블록체인 ID, 보안 및 개인정보보호

나재훈 응용보안/평가인증 프로젝트 그룹(PG504) 의장
ITU-T SG17 WP4 부의장
ISO TC307 전문위원
한국전자통신연구원(ETRI) 정보보호연구본부 전문위원

1. 머리말

이제는 블록체인/DLT(Distributed Ledger Technology) 용어는 ICT(Information and Communication Technology) 분야에서 일상적으로 접할 수 있는 상용어가 되었다. 국제적으로 전문가들이 블록체인/DLT 기술을 더욱 발전시키며, 보다 안전하게 산업에 적용하기 위해 다각적인 방법을 모색하고 있다. 블록체인/DLT 산업이 발전하기 위한 여러 가지 요소를 생각해 볼 수 있으며, 그 중 안전성과 신뢰성을 보장하는 것은 블록체인/DLT 기술과 산업의 미래를 결정 할 수 있는 매우 주요한 요소라고 판단 된다. 안전성과 신뢰성을 제공하기 위한 표준화 기구 중 ISO TC307(블록체인/DLT) 표준화 기구 활동을 중심으로 기술 및 표준화 진행을 살펴보고자 한다.

2. 블록체인(Blockchain)과 정보보호

블록체인/DLT는 P2P(Peer-to-Peer) 기술을 기반으로 데이터(트랜잭션)에 대한 신뢰(Trustness)를 제공하는 기술이다. 중앙의 서버가 없이, 독립된 엔티티(Entity)가 공유를 통하여 데이터의 무결성(Integrity)을 보장하는 기법이다. 블록체인의 처리 기본단위는 트랜잭션(Transaction)이며, 이 데이터에 대한 무결성을 암호처리 기법인 해시(Hash)를 이용하여 한번 기록하여 확정하면, 변경을 할 수 없는 기술적 특징을 갖는다. 트랜잭션들에 대하여 해시함수를 적용하여 생성한 해시값을 자신의 블록에 저장하고, 또 이전 블록의 해시값을 저장하고 연결하므로 블록체인이 만들어지며, 모든 참가자들은 모든 트랜잭션에 대한 전체 기록(Record)을 공유하게 된다. 이러한 방식으로 만들어진 블록체인은 분산 환경으로 한 참여자에 의하여 데이터를 제어할 수 없으며, 중앙 서버가 없는 탈중앙 방식으로 단일 서버의 다운과 같은 문제가 해결이 된다. 그러나 블록체인은 모든 문제를 푸는 요술 기술은 아니며, 아직 더 연구가 필요한 기술이다.

또 블록체인/DLT는 익명(Anonymity) 서비스를 제공한다. 참여자가 만든 공개키 쌍을 기반으로 참여자는 개인의 계정을 만든다. 이 계정은 공개키를 재료로 암호해시를 수행하여 산출된 해시값을 계정

으로 사용한다. 이러한 계정은 식별절차나 인증절차 없이 만들어지며, 참여자의 계정으로 사용된다. 즉 계정의 소유자가 누구인지를 알 수가 없는 기술적 절차이다. 그러나 시스템 내부에서 모든 트랜잭션은 투명하여, 추적이 가능하다. 각 계정은 투명하며(익명성이 없으나), 참여자는 개인 키를 가지고 계정에 접근이 가능하며, 개인 키를 가진 참여자에 대한 식별절차가 없으므로 익명성을 제공하게 되는 것이다. 즉, 비신뢰 공간에서, 서로 모르는 참여자 간에 트랜잭션의 신뢰를 구축하여 사업(business)이 가능하게 하는 것이다.

3. 보안

일반적으로 보안 목적이 정의된 후, 그러한 보안 목적을 달성하기 위한 보안 관리 프로세스가 수행된다. 그러나 현재 블록체인/DLT 관련 여타 기술 표준 기구에서 확인된 보안 목적이 없으며 아직 논의 중에 있다. 본 절에서는 블록체인/DLT 시스템에 관련된 보안 리스크와 취약점에 대해 소개한다.

블록체인/DLT 시스템은 토렌트와 같은 프로토콜 및 합의 메커니즘을 통해 노드 간에 공유하고 동기화하여 순차적 데이터를 저장하는 분산 연결 노드로 구성된다. 각 노드는 지정된 암호화 작업을 수행하는 암호화 모듈이 있다. 이러한 기본 구조에 따라 다음과 같은 일반적 보안 요소를 고려 한다.

- **네트워크 보안**
  - 인증 및 인가(Authentication and authorization)
  - 접근제어(Access control)
  - 침입 탐지(Intrusion Detection)
  - 목표 공격 방지(Targeted attack resistance)
  - 데이터 전파 공격 방지(Data propagation attack resistance)
- **암호화 알고리즘 및 프로토콜의 선택 및 구성**
  - 암호화 알고리즘 및 프로토콜의 손상/취약성 방지 (Compromise/vulnerability resistance in cryptographic algorithms and protocols)
- **암호 키 관리**
- **보안 관리 프로세스**
  - 리스크 분석(Risk analysis)
  - 위협 모델링 및 완화 (Threat modelling and mitigation)
  - 감사(Audit)
- **안전한 구현 및 인증**
- **가용성**

또한 블록체인/DLT 관련 보안 요소를 검토하면, 블록체인 프로토콜의 모든 보안이 완벽하게 구성되지 않는다. 이것은 블록체인/DLT의 복잡한 보안 모델로 인한 결과이며 더 많은 연구와 프로토콜에 대한 검증을 필요로 한다.

키 수명주기 관리 프로세스는 PKI와 같은 일반 암호화 응용 프로그램과 다르다. 예를 들어 일부 암호화폐 프로토콜에는 키 해지 프로세스가 없다. 따라서 블록체인/DLT에 대한 키 수명주기 관리의 새로운 표준 모델 정의가 필요하다.

권한 없는(Permissionless) 블록체인/DLT 시스템의 경우, 제3의 신뢰자 없이 합의 알고리즘이 트랜잭션의 유효성을 보장한다고 가정한다면, 이러한 합의 메커니즘은 분산장부에 저장된 데이터 및 트랜잭션이 신뢰할 수 없는 노드/플레이어(예: PoW 알고리즘의 경우 50%나 그 이하의 채굴권을 가진 노드)에 의해 손상되지 않았음을 보장해야 한다. 다음 사항은 블록체인/DLT가 고려해야 하는 보안요소이다.

- **합의 보안**
  - 51%의 공격 또는 유사한 다수의 합의 공격 (51% attack or similar majority consensus attacks
  - 합의 스푸핑(Consensus spoofing)
- **하드/소프트 포크 관리**
- **블록 데이터 관리**
  - 해시 알고리즘 관리(Hash algorithm management)
  - 월렛 키 관리(Wallet key management)
  - ID/주소 키 쌍 관리(Identity/address Key pair mgt)

3.1 취약점

블록체인/DLT 시스템 관련 알려진 취약점은 배포된 시스템의 감사 또는 학술 연구의 결과로부터 취합된 내용이다. 블록체인/DLT 시스템의 사용은 참가자들 간의 협업을 가정하기 때문에 기존의 취약성 목록은 일반적인 사이버 보안 취약점뿐만 아니라 사회 및 경제적 측면의 취약점도 포함하여야 한다.

3.1.1 사용자 측면 취약점

○ 사용자 앱 취약점: 사용자는 키, 자격 증명이 저장되는 사용자의 지갑을 통해 원장과 통신하므로 개인 키를 도용하거나 파괴 하는 지갑 도둑은 치명적이다.

○ 관리자 앱 취약점: 블록체인/DLT 시스템은 대개 사용자(일반적으로 광부라고 함)가 관리한다. 광부에게 돈을 지불함으로써 뇌물 공격을 수행하는 것이 가능하다.

3.1.2 API 측면 취약점

○ 외부 인터페이스 취약점: 오프 체인 시스템과의 통신은 취약점의 원천이 될 수 있다. 장부에 대한 안전한 오프 체인 데이터 처리가 필요하다.

○ 사용자 API 취약점

○ 관리자 API 취약점: 최근 마이닝 장비에 대한 공격은 제어 인터페이스의 저 수준 보안을 악용하여 공격자는 장치를 완전히 제어 할 수 있다. 예를 들면 장치를 자체 지갑에 바인딩 할 수 있다.

3.1.3 블록체인/DLT 플랫폼 측면 취약점

○ 트랜잭션 시스템 취약점: 신뢰할 수 있는 상대방이 없으면 트랜잭션의 정확성을 확인하기가 어려워 공격자는 유효성 검사에 영향을 주는 트랜잭션을 변경할 수 있다.

○ 합의 메커니즘의 취약점: 지금까지 제안되고 또 배포된 합의 메커니즘이 많이 있지만, PoW, PoS 및 BFTA 협의의 주된 위협 중 하나는 신뢰자가 없어 우려되는 이중 지출이다.

- **피니 공격**(finney attack): 악의적 광부(Miner)는 상인으로부터 제품을 받는 즉시 이중 지출 목적으로 사전 채광된 블록을 방송
- **무차별 공격**(brute force attack): 광부는 개인적으로 긴 블록체인 포크를 채굴하여 이중 지출을 시도
- **경쟁 공격**(race attack): 거래 생성과 일치 메커니즘에 의한 확인 사이의 지연을 이용한다. 공격자는 실제 확인 전에 다른 수신자에게 지연 없이 트랜잭션을 보낼 수 있음
- **벡터 76 또는 한 번의 확인 공격**: 경쟁 공격과 피니 공격의 조합이다. 악의적 광부가 특정 주소의 트랜잭션을 블랙리스트에 올리려고 함
- **50% 해시 파워 또는 골드 핑거 공격**: 공격자가 블록체인에서 계산 능력의 50% 이상을 제어하여 자신의 의지에 따라 합의 결정을 내림
- **이기적 채광 공격**(Selfish mining attack): 광부는 부적절한 인센티브를 얻기 위해 처리된 블록을 보류
- **코인 호핑 공격**(Coin-hopping attack): 광부는 처리된 블록의 검증 확률을 높이기 위해 프로토콜 해시 비율을 변경

- **지불 증명(proof-of-stake)**: 시스템에서는 비용(예: 전력)이 블록 유효성 확인에 관여하지 않기 때문에 광부가 모든 포크에서 쉽게 이중 지출을 유발하도록 마이닝 함으로 무분별 공격(a nothing at stake attack)을 수행
- **BFT(Byzantine Fault Tolerance)**: 1/3 이상의 악의적 노드가 프로토콜 오류를 발생

○ 회원 서비스 취약점: 시빌(Sybil) 공격에서 공격자는 자신의 존재를 감추기 위하여 네트워크에서 여러 개의 가상 신원을 만든다.
○ 이벤트 배포 취약점: 작업 증명 시스템에서 어려움은 블록 확인 간의 시간이다. 그 시간을 사용하여 공격자가 속도를 올리거나 주요 광부의 시계를 조정하여 그 문제에 영향을 미칠 수 있다.
○ 암호화 서비스 취약점: 암호화 서비스 취약점은 암호화 알고리즘 및 프로토콜의 설계, 구현 및 사용과 관련된 공통적인 취약점이다.
○ 원장 취약점
○ 상태 관리 취약점
○ 노드간 통신 취약점
○ 스마트 컨트랙트 취약점: 스마트 컨트랙트 논리 알고리즘에서 설계자는 스마트 컨트랙트 알고리즘의 모든 가능한 입력/출력을 고려하지 못하기 때문에, 잘못된 동작이 발생한다.

3.1.4 인프라 측면 취약점

○ 저장소 취약점: 장부에 저장된 데이터의 손상은 노드 장부의 무결성을 파괴하여, 장부를 무용하게 한다.
○ P2P 네트워크 취약점: 블록체인/DLT의 분산된 특성은 공격자에게 네트워크 탐색이 가능하도록 열려있다. 정보의 보급(공유)을 적절하게 변경하면 네트워크를 통해 효과적이고 저비용의 공격을 수행한다. DDoS 공격 중 공격자는 많은 트랜잭션을 전송하여 네트워크 리소스를 소모한다. 이클립스(eclipse) 경우나 네스프릿(netsplit) 공격에서 공격자는 피해자의 수신 및 발신 연결을 모두 독점하여 실제 장부를 인식하지 못하게 한다. 네크워크 트래픽에 대한 간섭을 하여, 특정 노드에 대한 트랜잭션 및 블록 전파를 지연시켜, 합의에 영향을 미친다.

4. ID(Identity)

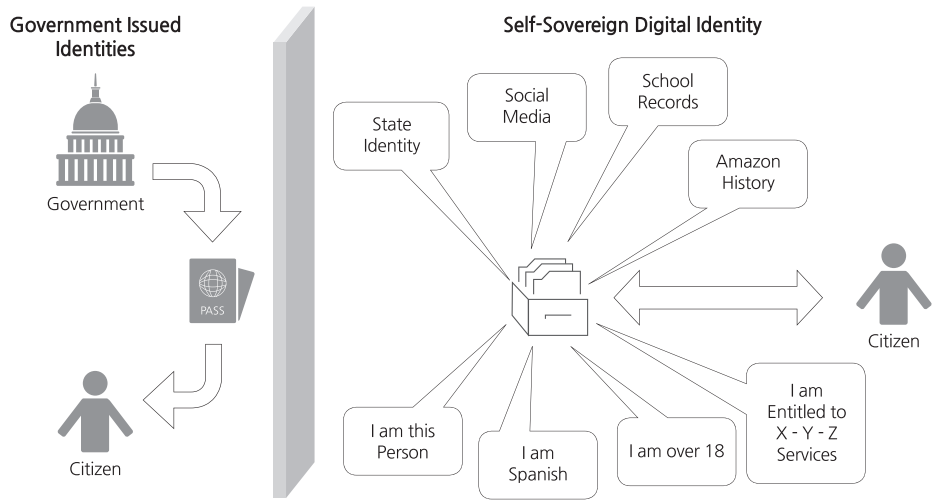
블록체인/DLT는 신분증 확인 과정에서 종이를 대체하는 도구이자 진정한 분산 증명을 제공하기 위한 분권 서명 형식으로 고려된다. 이러한 맥락에서, 다음과 같은 요구사항은 검토되어야 한다.

▶블록 체인
- 체인에 개인 정보가 저장되어 있지 않아야 함
- 어떠한 개별 블록체인/재단/회사도 프레임워크에 통합하지 않아야 함.

▶디자인
- 체인을 인식 불가(체인 불가지론)
- 최소 기능
  - 시장이 규제 준수/니즈에 맞는 솔루션에 적응 할 수 있도록 허용
  - 기존 인프라와 함께 작동
- Secure by design(디자인 단계 보안)

▶거버넌스
- 분권화
- 국제적 수준
- 채택 용이성

ID의 진화는 세 가지 기본 요구 사항을 충족시키려는 연구의 결과로 인식한다.



※ 출처: Whitepaper by TrustMyID - October-2017

[그림1] 자기 주권 ID 개념도

① **보안** - ID 정보는 의도하지 않은 공개로부터 보호
② **제어** - ID 소유자가 데이터를 보고 또 접근 할 수 있는 사람을 제어
③ **이식성** - 사용자는 자신이 원하는 곳 어디에서나 ID 데이터를 사용

이러한 요소를 충족하기 위하여 ID관리 기술은 중앙집중형(Centralized), 연합형(Federated), 사용자 중심형(User-centric), 그리고 자기주권형(Self-soverign)으로 진화하고 있다. 자기주권형은 개별 Silo와 별개이며 개별 제어, 보안 및 완전한 휴대성의 세 가지 필수 요소를 모두 제공한다. 이러한 의미에서 개인은 자신의 ID 제공자이다. 본질적으로 자신의 ID를 제공하기 때문에 외부인이 존재하지 않는다. 개인의 디지털 존재는 어떤 단일 조직과도 독립적이며, 아무도 이용자의 자기 주권적 ID를 이용자에게서 분리 할 수 없다.

자기 주권 ID 체계는 블록체인/DLT를 사용하여 분산된 식별자를 중앙 디렉터리가 없이 조회 할 수 있다. 블록체인/DLT는 ID 문제를 스스로 해결하지는 않지만 부족한 부분을 지원한다. 이를 통해 사람들은 자신이 오프라인일 때와 마찬가지로 분산되고 검증 가능한 자격 증명을 사용하는 것과 같이 증명할 수 있다. [그림 1]에서 블록체인/DLT에 자신의 ID(신원)를 등록하면, 블록체인/DLT 기반의 자신의 ID 증명을 발급되고, 그 ID 증명에 자신이 서명을 한다. 그리고 일반 사업소에서 자신의 블록체인/DLT ID 증명을 제시하면, 사업소에서는 사용자의 ID를 블록체인/DLT에 문의하여, 사용자의 신원정보가 합당함을 검증한다. 이렇듯 지갑형태의 ID를 소유하고 있으면, ID정보의 보안, 제어 및 이식성이 충족되며 더 나아가 개인정보보호의 궁극적인 목적을 충족하게 되는 모델로 추정하고 있다.

5. 개인정보보호

EU의 GDPR(General Data Protection Regulation)의 시행이 2018년 5월 25일이다. 이와 맞물려 ICT 산업은 여러 가지 대응과 조치를 하고

있다. 블록체인/DLT 서비스 또한 이러한 개인정보보호 법과 규정을 준수하여야 한다. 이에 블록체인/DLT 서비스 환경에서 고려하여야 할 기본적인 개인정보보호 요구사항을 질의형태로 검토한다.

① 블록체인/DLT 원장 레코드에 개인식별정보가 포함될 수 있습니까?

개인정보보호 커뮤니티의 합의는 법원 명령의 결과로 블록체인에 기록된 모든 개인 데이터를 제거할 수 있어야 한다는 것이다. 한 가지 예가 '잊혀 질 권리'에 해당 될 수 있다. 결과는 체인의 하드 포크이거나 체인 자체의 중단일 수 있다.

② 공적(Public) 블록체인/DLT 시스템에 개인식별정보가 포함될 수 있습니까?

규제 관점에서 개인 데이터를 블록체인/DLT 시스템에 직접 수록 하지 않는 것이 좋다. 공적 블록체인이라면 개인 정보를 입력하는 것은 규제 당국의 관점에서 안된다. 관련 법령이나 법적으로 허용된 데이터 주체의 동의하에 직접 승인되지 않는 한 개인식별정보에 대한 공개 액세스는 개인식별정보가 사용되는 방법을 제한 할 수 있는 방법이 명확하지 않기 때문에 최소화 원칙 및 동의 원칙을 위반한다.

③ 블록체인/DLT 시스템이 개인식별정보에 관한 개인의 권리를 지원할 수 있습니까?

개인은 개인식별정보 처리 동의를 철회하고, 블록체인/DLT 시스템에 대한 개인식별정보에 대해 문의한 후 수정 조항을 요구하는 권리, '잊혀질 권리' 등을 비롯하여 많은 관할 구역에서 개인 정보 보호 권리를 부여 받는다. 앞으로 상황이 악화 될 가능성이 있다. 더욱이, EU의 기본권 헌장 및 리스본 조약 제8조는 개인정보보호 권리를 명시적으로 인정하고 있다.

④ 사생활 보호법과 같은 관할권의 다른 법률 사이의 갈등에 어떻게 처리합니까?

일부 법률은 해당 관할 구역 내의 개인정보보호법과 대치되거나 심지어는 이를 위반할 수 있다. 예를 들어 보안과 관련된 법률에 따라 보안 목적으로 개인식별정보를 보관하거나 특정 유형의 자산(예: 토지, 부동산)의 소유권을 공개적으로 알고 있어야 한다. 이는 특정 관할 지역에서 이러한 유형의 데이터를 처리하는 블록체인/DLT 시스템의 개인정보보호 원칙을 제외 할 수 있다.

⑤ 프라이버시 문제가 블록체인/DLT 플랫폼에 영향을 미칩니까?

블록체인/DLT 플랫폼의 스마트 콘트랙트 또는 기타 소프트웨어 요소는 사용자 또는 제3자의 사생활을 모르게 잠재적으로 위협 할 수 있다. 책임자는 누구이며 가능한 보호는 무엇인가와 같은 요소를 고려하여야 한다.

⑥ 관할 구역 차이의 영향은 무엇입니까?

사생활 및 공개 요구 사항에 대한 사법부의 차이는 다음 사항을 포함한다.

- 개인 정보의 구성
- '기억할 권리'와 '잊혀질 권리'
- 국가 A 법 vs 국가 B 법 vs 세계화
- 데이터 위치 요구 사항

이러한 차이는 블록체인/DLT 시스템의 노드가 서로 다른 법률 및 규정이 적용되는 여러 관할 지역에 거주하는 경우뿐만 아니라 다른 국가 또는 관할권의 시민들의 개인 데이터를 저장 및 처리하는 경우에 중요한 문제이다.

⑦ 보호 대 공개

개인식별정보 보호 법률 및 규정뿐만 아니라 많은 관할 구역에는 특정 데이터의 보존 및 공개가 요구되는 법률 및 규정이 있다. 이 데이터에는 개인식별정보가 포함될 수 있다. 공개 요청 자체가 데이터 주체를 식별하고 관련 검색 속성을 제공하는 경우 비개인식별정보가 개인식별정보가 될 수 있음에 유의하여야 한다.

⑧ 입법 변경 및 대중의 기대에 따른 영향

입법과 대중의 기대가 바뀌면 요구 사항과 처벌이 강화 될 수 있다. 이것은 영원한 기록으로 의도된 블록체인/DLT 시스템에 대한 문제(도전) 일 수 있다.

⑨ 암호 기술의 발전

암호화를 사용하여 개인식별정보를 보호하는 것이 일반적이다. 암호화가 발전하면 기존 보호 기능이 손상되어 개인식별정보 위반이 발생할 수 있다. 예를 들어, 양자 암호는 기존 시스템과 보안에 대한 매우 실질적인 위협으로 간주된다. 원장 트랜잭션 레코드의 정보가 암호화되어 있기 때문에 불변이므로 원본 알고리즘이 손상된 경우 다른 형식의 암호화를 사용하도록 전환 할 수 없기 때문에 블록체인/DLT 시스템에 대한 문제점으로 대두된다. 암호화 진보는 개인식별정보의 기밀성을 훼손할뿐만 아니라 개인식별정보(서비스 거부)에 대한 액세스 및 데이터 신뢰(데이터의 보이지 않는 수정)에 영향을 주는 새로운 사이버 위협을 의미 할 수 있다.

⑩ 빅 데이터의 영향

기술의 진보는 '빅데이터'를 '거대한(Huge) 데이터'로 변형시킬 수 있다. 확장된 분석 및 프로파일링 기능은 다양한 외부 데이터 집합(및 블록 체인 자체의 내부 데이터 누적)과 함께 '해가없는(harmless)' 정보를 개인식별정보로 전환시킬 수 있다.

⑪ IoT와 블록 체인

사물 인터넷이 계속해서 성장함에 따라 블록체인/DLT 시스템과 함께 사용되고 있다. IoT 시스템은 개인식별정보로 분류 될 수 있는 정보를 처리 할 수 있으며, 이 데이터는 종종 개인의 감시 문제와 관련 있다. 우리는 또한 일반적으로 더 많은 의사소통을 고려할 수 있으나, M2M 및 V2X를 포함하여 아직 심도 있게 논의되지 않았다. 어떤 IoT 관련 데이터를 블록체인/DLT 시스템에 배치하고 개인정보보호 원칙 및 법률을 준수하는 것을 고려하여야 한다.

⑫ 블록체인/DLT 시스템 수명주기

모든 정보 시스템의 수명주기는 일반적으로 약 10년이다. 그러나 산업용 IoT 시스템의 경우 최대 30년의 수명주기를 계획한다. 블록체인/DLT 시스템은 장기 계획으로 마이그레이션이 필요할 수 있다. 개인식별정보에 대한 리스크를 포함하여 모든 마이그레이션은 위험(risky)하다. 블록체인/DLT 원장을 사용하여 어떻게 마이그레이션을 수행하느냐는 공개 문제(Open Question)이다.

⑬ 개인식별정보 컨트롤러는 누구?

여러 당사자가 공유하는 분산 시스템을 사용하면 누가 시스템을 책임지고 있는가에 대한 법적 질문이 생긴다. 특히 개인식별정보 수집 및 개인식별정보 처리와 관련하여 책임 소재에 질의를 하게 된다. 많은 관할 지역은 '개인식별정보 컨트롤러'에 대한 역할을 기술하는 것이 관례이다. 개인식별정보 컨트롤러는 개인식별정보의 수집 및 처리와 개인식별정보 주체로부터 개인식별정보 수집의 통지 및 동의에 대

한 정보를 수집하여야 한다. 이것은 공적 블록체인/DLT 시스템에서 설정하기도 어려울뿐더러 사적 블록체인/DLT 시스템에서도 확실하지 않다.

6. 맺음말

블록체인/DLT 기술은 국가간 환거래에서 환전 수수료를 파격적으로 줄이는 것을 목표로 한다. 블록체인 기술은 암호해시를 기반으로 고안되었으며, P2P 기술로 분산원장이 구축 된 메커니즘이다. 그러나 블록체인/DLT는 정보보호에서 추구하는 모든 서비스를 제공하고 있지 않다. 특히 탈중앙, 분산 환경에서 인증 및 키 분배는 향후 진정한 신뢰 환경을 구축함에 있어서 초석이 되는 문제이다. 이 문제를 풀기 위하여 국제적으로는 R3가 국내에서는 은행연합회에서 공동인증서를 개발을 추진하고 있다. 이렇듯 산업계에서는 디지털 전자화폐에 대하여 많은 관심을 보이고 있으나, 그 자체 기술과 그 응용에 대하여 아직 연구가 필요한 기술이다. 국제적으로 영국이 제일 먼저 암호화폐를 공식 승인한 국가이며, 이를 차차 많은 서방국가가 승인을 한 상태이다. 이렇듯 금융에 선두 그룹인 서방 국가들이 블록체인/DLT 기술에 대하여 선점을 하려고 하는 노력이 엿보이고 있으며, 이 기술을 확대하고자 하는 노력이 병행되고 있다. 향후 스마트 컨트랙트, 헬스정보, 농수산물 및 저작물 유통, 등기소등 많은 분야에 적용을 위하여 노력을 아끼지 않고 있는 상황이다. 블록체인/DLT를 이용하여 기존의 ICT 서비스를 개선 또는 대체하는 작업이 우선 진행되고 있으며, 이러한 작업이 일단락되면, 향후 블록체인/DLT 기술 및 서비스를 개선하는 연구가 후속될 것으로 전망한다.

[참고문헌]

[1] ISO 1st WD TR23245 Security Risks and vulnerabilities, 2018. 03. 27

[2] ISO 1st WD TR23244 Overview of Privacy and PII protection, 2018. 04. 03

[3] ISO 1st WD TR23246 Overview of Identity, 2018. 04. 03

[주요 용어 풀이]

- DLT: Distributed Ledger Technology, 분산된 피투피(P2P, Peer-to-Peer)망 내 참여자들이 모든 거래 목록을 지속적으로 갱신하는 디지털 원장(출처: ITU-T FocusGroup on DFS)
- ICT: Information and Communications Technology, 전기 통신과 컴퓨터를 결합한 고도의 신사회 기반을 형성하는 기술 분야
- ID: Identity, 각종 ID와 주민번호, 전자우편주소, 신용카드번호, 주소 등 사이버스페이스 상에서 개인식별을 가능하게 하는 정보
- GDPR: General Data Protection Regulation, 유럽 의회에서 유럽 시민들의 개인정보 보호를 강화하기 위해 만든 통합 규정
- M2M: Machine to Machine, 기계와 기계 사이의 통신. 사물 통신(M2M)은 기계, 센서, 컴퓨터 등 다양한 장치들이 유무선 통신 기술을 이용해 서로 정보를 교환하게 함으로써 개별 장치들의 기능이나 성능을 개선시켜 주고 개별 장치들이 제공하지 못했던 새로운 지능형 서비스를 제공한다
- P2P: Peer-to-Peer, PC 대 PC, 개인 대 개인처럼 서버의 도움 없이 일대일 통신을 하는 관계
- V2X: Vehicle to Everything communication, 차량을 중심으로 유무선망을 통해 정보를 제공하는 기술. V2X는 차량과 차량 사이의 무선 통신(V2V, Vehicle to Vehicle), 차량과 인프라 간 무선 통신(V2I, Vehicle to Infrastructure), 차량 내 유무선 네트워킹(IVN, In-Vehicle Networking), 차량과 이동 단말 간 통신(V2P, Vehicle to Pedestrian) 등을 총칭한다. V2X를 이용하여 차량과 도로의 정보 환경, 안정성, 편리성 등을 향상시킬 수 있다