchain Technology
TIDMWG – Trusted IoT Data Management Working Group	P2144.1	Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management
	P2144.2	Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management
	P2144.3	Standard for Assessment of Blockchain-based Internet of Things (IoT) Data Management
BCGOVWG-Blockchain Governance Working Group	P2145	Blockchain governance standards

IEEE

WGs	#	Title
Blockchain WG	P2418.1	Standard for the Framework of Blockchain Use in Internet of Things(IoT)
DBC WG – Data Format for Blockchain Systems	P2418.2	Standard Data Format for Blockchain Systems
DTLA WG – Distributed Ledger Technology in Agriculture	P2418.3	Standard for the Framework of Distributed Ledger Technology(DLT) Use in Agriculture
DTLCAV WG – Distributed Ledger Technology in Connected and Autonomous Vehicles	P2418.4	Standard for the Framework of Distributed Ledger Technology(DLT) Use in Connected and Autonomous Vehicles(CAVs)
BCE WG – Blockchain in Energy	P2418.5	Standard for Blockchain in Energy
BDLTH WG – Blockchain and Distributed Ledger Technology(DLT) in Health	P2418.6	Standard for the Framework of Distributed Ledger Technology(DLT) Use in Healthcare and the Life and Social Sciences
BSCF WG – Blockchain in Supply Chain Finance	P2418.7	Standard for the Use of Blockchain in Supply Chain Finance
BGA WG – Blockchain for Government Affairs	P2418.8	Standard for Blockchain Applications in Governments
CBSTWG – Cryptocurrency Based Security Tokens Working Group	P2418.9	Standard for Cryptocurrency Based Security Tokens
DAWG – Digital Asset Working Group	P2418.10	Standard for Blockchain-based Digital Asset Management

IEEE

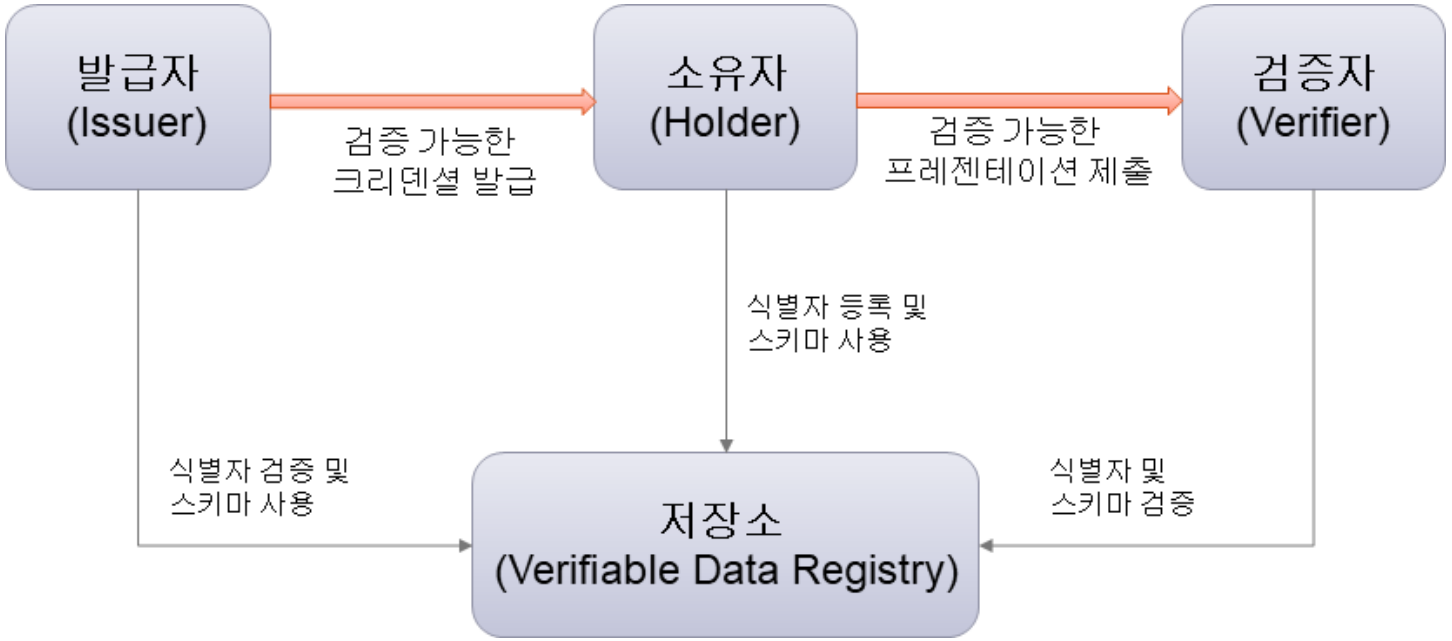
WGs	#	Title
Cryptocurrency Exchange Working Group (CEWG)	P2140.1	Standard for General Requirements for Cryptocurrency Exchanges
	P2140.2	Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges
	P2140.3	Standard for User Identification and Anti-Money Laundering on Cryptocurrency Exchanges
	P2140.4	Standard for Distributed/Decentralized Exchange Framework using DLT (Distributed Ledger Technology)
	P2140.5	Standard for Custodian Framework of Cryptocurrency
Cryptocurrency Payment Working Group (CPWG)	P2143.1	Standard for General Process of Cryptocurrency Payment
	P2143.2	Standard for Cryptocurrency Payment Performance Metrics
	P2143.3	Standard for Risk Control Requirements for Cryptocurrency Payment

블록체인 표준화 추세

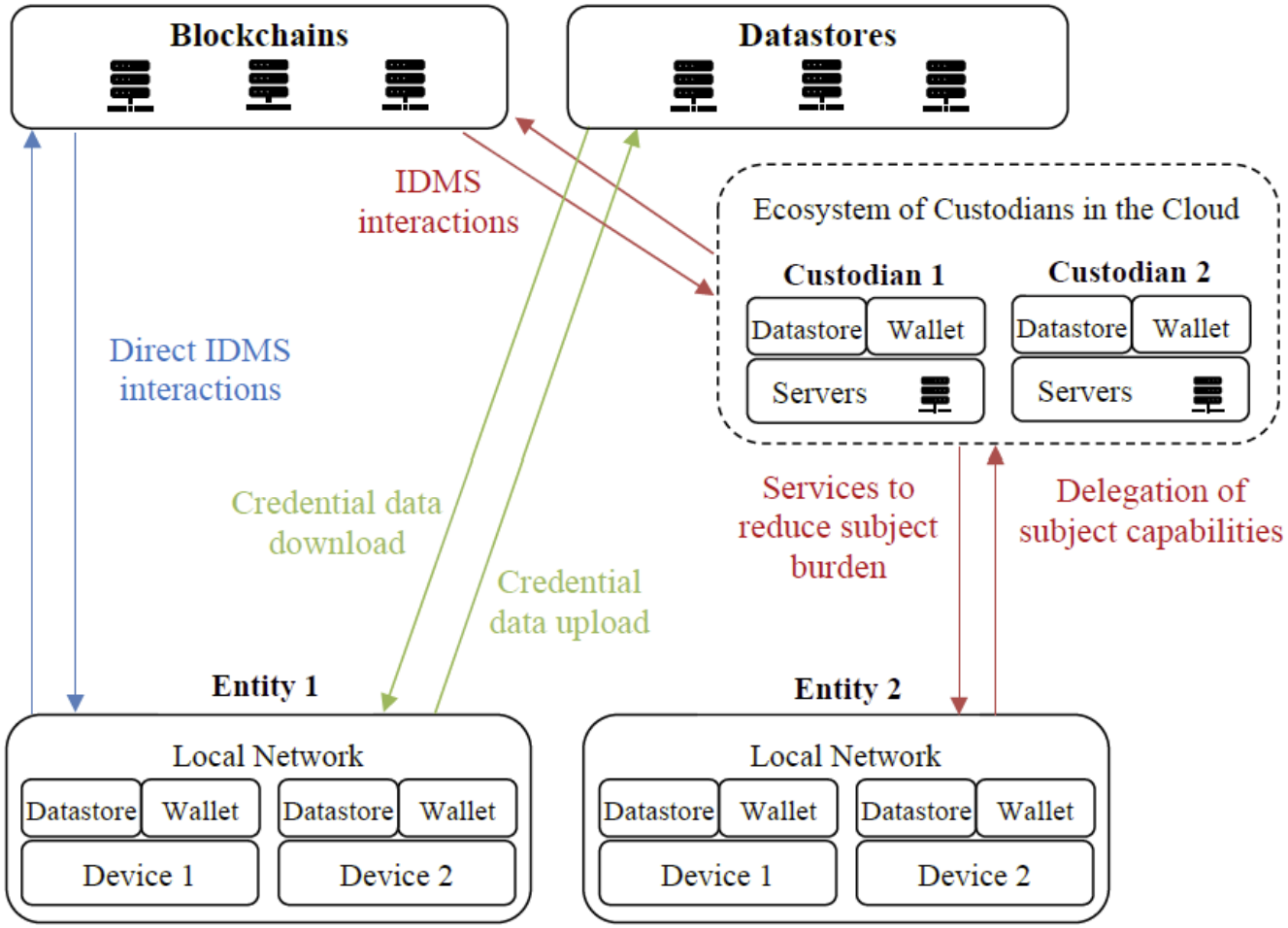
- ✓ 기초에서 상호운용성으로
  - 용어, 참조구조 기반
  - 유스케이스, 거버넌스, 스마트 컨트랙트 등 기술 분야별 연구
  - 상호운용성으로 확장
- ✓ 보안
  - 실제 사고 및 이론에 기초한 위협 분석
  - 개인정보보호 등 응용 분야별 보안 요구사항
  - 아키텍처에 기초한 취약성 분석 및 통제 개발 필요
  - 상호 연결을 위한 보안 심사 연구 필요

분산 신원 표준화 – W3C

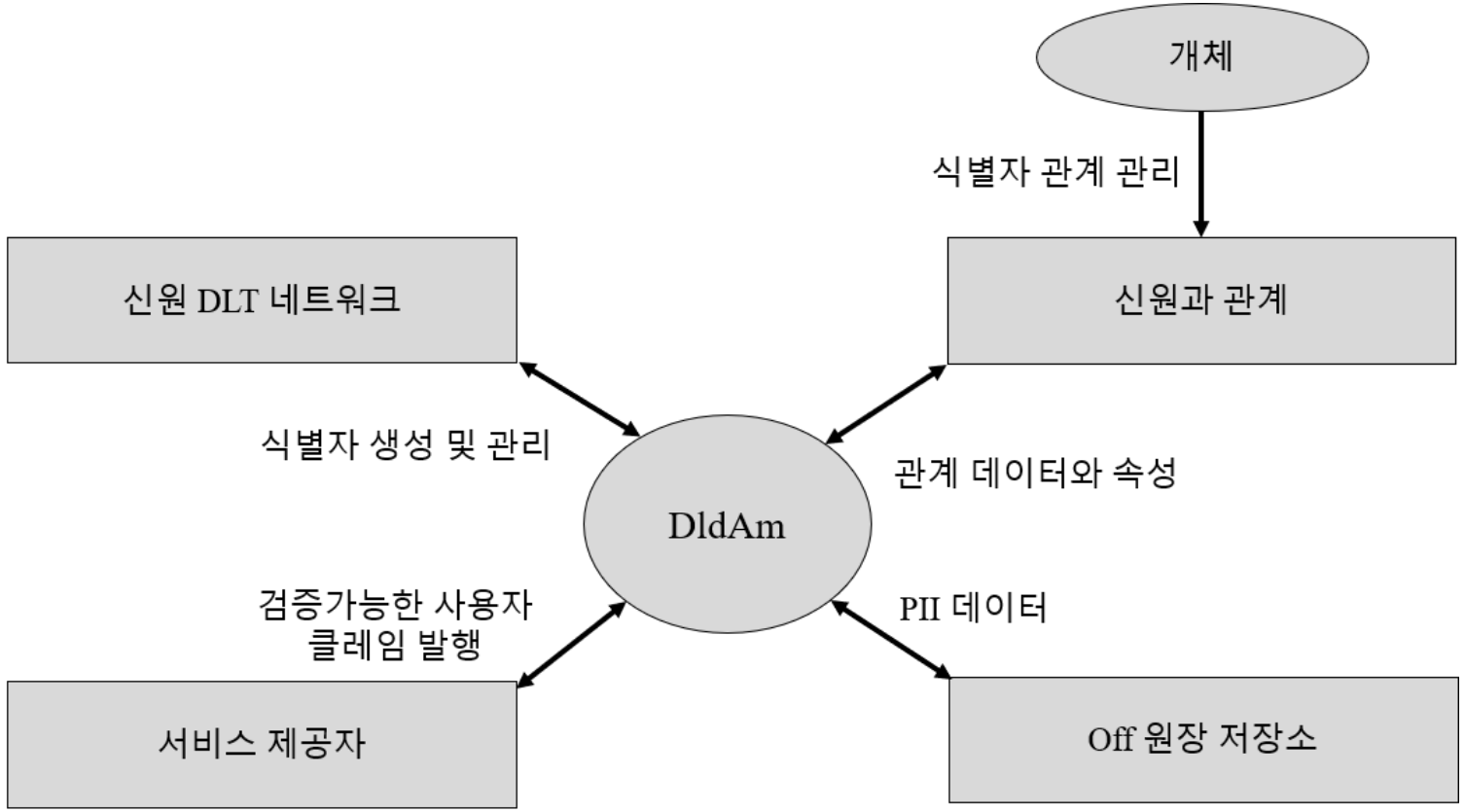
✓ W3C 표준 기반



분산 신원 표준화 - NIST



분산 신원 표준화 – ITU-T



* **DldAm** : Decentralized identity and Access Management System
분산형 신원 및 접근관리 시스템

GISC2020
Global ICT Standards Conference

뉴 노멀 시대
선도를 위한
ICT 표준의
역할

결언: 현실의 문제

- ✓ 국제 표준 추세 모니터링, 준용 및 주도
  - 글로벌 블록체인 네트워크에 연계
- ✓ 의사결정자들의 기술 이해
  - 스마트 계약과 오라클 문제
  - 컨센서스 알고리즘
  - 유용한 활용사례
  - 구현방법론 및 감사
- ✓ Industrial vs. Institutional Technology