국가 · 공공기관 도입을 위한

블록체인 암호기술 가이드라인

2020. 12.



국가정보원
과학기술정보통신부
국가보안기술연구소
한국정보통신기술협회

머리말

블록체인은 데이터에 대한 투명성, 불변성, 신뢰성 등의 가치를 부여할 수 있다는 기술적 특징으로 인해 최근 국가·공공기관에서는 다양한 서비스에 블록체인을 접목하기 위한 시도가 이루어지고 있고 관련 사업들이 증가하고 있다.

블록체인이 많은 장점을 가지는 이유는 각종 암호기술이 제공하는 무결성, 부인방지 등의 보안 기능이 복합적으로 결합되어 설계된 인프라 기술이기 때문이며 이로 인해 대부분의 사업담당자들은 블록체인을 기반으로 서비스를 구축할 경우 안전할 것이라는 막연한 기대를 하게 된다.

그러나 블록체인을 활용함에 있어 간과되고 있는 부분은 블록체인의 기반이 되는 암호기술이 올바르게 사용되고 있는지 여부이다. 안전성이 높은 암호기술이 적용되어 있다 하더라도 암호키를 소스코드에 고정하여 사용하는 등 적합하지 않은 방법으로 구현하는 경우 블록체인 기술을 적용하더라도 취약점에 노출될 수 있다.

따라서, 국가·공공기관에 안전한 블록체인 구축을 유도하기 위한 방향성 제시가 필요하며 이를 위한 목적으로 블록체인 암호기술 가이드라인이 작성되었다.

본 가이드라인은 국가·공공기관에 주로 도입되는 허가형 블록체인을 대상으로 암호기술 관점에서 갖춰야 할 기본 요건을 제시한다. 1장에서 블록체인 기술 개요를 시작으로 블록체인과 암호기술, 블록체인 구성별 특징을 설명하고 2장에서 블록체인 구축 시 고려되어야 할 17가지 준수 사항 및 준수 방안을 제시하였다.

또한, 사업 수행 시 쉽게 참고하도록 용어 정의 및 체크리스트를 제공하였으며 이를 통해 국가·공공기관 사업담당자들의 블록체인에 대한 의식 제고와 함께 블록체인에 대한 신뢰성과 보안성 향상에 기여할 수 있기를 기대한다.

Contents

1. 블록체인 기술 개요 7

1.1. 블록체인 9

1.2. 블록체인과 암호기술 10

1.2.1. 암호학적 해시 함수 10

1.2.2. 공개키 암호 11

1.2.3. 기타 암호 알고리즘 13

1.3. 블록체인 구성 13

1.3.1. 블록체인 아키텍처 13

1.3.2. 블록체인 네트워크 15

1.3.3. 계정 관리 15

1.3.4. 트랜잭션, 블록, 원장 16

1.3.5. 합의 프로토콜 20

1.3.6. 스마트 컨트랙트 22

1.3.7. 블록체인 서비스 24

2. 블록체인 암호기술 가이드라인 25

2.1. 암호 사용기준 28

2.2. 계정 관리 30

2.3. 데이터 전송 보안 35

2.4. 합의 프로토콜 37

2.5. 원장 39

2.6. 스마트 컨트랙트 43

2.7. 데이터베이스 45

3. 용어 정의 47

4. 약어 58

5. 체크리스트 60

6. 참고문헌 62

7. 부록 64

Contents

[표 차례]

[표 1-1] 대표적인 합의 프로토콜 21
[표 2-1] 암호모듈 검증제도 검증대상 암호 알고리즘.....29
[표 7-1] 블록체인에서 활용되는 암호기술 64

[그림 차례]

[그림 1-1] 블록체인의 특징.....9
[그림 1-2] 전자 서명 개념도.....12
[그림 1-3] 블록체인 참조 구조.....14
[그림 1-4] 트랜잭션 구조.....16
[그림 1-5] 블록 구조.....17
[그림 1-6] 원장 구조.....18
[그림 1-7] 트랜잭션 처리 과정.....19
[그림 1-8] 스마트 컨트랙트 실행 과정 23

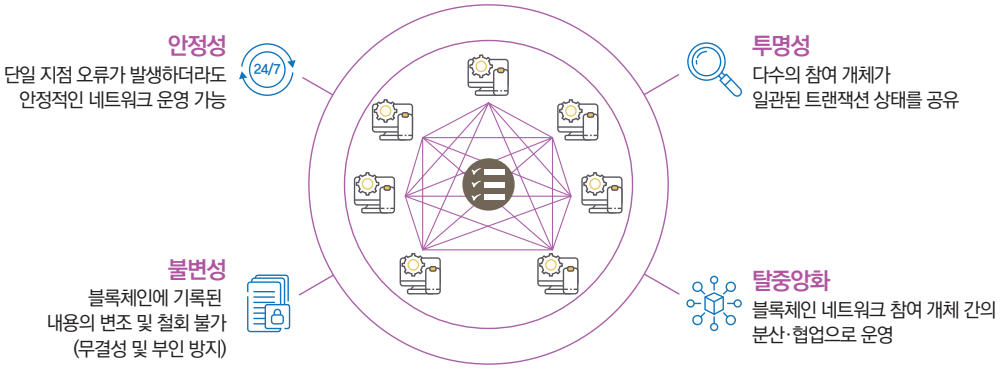
1

블록체인 기술 개요

1.1. 블록체인

블록체인은 네트워크 내의 참여 개체가 공동으로 정보 및 가치의 이동을 기록·검증·보관·실행함으로써 중개자 없이도 데이터의 신뢰성 확보를 가능하게 하는 기술이다. 블록체인은 참여 개체 모두 거래 내역을 볼 수 있는 투명성, 한 번 연결된 블록은 수정하거나 삭제하기 어려운 불변성 등의 기술적 특성을 보유하고 있다.

기술적으로 정의하자면, 블록체인은 네트워크에 분산된 개체들이 합의 프로토콜을 통해 합의된 블록을 암호학적 해시 함수를 이용하여 덧붙이기만 가능하도록 차례로 연결한 분산 원장이다. 일반적으로 블록체인은 암호학적 해시 함수와 전자 서명 등의 암호기술을 이용하여 구현된다.



[그림 1-1] 블록체인의 특징

블록체인은 다음과 같은 특징을 가진다. ([그림1-1] 참조)

탈중앙화 decentralization	블록체인 네트워크 참여 개체 간의 분산 · 협업으로 운영
투명성 transparency	다수의 참여 개체가 일관된 트랜잭션 상태를 공유
불변성 immutability	블록체인에 기록된 내용의 변조 및 철회 불가 (무결성 및 부인 방지)
안정성 reliability	단일 지점 오류가 발생하더라도 안정적인 네트워크 운영 가능

블록체인은 일반적으로 참여 방법에 따라 다음과 같이 분류할 수 있다.

비허가형 퍼블릭 블록체인	어느 개체나 제한 없이 네트워크에 참여하여 원장의 내용을 읽고, 블록을 생성하여 원장에 기록할 수 있는 블록체인 ex) Bitcoin, Ethereum 등
허가형 퍼블릭 블록체인	어느 개체나 제한 없이 네트워크에 참여하여 원장의 내용을 읽을 수 있지만, 블록을 생성하여 원장에 기록하기 위해서는 특정 그룹의 허가가 필요한 블록체인 ex) EOS, Ripple, Sovrin 등
허가형 프라이빗 블록체인	블록을 생성하여 원장에 기록하는 것뿐만 아니라 네트워크에 참여하여 원장의 내용을 읽기 위해서도 특정 그룹의 허가가 필요한 블록체인 ex) Hyperledger Fabric, Hyperledger Indy 등

국가 · 공공기관에서 도입할 블록체인 솔루션은 블록 생성 등에 대한 권한 관리가 필요할 것으로 예상되므로 본 가이드라인은 허가형 블록체인을 기준으로 작성하였다.

1.2. 블록체인과 암호기술

블록체인은 불변성, 투명성 등을 제공하기 위해 해시 함수, 전자 서명 등 다양한 암호기술을 사용한다. 본 절에서는 블록체인에 대한 이해를 돕기 위해, 블록체인에 사용되는 주요 암호기술을 개략적으로 설명한다.

1.2.1. 암호학적 해시 함수

암호학적 해시 함수 (cryptographic hash function)

암호학적 해시 함수는 암호 알고리즘의 일종으로 긴 길이의 데이터를 압축하여 일정 길이(256비트, 512비트 등)의 고윳값을 출력한다. 해시 함수의 출력은 해시값(hash value), 해시(hash), 메시지 다이제스트(message digest), 메시지 지문(message fingerprint) 등으로 불린다. 암호학적 해시 함수는 일반적으로 다음과 같은 성질을 가진다.

역상 저항성 pre-image resistance	주어진 해시값을 출력하는 입력 데이터를 찾기 어려운 성질
충돌 저항성 collision resistance	동일한 해시값을 출력하는 두 개 이상의 입력 데이터를 찾기 어려운 성질

암호학적 해시 함수는 입력 데이터에 한 비트 변화만 생기더라도 해시값이 완전히 달라지므로 데이터 무결성 검증에 주로 활용된다. 대표적인 암호학적 해시 함수로는 우리나라 국가 표준 LSH, 미국 NIST 및 ISO/IEC에서 표준으로 제정한 SHA-2, SHA-3 등이 있다.

1.2.2. 공개키 암호

공개키 암호는 공개키 암호 체계(public key cryptosystem)에서 공개키를 사용하는 기능과 개인키를 사용하는 기능을 제공하는 함수로 구성되어, 공개키와 개인키의 비대칭적인 특성에 기반하여 암호화, 전자 서명 생성·검증, 키 교환 등의 기능을 제공할 수 있는 암호기술이다.

대표적인 공개키 암호로는 기밀성 제공을 위한 암호화 방식(encryption scheme), 무결성, 인증 및 부인 방지를 제공하는 전자 서명 방식(digital signature scheme), 그리고 비밀키 공유를 위한 키 교환 방식(key exchange protocol)이 있다.

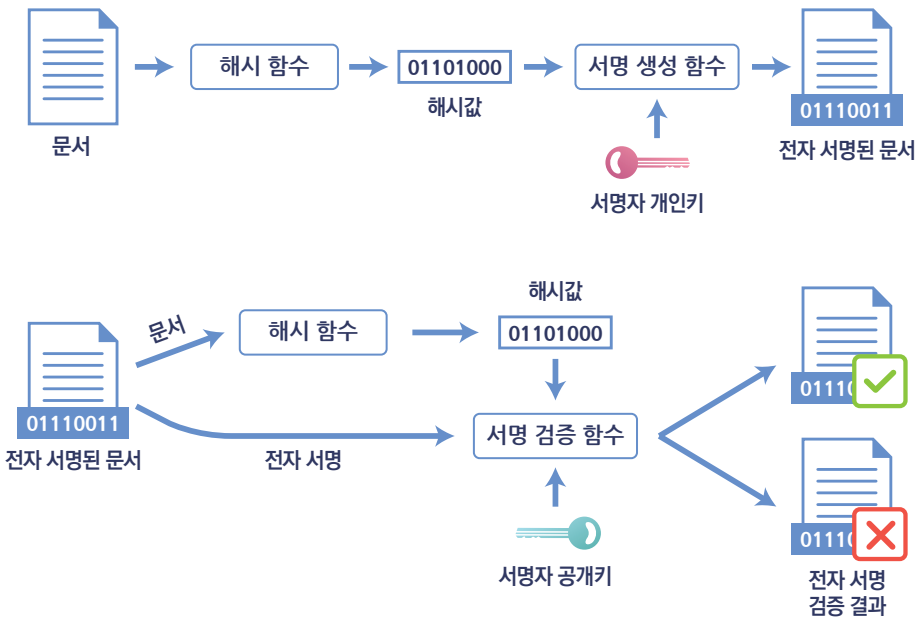
암호화 방식

암호화 함수와 복호화 함수로 구성된 암호화 방식에서, 암호화 함수는 평문과 공개키를 입력받아 암호문을 생성하는 기능을 수행하고 복호화 함수는 암호문과 개인키를 입력받아 암호문에 대응하는 평문을 계산하는 기능을 수행한다. 암호화 방식이 보장하는 기밀성은 암호화 과정에서 사용된 공개키에 대응하는 개인키 소유자만 암호문을 복호화할 수 있는 특성에 기반한다.

전자 서명 방식

전자 서명은 블록체인 기술의 구현에서 핵심적인 역할을 담당한다. 전자 서명은 서명자를 확인하고 서명자가 전자 문서(전자적 형태로 작성되어 송수신되거나 저장되는 정보)에 서명하였음을 보증하기 위하여, 해당 전자 문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보이다.

서명 생성 함수와 서명 검증 함수로 구성된 전자 서명 방식에서, 서명 생성 함수는 메시지와 개인키를 입력받아 전자 서명을 생성하는 기능을 수행하고 서명 검증 함수는 메시지, 전자 서명, 공개키를 입력받아 (메시지에 대한) 전자 서명의 유효성(validity)을 검증하는 기능을 수행한다. ([그림 1-2] 참조) 전자 서명 방식이 보장하는 무결성과 부인 방지 특성은 개인키 소유자만 유효한 서명 생성이 가능하다는 특성에 기반을 둔다.



[그림 1-2] 전자 서명 개념도

일반적으로 블록체인 SW 플랫폼은 전송 데이터의 출처 및 유효성 검증과 부인 방지 기능을 제공하기 위해 전자 서명을 활용하며, 주로 타원곡선 기반의 전자 서명 방식을 사용한다.

1.2.3. 기타 암호 알고리즘

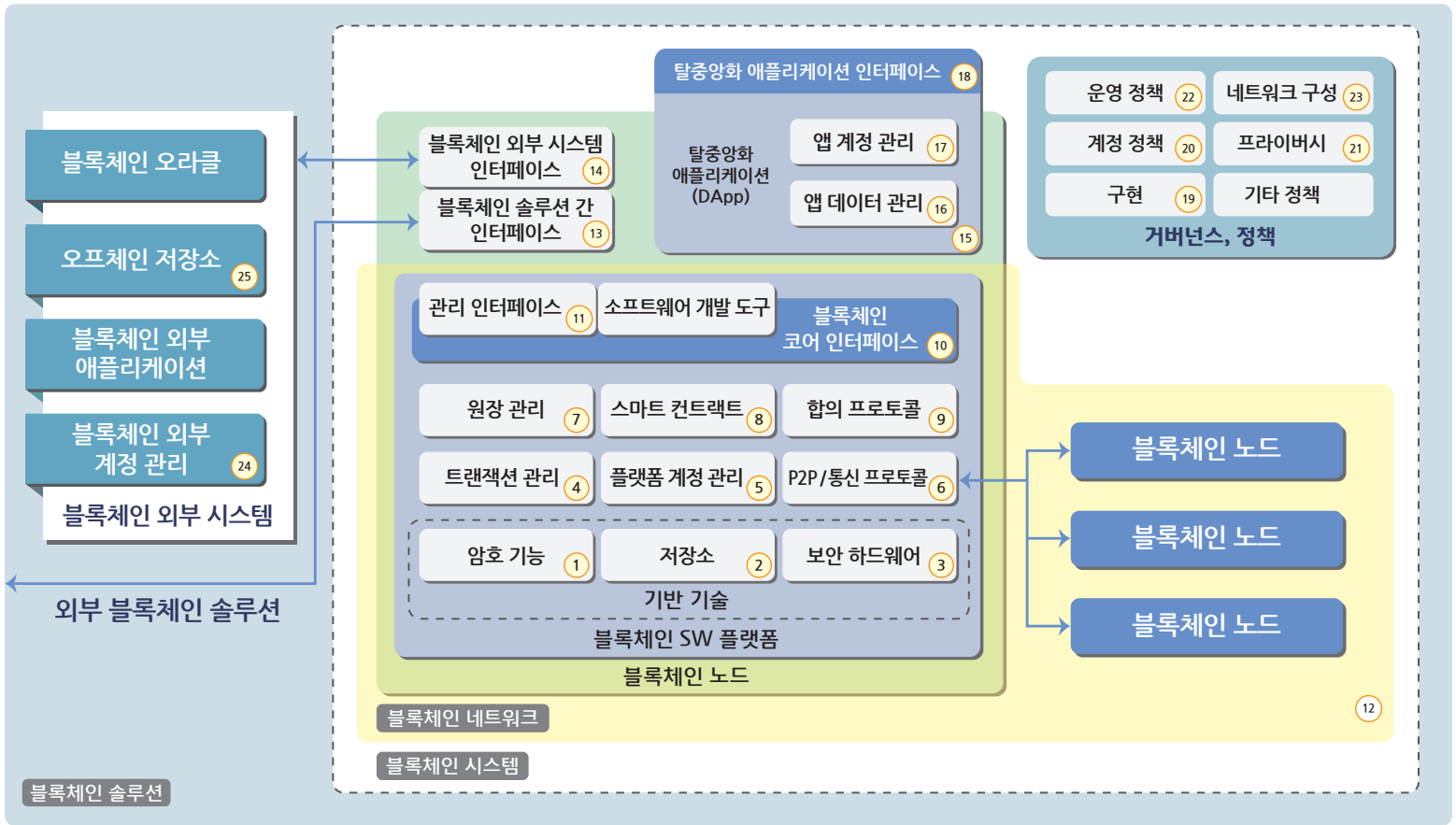
최근에는 무결성과 부인 방지 기능 외에도 개인정보 · 프라이버시 보호 등 추가적인 보안 기능을 제공하기 위해 영지식 증명 등 다양한 암호기술을 블록체인에 적용하기 위한 연구가 진행되고 있다. ([표 7-1] 참조)

1.3. 블록체인 구성

1.3.1. 블록체인 아키텍처

일반적인 블록체인 아키텍처는 블록체인 SW 플랫폼, 블록체인 시스템, 블록체인 솔루션으로 구성되며, 이를 도식화하면 [그림 1-3]과 같다.

- 블록체인 SW 플랫폼은 각 블록체인 노드에 탑재되어 블록체인 노드가 블록체인 시스템에 참여할 수 있도록 제공되는 프로세스(암호 기능, 트랜잭션 관리, 스마트 컨트랙트, 탈중앙화 애플리케이션 등), 저장소(안전한 저장소, 원장 관리 등), 통신 기능(P2P/통신 프로토콜, 합의 프로토콜, 애플리케이션 인터페이스 등)의 집합이다.
- 블록체인 시스템은 운영 정책, 네트워크 구성 방법 등 사전에 정의된 거버넌스 · 정책에 따라 네트워크를 구성하고 블록체인을 공유할 수 있도록 구현한 것이다.
- 블록체인 솔루션은 블록체인 기반 서비스를 제공하는 데 필요한 모든 기능을 통합 구현한 것이다. 일반적으로 블록체인 솔루션은 블록체인 시스템을 기반으로 블록체인 외부 시스템(블록체인 오라클, 오프체인 저장소 등), 외부 블록체인 솔루션과의 연계 기능을 포함한 개념이다.



[그림 1-3] 블록체인 참조 구조

1.3.2. 블록체인 노드

블록체인 노드는 블록체인 시스템에 참여하여 네트워크를 구성하는 기기 또는 프로그램으로 아래와 같은 기능의 일부 또는 전체를 수행할 수 있다.

트랜잭션 생성	자발적으로 또는 다른 개체의 요청을 받아 트랜잭션 생성 및 네트워크로 전파
트랜잭션 검증	다른 노드가 생성한 트랜잭션의 유효성 검증, 필요하다면 트랜잭션 보증을 수행하여 자신의 전자 서명 추가
블록 생성	유효성이 검증된 트랜잭션을 포함한 신규 블록 생성 및 네트워크로 전파
원장 관리	수신된 신규 블록을 이용하여 원장을 갱신하고 완전한 블록체인 사본 유지
기타 역할	블록체인 SW 플랫폼 계정 관리, 스마트 컨트랙트 관리, 네트워크 관리, 외부 인터페이스 제공 등

1.3.3. 계정 관리

블록체인 솔루션은 참여 개체를 식별하기 위해 개체별로 계정을 부여하며, 허가형 블록체인 솔루션은 계정을 관리할 수 있는 계정 관리 시스템을 가져야 한다. 블록체인의 계정은 블록체인 SW 플랫폼 계정, 블록체인 외부 시스템 계정, 탈중앙화 애플리케이션 계정(DApp 계정) 등으로 나눌 수 있으며 분류에 따라 별도의 계정 관리 시스템을 가질 수 있다.

블록체인 SW 플랫폼 계정은 블록체인 네트워크에 참여하는 개체에 부여되며, 블록체인 SW 플랫폼에서 자체적으로 제공하는 계정 관리 시스템으로 관리된다. 블록체인 SW 플랫폼 계정을 소유한 개체는 트랜잭션 생성 · 검증, 블록 조회 · 생성 · 검증, 스마트 컨트랙트 설치 · 실행, 블록체인 코어 인터페이스 접근 등 블록체인 SW 플랫폼 내에서 다양한 역할을 수행할 수 있으며 계정별로 역할과 권한이 다를 수 있다. 블록체인 SW 플랫폼 계정은 전자 서명을 생성하기 위한 개인키 · 공개키 쌍을 필요로 한다.

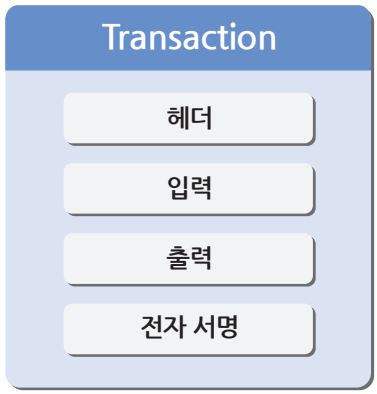
블록체인 외부 시스템 계정은 블록체인 네트워크에 직접 참여할 수 없으며, 블록체인 시스템에 접근하기 위해서는 별도의 인터페이스를 통해 간접적으로 접근해야 한다.

탈중앙화 애플리케이션 계정(DApp 계정)은 탈중앙화 애플리케이션을 통해 원장 조회 · 기록, 외부 시스템 자료 조회, 스마트 컨트랙트 실행 등을 할 수 있으며 전자서명을 생성하기 위한 개인키 · 공개키 쌍을 필요로 한다.

1.3.4. 트랜잭션, 블록, 원장

트랜잭션 구조

트랜잭션은 자산의 이동 또는 생성과 같이 블록체인에서 발생하는 이벤트의 기록이다. 트랜잭션은 일반적으로 헤더, 입력, 출력, 전자 서명으로 구성되며([그림 1-4] 참조), 블록체인 SW 플랫폼별로 상세 구성은 다를 수 있다. 헤더에는 트랜잭션 관련 정보들이 기록되고, 스마트 컨트랙트의 실행 결과 등을 포함한 트랜잭션 처리 데이터는 입력 · 출력에 포함되며, 트랜잭션 생성 개체의 전자 서명이 첨부된다(필요하다면 트랜잭션 생성 요청 개체의 전자 서명도 포함). 암호화폐의 경우, 송금 개체의 정보와 수신 개체의 정보가 입력과 출력에 각각 기록되며, 송금 개체의 전자 서명이 첨부된다. 스마트 컨트랙트의 경우, 실행에 필요한 매개변수와 수행 결과가 입력과 출력에 각각 기록되며, 실행 개체의 전자 서명이 포함될 수도 있다.

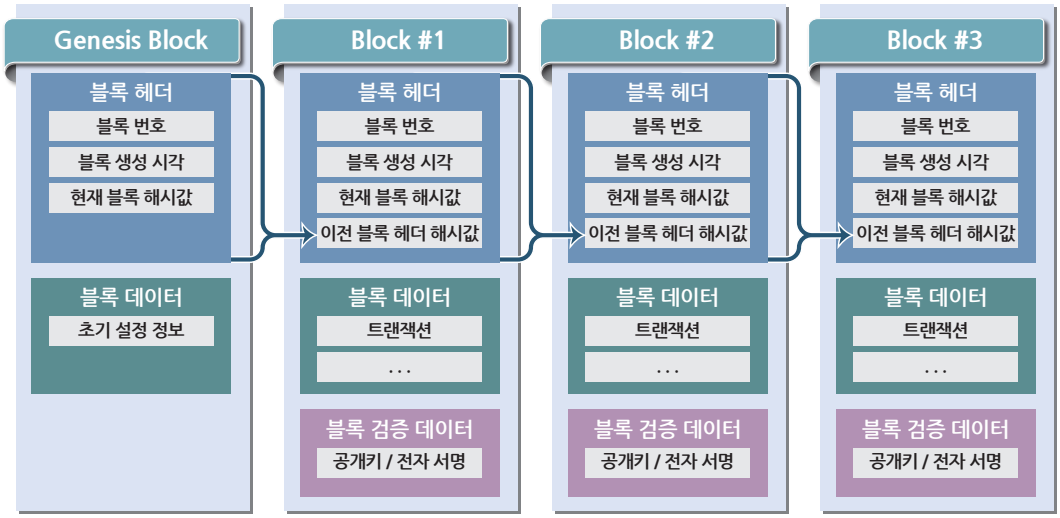


[그림 1-4] 트랜잭션 구조

블록 구조

블록은 일반적으로 블록 헤더, 블록 데이터, 블록 검증 데이터로 이루어진다. ([그림 1-5] 참조)

- 블록 헤더는 블록 번호, 블록 생성 시각, 블록 데이터의 해시값, 그리고 이전 블록 헤더의 해시값을 포함한다.
- 블록 데이터는 다수의 트랜잭션을 포함한다.
- 블록 검증 데이터는 블록을 생성하는 개체의 공개키와 전자 서명 값을 포함한다.



[그림 1-5] 블록 구조

원장

블록체인 기술에서 원장은 블록체인 참여 개체가 합의한 블록들을 체인으로 연결해 놓은 자료 구조이다. ([그림 1-6] 참조) 합의 프로토콜을 이용한 합의를 통해 모든 참여 개체가 동일한 원장을 공유할 수 있으며, 완결성을 제공하는 합의 프로토콜을 통해 원장에 기록된 블록이 삭제되지 않음을 보장할 수 있다. 또한, 해시 함수를 이용한 체인을 통해 원장에 기록된 블록이 변조되지 않는 특성을 제공한다.

원장에 기록된 트랜잭션은 단순 나열 형태로, 필요한 정보를 즉시 추출하기 어렵다. 이를 보완하기 위해 블록체인 SW 플랫폼은 원장을 유용하게 활용할 수 있는 형태로 가공한 상태 DB를 제공한다. 상태 DB는 공유되지 않고 블록체인 참여 개체가 개별

관리하지만, 공유된 원장에 기록된 내용을 기반으로 관리하기 때문에 각 개체의 상태 DB 내용은 모두 동일하다.

> 계좌의 거래 내역을 포함한 잔액 조회는 일반적인 금융 서비스뿐만 아니라 블록체인 기반 금융 서비스에서도 매우 빈번하게 발생한다. 원장에는 거래가 단순 나열된 형태로 기록되기 때문에, 특정 계좌의 거래 내역 및 잔액을 확인하려면 기록된 모든 거래를 확인해야 한다. 이를 개선하기 위해 블록체인 참여 개체는 상태 DB에 계좌별 거래 내역 및 잔액을 정리하여 관리할 수 있다.



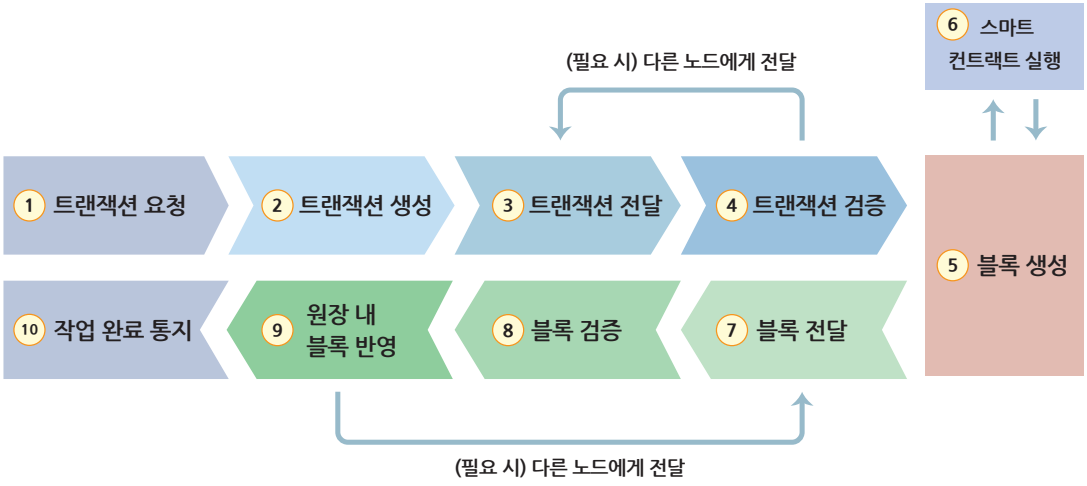
[그림 1-6] 원장 구조

트랜잭션 처리 과정

일반적인 블록체인 SW 플랫폼의 트랜잭션 처리 과정은 다음과 같다. ([그림 1-7] 참조) 상세 과정은 블록체인 SW 플랫폼별로 다를 수 있다.

1. 블록체인에 기록이 요구되는 행위를 하려는 개체는 트랜잭션 생성 권한을 가진 개체에게 트랜잭션 생성을 요청한다.
2. 생성 요청을 받은 개체는 트랜잭션을 생성한다.
3. 트랜잭션을 생성한 개체는 트랜잭션을 네트워크 내의 다른 노드에게 전달한다.
4. 생성된 트랜잭션을 전달받은 노드는 트랜잭션이 올바른지 검증한다.

5. 블록을 생성할 수 있는 권한을 지닌 노드는 전달받은 트랜잭션들을 모아 블록을 생성한다.
6. 블록을 생성하는 과정에 스마트 컨트랙트가 포함되어 있다면 스마트 컨트랙트를 실행하고, 실행 결과를 블록에 포함한다.
   ※ 스마트 컨트랙트의 실행은 블록체인 SW 플랫폼에 따라 트랜잭션 생성 시점에 이루어질 수도 있다.
7. 블록을 생성한 개체는 블록을 다른 노드에게 전달한다.
   ※ 필요에 따라 트랜잭션과 블록의 전달은 여러 차례 이루어질 수 있다.
8. 생성된 블록을 전달받은 노드는 블록 헤더와 블록에 담긴 트랜잭션이 올바른지 검증한다.
9. 올바른 블록인 경우 노드는 자신의 원장에 새로운 블록을 반영하고, 자신의 상태 DB를 갱신한다.
10. 트랜잭션을 생성한 개체는 트랜잭션이 블록에 반영되면 요청 개체에게 작업이 완료되었음을 알린다.



[그림 1-7] 트랜잭션 처리 과정

1.3.5. 합의 프로토콜

블록체인은 분산 컴퓨팅 기술에 기반을 두고 있으며 여러 참여 개체가 동일한 원장을 공유하기 위해 합의 프로토콜을 사용한다. 블록체인 네트워크에서는 일부 노드에 비잔틴 장애(내부 관리자의 악의적인 조작, 해킹 등)를 제외한 일반적인 장애(정전, 네트워크 연결 실패 등)가 발생하더라도 정상적으로 동작할 수 있는 합의 프로토콜이 사용된다. 또한, 일부 노드에 일반적인 장애뿐만 아니라 비잔틴 장애가 발생하더라도 정상적으로 동작할 수 있는 합의 프로토콜이 사용되는 경우도 많다.

블록체인에서 사용되고 있는 합의 프로토콜들은 장애 내성, 단위 시간당 최대 트랜잭션 처리량(throughput), 트랜잭션이 변경될 수 없는 상태가 될 때까지 걸리는 시간(time to finality) 등의 관점에서 특성을 비교할 수 있다. 블록체인에서 사용되는 대표적인 합의 프로토콜은 [표 1-1]과 같다.

합의 프로토콜	설명	적용 블록체인	장애 내성 특성	완결성	throughput	time to finality	확장성	활용 사례
PoW (Proof of Work)	소모한 연산량이 많을수록 블록을 생성할 확률 증가	비허가형	비잔틴 장애 내성	무	낮음	매우 느림	매우 높음	Bitcoin, Ethereum
PoS (Proof of Stake)	투자한 지분이 많을수록 블록을 생성할 확률 증가	허가형/ 비허가형	비잔틴 장애 내성	유/무	보통	느림	높음	Ethereum Casper, Algorand
PoA (Proof of Authority)	생성된 블록을 채택하는 과정에서 참여 개체들의 평가를 반영한 평판 활용	허가형	비잔틴 장애 내성	유	높음	빠름	보통	Enterprise Ethereum
DPoS (Delegated Proof of Stake)	지분을 기반으로 한 투표를 이용하여 블록을 생성할 개체 선정	허가형/ 비허가형	비잔틴 장애 내성	유	높음	보통	매우 높음	EOS.IO
PBFT (Practical Byzantine-Fault Tolerance)	사전에 정의된 절차에 따라 블록을 생성할 개체를 선정하며, 생성한 블록에 대한 나머지 개체의 동의 요청	허가형	비잔틴 장애 내성	유	높음	빠름	매우 낮음	—
Raft	사전에 정의된 절차에 따라 블록을 생성할 개체를 선정하며, 생성한 블록에 대한 나머지 개체의 동의 요청	허가형	일반 장애 내성	유	높음	매우 빠름	낮음	Hyperledger Fabric, R3 Corda

[표 1-1] 대표적인 합의 프로토콜

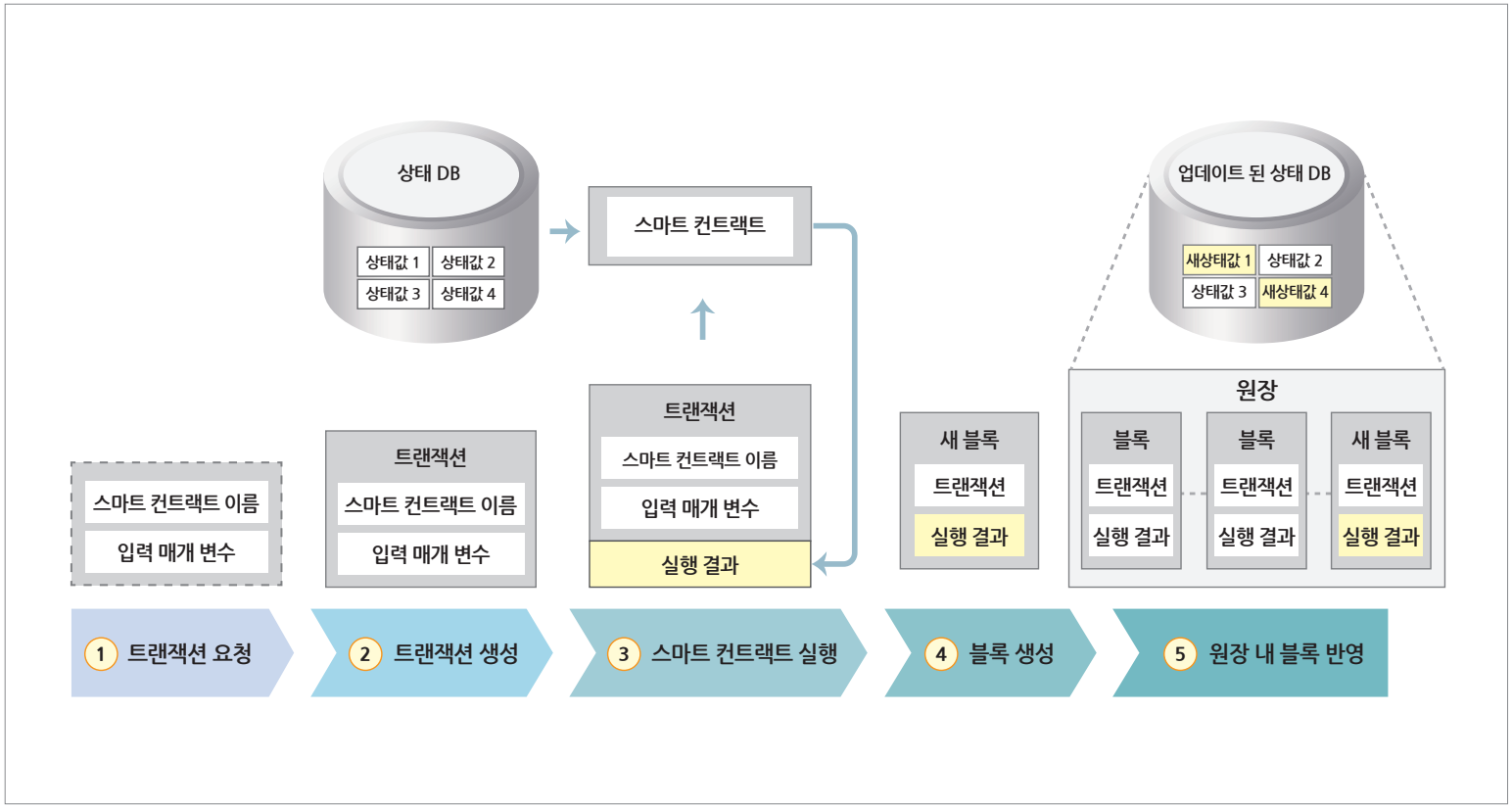
1.3.6. 스마트 컨트랙트

블록체인 스마트 컨트랙트는 모든 실행 결과가 블록체인에 기록되는 블록체인 시스템상의 컴퓨터 프로그램이다. 블록체인 스마트 컨트랙트는 입력 매개변수 외에는 블록체인에 기록된 데이터만을 사용하기 때문에 블록체인 시스템 내 어떤 참여 개체가 실행하더라도 같은 결과를 얻을 수 있으며, 누구나 결과를 검증할 수 있는 특성을 가진다.

블록체인 스마트 컨트랙트를 실행하는 과정은 다음과 같다. ([그림 1-8] 참조) 상세 과정은 블록체인 SW 플랫폼별로 다를 수 있다.

1. 스마트 컨트랙트를 실행하려는 개체는 해당 스마트 컨트랙트의 이름과 실행에 필요한 입력 매개변수를 트랜잭션을 생성할 수 있는 개체에게 전달한다.
2. 트랜잭션을 생성할 수 있는 개체는 전달받은 내용을 기반으로 트랜잭션을 생성하고, 스마트 컨트랙트를 실행할 수 있는 개체에게 전달한다.
3. 스마트 컨트랙트를 실행할 수 있는 개체는 자신의 현재 상태 DB를 참고하여 스마트 컨트랙트를 실행하고 실행 결과를 전달받은 트랜잭션에 덧붙인 후, 블록 생성 노드에게 전달한다.
4. 블록 생성 노드는 전달받은 트랜잭션을 블록에 포함하고, 전달받은 실행 결과에 따라 자신의 원장과 상태 DB를 업데이트한 후 생성된 블록을 전파한다.
5. 블록을 전달받은 개체들은 각자 자신의 원장과 상태 DB를 업데이트한다.

위의 과정에서 블록체인 네트워크에 스마트 컨트랙트의 실행 결과가 포함된 트랜잭션이 공유되므로 블록체인 시스템 내 모든 개체는 자신의 상태 DB를 활용하여 스마트 컨트랙트가 올바르게 실행되었는지 검증할 수 있다.



[그림 1-8] 스마트 컨트랙트 실행 과정

1.3.7. 블록체인 서비스

탈중앙화 애플리케이션

탈중앙화 애플리케이션은 블록체인 솔루션에 참여하는 개체가 블록체인 시스템을 활용할 수 있도록 블록체인 시스템상에서 운영되는 애플리케이션이다. 애플리케이션 사용 개체는 탈중앙화 애플리케이션이 제공한 사용자 인터페이스를 활용하여 블록체인 내용 조회, 스마트 컨트랙트 실행 등의 작업을 요청할 수 있다. 작업 요청을 받은 탈중앙화 애플리케이션은 스마트 컨트랙트와 API를 사용하여 요청받은 작업을 수행한다.

오프체인 저장소

오프체인 저장소는 블록체인 시스템과 연관이 있지만, 블록체인 시스템 외부에 위치, 수행, 또는 운영되는 저장소이다. 블록체인은 블록을 삭제하지 않고 이어 붙이기만 하는 특성이 있어, 참여 개체가 저장해야 하는 데이터의 양이 지속해서 늘어날 수밖에 없다. 그러므로 대량의 데이터를 지속해서 블록체인에 기록할 경우, 모든 참여 개체가 대량의 데이터를 저장해야 한다. 또한, 블록체인의 데이터는 모든 참여 개체가 접근할 수 있으며, 한 번 기록된 데이터는 삭제할 수 없어 개인정보 등 민감 정보를 저장하기에 적합하지 않다. 이러한 문제를 해결하기 위해 대량의 데이터나 민감 데이터는 별도의 외부 저장소나 서버에 보관하고 블록체인에는 저장 위치, 데이터의 해시값, 메타 데이터 등만 기록하는 방법을 활용할 수 있다. 이는 블록체인 유지에 필요한 저장 데이터의 양을 줄일 수 있으며, 개인정보 등의 민감 데이터를 안전하게 보관할 수 있게 해준다.

블록체인 오라클

블록체인 오라클은 블록체인 시스템 외부에서 생성된 데이터를 이용하여 블록체인에 정보를 제공하는 서비스이다. 대부분의 블록체인 시스템은 외부에서 생성된 데이터(온도 센서가 측정한 온도, 주식 시장의 주가, 전력 사용량 등)를 필요로 하는데, 외부 데이터에 직접 접근할 수 없으므로 블록체인 오라클을 이용해 데이터를 입력받는다. 따라서 블록체인 오라클이 제공해 준 데이터를 신뢰할 수 없다면, 제공된 데이터를 활용해 생성한 블록체인 시스템의 데이터 역시 신뢰할 수 없다. 이러한 신뢰 문제를 블록체인 오라클 문제라 한다. 이 문제를 해결하기 위해서는 신뢰할 수 있는 개체가 오라클을 관리하게 하거나 다수의 오라클을 활용하는 등의 대책을 마련할 수 있다.

2
블록체인 암호기술 가이드라인

본 장은 국가·공공기관에서 안전한 블록체인을 구축하기 위해 준수해야 할 17개의 가이드라인 항목을 제시한다. 각 항목은 준수 사항, 가이드라인 적용 범위, 미준수 시 위협, 가이드라인 준수 방안으로 구성되어 있으며, 예시는 다음과 같다.

❶ Guideline 2-4

계정의 개인키와 공개키 쌍은 교체할 수 있어야 한다.

❷ 가이드라인 적용 범위

ⓘ 암호 기능(1), 플랫폼 계정 관리(5), 앱 계정 관리(17), 계정 정책(20)

❸ 미준수 시 위협

⚠ 기기 변경, 유효기간 만료, 개인키 유출 등이 발생했을 때 개인키와 공개키 쌍을 교체할 수 없으면 계정의 안전한 사용 불가

❹ 가이드라인 준수 방안

- 계정의 개인키와 공개키 쌍은 교체할 수 있어야 한다.❺
  - 계정의 주 식별자로 공개키를 사용하는 경우, 새로운 키 쌍을 이용하여 계정을 생성하고 이전 계정을 폐기하는 방법을 사용할 수 있다.
  - 계정의 주 식별자로 ID 등을 사용하는 경우, 계정 정보에 포함된 공개키를 교체하는 방법을 사용할 수 있다.
- 키의 유효기간을 설정하여 주기적으로 계정의 개인키와 공개키 쌍이 교체되도록 할 것을 권고한다.❺
  - 유효기간은 사용 환경, 서비스 등을 고려하여 설정할 수 있다.❺
- 키가 교체되거나 유효기간이 만료되는 즉시 이전 키는 새로운 기록 및 통신 등에 사용할 수 없어야 한다.
  - 공개키의 경우 교체되거나 유효기간이 만료되어도 지난 기록의 검증 등을 위하여 일정 기간 사용할 수 있다.
- 지난 기록의 검증, 서비스의 연속성 등을 고려하여 교체 이전의 공개키를 관리할 수 있다.
- 신규 개인키와 공개키 쌍은 Guideline 2-3에서 명시한 방법에 따라 안전하게 생성 · 등록 · 저장되어야 한다.
- 키 교체, 유효기간 설정 등 키 관리 고려사항은 미국 NIST가 발간한 'NIST SP 800-57 Part 1 Rev. 5, Recommendation for Key Management: Part 1 – General'[14]을 참고할 수 있다.

❶ 준수 사항: 국가·공공기관의 안전한 블록체인 도입을 위한 암호기술 기준이 제시되어 있다.

❷ 가이드라인 적용 범위: 블록체인 참조 구조상 가이드라인이 적용되는 영역을 나타낸 것으로 세부구조별 번호를 이용하여 '[그림 1-3] 블록체인 참조 구조'에서 적용 영역을 확인할 수 있다.

❸ 미준수 시 위협: 가이드라인을 준수하지 않았을 때 발생할 수 있는 위협을 기술하였다.

❹ 가이드라인 준수 방안: 가이드라인을 준수하기 위해 참고할 수 있는 사항들을 기술하였다.

❺ 가이드라인의 기술에 사용된 '해야 한다', '권고한다', '할 수 있다'의 의미는 다음과 같다.

→ 해야 한다(shall) : 의무, 강제함 (requirement)
→ 권고한다(should) : 권고함 (recommendation)
→ 할 수 있다(may) : 허용함 (something is permitted)

2.1. 암호 사용기준

Guideline 1-1

암호 알고리즘 사용 시, 암호모듈 검증제도 검증대상 암호 알고리즘을 사용할 것을 권고한다.

가이드라인 적용 범위

ⓘ 블록체인 솔루션 전반

미준수 시 위협

⚠ 안전하지 않은 암호 알고리즘 사용 시 데이터 위·변조 등의 위협 발생 가능

가이드라인 준수 방안

암호 알고리즘 사용 시, 암호모듈 검증제도(KCMVP) 검증대상 암호 알고리즘을 사용할 것을 권고한다.

- 검증대상 암호 알고리즘 목록은 [표 2-1]과 같다.
- 각 암호 알고리즘의 상세 규격은 '암호모듈 검증제도' 웹페이지[2]에 명시된 참조 표준을 참고할 수 있다.
- 검증대상 암호 알고리즘 외에 다음 기준을 만족하는 암호 알고리즘을 사용할 수 있다.
  - 공식 표준화 기구(ISO/IEC, ITU-T, ETSI 등) 또는 사실 표준화 기구(IEEE, IETF, W3C, 3GPP, FIDO 등)의 표준 암호 알고리즘
  - 과학기술정보통신부와 한국인터넷진흥원이 발간한 '암호 알고리즘 및 키 길이 이용 안내서'[1]에 명시된 암호 알고리즘

블록체인 솔루션에 사용되는 모든 암호 알고리즘의 목록 및 용도를 관리해야 한다.

분류	암호 알고리즘	
블록 암호	ARIA	운영모드 · 기밀성(ECB, CBC, CFB, OFB, CTR) · 기밀성/인증(CCM, GCM)
	SEED	운영모드 · 기밀성(ECB, CBC, CFB, OFB, CTR) · 기밀성/인증(CCM, GCM)
	LEA	운영모드 · 기밀성(ECB, CBC, CFB, OFB, CTR) · 기밀성/인증(CCM, GCM)
	HIGHT	운영모드 · 기밀성(ECB, CBC, CFB, OFB, CTR)
해시 함수	SHA-2	SHA-224/256/384/512
	LSH	LSH-224/256/384/512/512-224/512-256
	SHA-3	SHA3-224/256/384/512
메시지 인증	해시 함수 기반	HMAC
	블록 암호 기반	CMAC, GMAC
난수 발생기	해시 함수 기반	Hash_DRBG, HMAC_DRBG
	블록 암호 기반	CTR_DRBG
공개키 암호	RSAES	공개키 길이: 2048, 3072 해시 함수: SHA-224, SHA-256
전자 서명	RSA-PSS	공개키 길이: 2048, 3072 해시 함수: SHA-224, SHA-256
	KCDSA	(공개키 길이, 개인키 길이): (2048, 224), (2048, 256) 해시 함수: SHA-224, SHA-256
	EC-KCDSA	P-224, P-256, B-233, B-283, K-233, K-283 해시 함수: SHA-224, SHA-256
	ECDSA	P-224, P-256, B-233, B-283, K-233, K-283 해시 함수: SHA-224, SHA-256
키 설정	DH	(공개키 길이, 개인키 길이): (2048, 224), (2048, 256)
	ECDH	P-224, P-256, B-233, B-283, K-233, K-283
키 유도	KBKDF	HMAC, CMAC
	PBKDF	HMAC

[표 2-1] 암호모듈 검증제도 검증대상 암호 알고리즘

2.2. 계정 관리

Guideline 2-1

계정을 관리할 수 있는 시스템을 제공해야 한다.

가이드라인 적용 범위

ⓘ 플랫폼 계정 관리(5), 앱 계정 관리(17), 블록체인 외부 계정 관리(24)

미준수 시 위협

⚠ 허가형 블록체인에서 참여 개체의 계정 생성 및 폐기, 권한 관리 등을 제공하는 계정 관리 시스템이 없으면 다음과 같은 위협 발생 가능

- 블록체인 내 · 외부에 저장된 민감 데이터 유출
- 악의적인 트랜잭션 또는 블록 생성을 통한 자산 탈취
- 서비스 거부 공격, 중간자 공격 등 사이버 공격에 노출

가이드라인 준수 방안

계정 관리 시스템은 다음을 수행할 수 있다.

- 계정 생성 · 폐기
- 계정의 공개키 등록 · 교체
- 권한 부여 · 조회 · 수정

계정 관리 시스템은 다음과 같은 체계에 기반을 둘 수 있다.

- X.509 인증서 확장 체계
  - ITU-T X.509[13] 및 RFC 5280[6] 문서의 규격을 준수해야 한다.
- 디렉터리 서비스
  - LDAP[12]와 Kerberos[8] 구현 사례를 참조할 수 있다.
  - 블록체인 외부 계정 관리를 위해 ID/PW 기반의 디렉터리 서비스를 사용할 수 있다.
- 자기 주권 신원 구조
  - Verifiable credential[16]과 DID[15] 규격을 참조할 수 있다.

본 절의 가이드라인은 트랜잭션 및 블록 생성 계정, 관리자 계정 등 분산 원장 생성에 관여하는 계정에 적용된다. 계정은 블록체인 노드(blockchain node), 서비스 제공자(service provider), 최종 사용자(end-user), 기기(device), 프로세스(process) 등 다양한 형태의 개체가 소유할 수 있다.

Guideline 2-2

계정을 생성하려는 개체와 계정을 관리하는 시스템은 상호 인증을 수행해야 한다.

가이드라인 적용 범위

ⓘ 플랫폼 계정 관리(5), 관리 인터페이스(11), 앱 계정 관리(17), 탈중앙화 애플리케이션 인터페이스(18), 블록체인 외부 계정 관리(24)

미준수 시 위협

⚠ 계정을 생성하려는 개체의 인증을 수행하지 않을 경우, 해커 등 악의적인 개체가 정당한 개체로 위장하여 블록체인 서비스 참여 가능

⚠ 계정 관리 시스템의 인증을 수행하지 않을 경우, 해커 등 악의적인 개체가 계정 관리 시스템으로 위장하여 블록체인 서비스에 참여하거나 계정을 생성하려 하는 정당한 개체의 블록체인 서비스 참여 차단 가능

가이드라인 준수 방안

계정을 생성하려는 개체는 상대가 블록체인 솔루션의 계정 관리 시스템인지 확인하기 위해 다음을 사용할 수 있다.

- 네트워크 인증: PKI, 디렉터리 서비스, 인증서, 사전 등록된 크리덴셜
- 대면 인증: 계정 생성 위탁 기관 방문 등

계정을 관리하는 시스템은 계정을 생성하려는 개체가 블록체인 솔루션에 참여 가능한 개체인지 확인하기 위해 다음을 사용할 수 있다.

- 네트워크 인증: PKI, 디렉터리 서비스, 인증서
- 본인 인증 서비스: 통신사 인증, 카드사 인증, 은행 인증, iPIN, FIDO
- 개방형 인증 서비스: OAuth, DID, openID
- 대면 인증: 주민등록증, 운전면허증, 여권 등 사진이 포함된 실물 신분증 활용

Guideline 2-3

계정을 생성하려는 개체는 개인키와 공개키 쌍을 안전하게 생성한 후, 공개키를 계정을 관리하는 시스템에 등록하고, 개인키를 안전하게 저장해야 한다.

가이드라인 적용 범위

ⓘ 암호 기능(1), 저장소(2), 보안 하드웨어(3), 플랫폼 계정 관리(5), 앱 계정 관리(17), 계정 정책(20)

미준수 시 위협

⚠ 개인키가 안전하게 생성되지 않거나 저장되지 않으면, 제3자가 개인키를 소유한 계정의 권한 행사 가능

⚠ 공개키가 계정을 관리하는 시스템에 정상적으로 등록되지 않으면, 전자 서명 생성 계정의 권한 확인 불가

가이드라인 준수 방안

계정을 생성하려는 개체는 계정의 개인키를 안전하게 생성 및 저장해야 한다.

- 안전한 하드웨어를 사용할 것을 권고하며, 다음 하드웨어를 사용할 수 있다.
  - 하드웨어 보안 모듈(HSM, Hardware Security Module)
  - 신뢰 플랫폼 모듈(TPM, Trusted Platform Module)
  - 하드웨어 기반 신뢰 실행 환경(TEE, Trusted Execution Environment)
- 안전한 하드웨어를 사용할 수 없는 경우, OS에서 제공하는 소프트웨어 보안 기능을 사용할 것을 권고한다.

계정을 생성하려는 개체는 다음과 같은 절차를 거쳐 공개키를 계정 관리 시스템에 등록해야 한다.

- 개체는 계정 관리 시스템과 Guideline 2-2에서 명시한 상호 인증을 수행해야 한다.
- 상호 인증을 마친 개체는 공개키를 계정 관리 시스템에 전송한다.
- 계정 관리 시스템은 개체가 전송한 공개키에 대해 유효성을 확인할 수 있는 인증서를 발급하거나 공개키를 조회할 수 있도록 등록한다.

Guideline 2-4

계정의 개인키와 공개키 쌍은 교체할 수 있어야 한다.

가이드라인 적용 범위

ⓘ 암호 기능(1), 플랫폼 계정 관리(5), 앱 계정 관리(17), 계정 정책(20)

미준수 시 위협

⚠ 기기 변경, 유효기간 만료, 개인키 유출 등이 발생했을 때 개인키와 공개키 쌍을 교체할 수 없으면 계정의 안전한 사용 불가

가이드라인 준수 방안

- 계정의 개인키와 공개키 쌍은 교체할 수 있어야 한다.
  - 계정의 주 식별자로 공개키를 사용하는 경우, 새로운 키 쌍을 이용하여 계정을 생성하고 이전 계정을 폐기하는 방법을 사용할 수 있다.
  - 계정의 주 식별자로 ID 등을 사용하는 경우, 계정 정보에 포함된 공개키를 교체하는 방법을 사용할 수 있다.
- 키의 유효기간을 설정하여 주기적으로 계정의 개인키와 공개키 쌍이 교체되도록 할 것을 권고한다.
  - 유효기간은 사용 환경, 서비스 등을 고려하여 설정할 수 있다.
- 키가 교체되거나 유효기간이 만료되는 즉시 이전 키는 새로운 기록 및 통신 등에 사용할 수 없어야 한다.
  - 공개키의 경우 교체되거나 유효기간이 만료되어도 지난 기록의 검증 등을 위하여 일정 기간 사용할 수 있다.
- 지난 기록의 검증, 서비스의 연속성 등을 고려하여 교체 이전의 공개키를 관리할 수 있다.
- 신규 개인키와 공개키 쌍은 Guideline 2-3에서 명시한 방법에 따라 안전하게 생성 · 등록 · 저장되어야 한다.
- 키 교체, 유효기간 설정 등 키 관리 고려사항은 미국 NIST가 발간한 'NIST SP 800-57 Part 1 Rev. 5, Recommendation for Key Management: Part 1 – General'[14]을 참고할 수 있다.

Guideline 2-5

계정은 폐기할 수 있어야 하며, 폐기된 계정은 폐기 즉시 사용할 수 없어야 한다.

가이드라인 적용 범위

ⓘ 플랫폼 계정 관리(5), 앱 계정 관리(17), 계정 정책(20), 블록체인 외부 계정 관리(24)

미준수 시 위협

⚠ 계정이 정상적으로 폐기되지 않으면 공격자가 해당 계정을 공격에 이용 가능

가이드라인 준수 방안

계정의 폐기 여부를 확인할 수 있는 기능을 제공할 것을 권고한다.

- 공개키의 인증을 위해 공개키 기반 구조(PKI)를 이용하는 경우, 계정 관리 시스템은 인증서 폐기 목록(CRL) 또는 온라인 인증서 상태 프로토콜(OCSP)을 활용하여 블록체인 참여 개체가 계정이 소유한 공개키의 유효성을 확인할 수 있는 기능을 제공할 것을 권고한다.
- 디렉터리 서비스를 이용하는 경우, 계정 관리 시스템은 블록체인 참여 개체가 계정의 유효성을 확인할 수 있는 기능을 제공할 것을 권고한다.
- DID, 블록체인 기반 계정 관리 시스템 등 탈중앙화 시스템을 이용하는 경우, 계정의 폐기 여부를 모든 참여 개체가 조회할 수 있는 블록체인에 기록할 것을 권고한다.

2.3. 데이터 전송 보안

Guideline 3-1

블록체인 시스템 내의 개체와 데이터를 주고받으려는 개체는 상호 인증을 수행해야 한다.

가이드라인 적용 범위

ⓘ P2P/통신 프로토콜(6), 관리 인터페이스(11), 블록체인 네트워크(12), 블록체인 솔루션 간 인터페이스(13), 블록체인 외부 시스템 인터페이스(14), 탈중앙화 애플리케이션 인터페이스(18)

미준수 시 위협

⚠ 상대의 식별 및 인증이 이루어지지 않으면 공격자가 적법한 개체로 위장하여 정보를 탈취하거나 악의적인 행위 가능

가이드라인 준수 방안

상대에 대한 인증은 전자 서명을 이용할 것을 권고한다.

- 전자 서명은 식별자와 재전송 공격을 방지하기 위한 데이터를 포함해야 한다.
- 전자 서명을 사용할 수 없는 경우, 지식 기반 또는 소유 기반 인증 등을 사용할 수 있다.

Guideline 3-2

블록체인 솔루션에서 전송되는 모든 데이터를 안전하게 보호해야 한다.

가이드라인 적용 범위

ⓘ P2P/통신 프로토콜(6), 관리 인터페이스(11), 블록체인 네트워크(12), 블록체인 솔루션 간 인터페이스(13), 블록체인 외부 시스템 인터페이스(14), 탈중앙화 애플리케이션 인터페이스(18), 네트워크 구성(23)

미준수 시 위협

⚠ 전송 데이터가 안전하게 보호되지 않으면 데이터의 탈취 · 위조 · 변조 등의 공격 가능

가이드라인 준수 방안

안전한 암호학적 프로토콜을 활용하여 전송 데이터의 기밀성과 무결성을 보장해야 한다.

- 안전한 암호학적 프로토콜에서 사용되는 암호 알고리즘은 Guideline 1-1을 만족하여야 한다.
- 안전한 암호학적 프로토콜로는 TLS 또는 DTLS를 사용할 것을 권고한다.
  - TLS 1.2 또는 DTLS 1.2 이상을 사용해야 한다.
- 단, 누구에게나 공개되어도 무방한 데이터의 경우 기밀성을 보장하지 않을 수 있으나 이로 인한 블록체인 솔루션의 안전성 저하가 발생하지 않아야 한다.

2.4. 합의 프로토콜

Guideline 4-1

제공하려는 서비스 환경에 요구되는 안전성 · 효율성 특성(장애 허용, 처리 속도 등)을 만족하는 합의 프로토콜을 사용해야 한다.

가이드라인 적용 범위

ⓘ 합의 프로토콜(9), 블록체인 네트워크(12), 운영 정책(22), 네트워크 구성(23)

미준수 시 위협

⚠ 안전하지 않거나 서비스 환경에 부합하지 않는 합의 프로토콜을 사용할 경우 서비스 장애 발생 가능

가이드라인 준수 방안

다음 조건을 만족하는 합의 프로토콜을 사용해야 한다.

- 항상 정해진 규칙을 만족하는 합의에 도달해야 한다(liveness, safety).
  - 합의에 참여하는 노드 중 일부에 장애가 발생하더라도 합의를 도출할 수 있는 합의 프로토콜을 사용해야 한다.
  - 합의에 참여하는 노드가 담합, 거짓 응답 등 프로토콜의 규칙을 의도적으로 위반하는 행위를 할 가능성이 있는 경우 비잔틴 장애 허용(BFT) 기능을 제공하는 합의 프로토콜을 사용해야 한다.
- 합의가 완료되어 원장에 기록된 블록은 삭제되지 않아야 한다(finality).

합의 프로토콜을 결정할 때 트랜잭션 처리 속도를 고려해야 한다.

- 단위 시간당 최대 트랜잭션 처리량과 트랜잭션이 변경될 수 없는 상태가 될 때까지 걸리는 시간을 고려해야 한다.

Guideline 4-2

합의에 참여하는 노드 수는 서비스 환경과 합의 프로토콜을 고려하여 결정해야 한다.

가이드라인 적용 범위

ⓘ 합의 프로토콜(9), 블록체인 네트워크(12), 운영 정책(22), 네트워크 구성(23)

미준수 시 위협

⚠ 충분한 수의 노드가 확보되지 않은 상황에서 일부 노드에 장애 또는 공격이 발생할 경우, 다음과 같은 위협 발생 가능

- 합의 도출 실패로 인한 서비스 중단 위협
- 공격자가 의도한 합의 도출로 인한 자산 탈취 등의 위협

가이드라인 준수 방안

서비스 환경에서 동시에 발생 가능한 최대 장애 노드의 수를 x라고 가정할 경우, 장애에 대한 내성을 가지기 위해 합의에 참여하는 노드의 수(N)는 다음을 만족해야 한다.

- 비잔틴 장애를 고려하지 않는 경우, $N \geq 2x+1$
- 비잔틴 장애를 고려하는 경우, $N \geq 3x+1$
- 단, $N \geq 4x+1$과 같이 더 많은 수의 합의 노드를 요구하는 합의 프로토콜을 사용하는 경우, 그 기준을 따라야 한다.
- 장애는 동시에 둘 이상의 노드에서 발생하는 것($x \geq 2$)을 가정할 것을 권고한다.

안정적이고 효율적인 블록체인 서비스 운영을 위해 노드를 다음과 같은 방법으로 구축할 수 있다.

- 물리적으로 원격지에 구축
- 안전한 클라우드에 구축
  - 노드를 클라우드에 구축할 때 행정안전부에서 발간한 '행정 · 공공기관 민간 클라우드 이용 가이드라인'[3]을 참고할 수 있다.

※ 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(법률 제17344호, 2020. 6. 9.)은 국가 · 공공기관의 클라우드컴퓨팅 사용을 권장하고 있다.

탈중앙성을 강화하기 위해 합의에 참여하는 노드들을 다수의 주체가 나누어 관리할 수 있다.

2.5. 원장

Guideline 5-1

트랜잭션에는 트랜잭션의 생성 과정에 참여한 모든 개체의 식별자 및 전자 서명, 재전송 공격을 방지하기 위한 데이터가 포함되어야 한다.

가이드라인 적용 범위

ⓘ 트랜잭션 관리(4)

미준수 시 위협

⚠ 트랜잭션에 식별자 또는 전자 서명이 포함되어 있지 않으면 적법하지 않은 개체가 악의적인 트랜잭션 생성 가능

⚠ 트랜잭션에 재전송 공격을 방지하기 위한 데이터가 포함되어 있지 않으면 원장에 기록된 트랜잭션을 이용하여 재전송 공격 가능

가이드라인 준수 방안

- 트랜잭션 생성 과정에 참여하는 개체는 트랜잭션에 포함될 데이터의 유효성을 검증하고, 자신의 전자 서명을 생성하여야 한다.
  - 트랜잭션 데이터의 유효성 검증 과정에서는 헤더, 입력 데이터 형식, 출력 데이터 형식 및 상태 변화 등을 검증한다.
- 식별자와 전자 서명을 이용해 트랜잭션 생성 과정에 정당한 권한을 가진 개체들이 참여하였음을 확인할 수 있어야 한다.
  - 익명 식별자, 개체가 속한 조직의 식별자 등 특정 개체를 명시하지 않는 식별자도 존재할 수 있다.
- 재전송 공격을 방지하기 위한 데이터로는 생성 시각을 활용할 것을 권고한다.
  - 생성 시각은 협정 세계시(UTC)를 사용할 것을 권고한다.

Guideline 5-2

블록을 생성하는 개체는 블록에 포함할 트랜잭션 생성에 참여한 개체의 권한과 전자 서명을 검증해야 한다.

가이드라인 적용 범위

ⓘ 트랜잭션 관리(4), 원장 관리(7), 블록체인 네트워크(12)

미준수 시 위협

⚠ 트랜잭션 생성에 참여한 개체의 권한 또는 전자 서명을 검증하지 않으면 트랜잭션 위·변조 공격 발생 가능

가이드라인 준수 방안

- 블록을 생성하는 개체는 트랜잭션 생성에 참여한 모든 개체의 권한과 전자 서명을 검증해야 한다.
- 블록을 생성하는 개체는 블록에 포함할 트랜잭션 데이터의 유효성을 검증할 것을 권고한다.
  - 트랜잭션 데이터의 유효성 검증 과정에서는 헤더, 입력 데이터 형식, 출력 데이터 형식 및 상태 변화 등을 검증한다.

Guideline 5-3

블록 헤더에 직전 블록의 해시값이 포함되어야 한다.

가이드라인 적용 범위

원장 관리(7)

미준수 시 위협

블록체인의 무결성이 보장되지 않아 확정된 블록의 위·변조 및 삭제 가능

가이드라인 준수 방안

블록의 해시값은 블록의 고유 정보로서 동일한 해시값을 가지는 서로 다른 블록을 찾을 수 없어야 한다.

- 해시값을 생성하기 위해서는 Guideline 1-1을 만족하는 암호학적 해시 함수를 사용해야 한다.
- 블록의 해시값을 생성하기 위한 입력으로 다음을 사용할 수 있다.
  - 블록 전체
  - 블록 내 모든 트랜잭션의 해시값이 포함된 블록 헤더

Guideline 5-4

블록에는 블록을 생성한 개체의 식별자 및 전자 서명, 생성 시각이 포함되어야 한다.

가이드라인 적용 범위

ⓘ 원장 관리(7), 블록체인 네트워크(12)

미준수 시 위협

⚠ 블록에 블록을 생성한 개체의 식별자 또는 전자 서명이 포함되지 않으면 적법하지 않은 개체가 악의적인 블록 생성 가능

⚠ 블록에 생성 시각이 포함되지 않으면 합의에 참여하는 노드들이 블록 생성을 위한 기준 시각을 동기화하기 어려워 합의 프로토콜 오동작 가능

가이드라인 준수 방안

식별자와 전자 서명을 이용해 정당한 권한을 가진 개체가 블록을 생성하였음을 확인할 수 있어야 한다.

- 익명 식별자, 개체가 속한 조직의 식별자 등 특정 개체를 명시하지 않는 식별자도 존재할 수 있다.

블록을 생성하는 개체는 블록 내 트랜잭션에 포함된 모든 전자 서명을 검증하고, 자신의 전자 서명을 생성하여야 한다.

블록체인 시스템 내 모든 개체의 시각은 동일하게 유지되어야 한다.

- 시각은 협정 세계시(UTC)를 사용할 것을 권고한다.

2.6. 스마트 컨트랙트

Guideline 6-1

스마트 컨트랙트의 실행 결과는 검증할 수 있어야 한다.

가이드라인 적용 범위

ⓘ 스마트 컨트랙트(8), 탈중앙화 애플리케이션(15), 프라이버시(21)

미준수 시 위협

⚠ 스마트 컨트랙트 실행 개체가 실행 결과 조작 가능

가이드라인 준수 방안

- 스마트 컨트랙트의 실행 결과를 검증할 수 있도록 트랜잭션 검증 노드에게 스마트 컨트랙트의 명세와 매 실행 시 사용된 입력값과 출력값이 제공되어야 한다.
  - 스마트 컨트랙트의 명세로는 소스코드나 컴파일된 코드 등을 사용할 수 있다.
- 단, 기업 기밀 유지, 개인정보 보호 등의 목적으로 앞에서 명시한 정보를 공개하지 않을 수 있지만, 이 경우에도 검증할 수 있어야 한다.
  - 정보를 공개하지 않고 실행 결과를 검증하기 위해서 해시 함수, 영지식 증명 등의 암호학적 방법 또는 하드웨어 기반 신뢰 실행 환경(TEE)을 활용한 실행 정보 은폐, 정보 공개 대상 제한 등의 비암호학적 방법을 사용할 수 있다.

Guideline 6-2

스마트 컨트랙트에는 알려진 소스코드 보안 취약점이 존재하지 않아야 한다.

가이드라인 적용 범위

ⓘ 원장 관리(7), 스마트 컨트랙트(8), 구현(19)

미준수 시 위협

⚠ 소스코드 보안 취약점을 이용한 비정상적인 코드 실행을 통해 자산 탈취, 서비스 거부 공격 등 가능

가이드라인 준수 방안

스마트 컨트랙트의 소스코드 보안 취약점을 진단하고 보완해야 한다.

- 행정안전부와 한국인터넷진흥원이 발간한 '소프트웨어 개발보안 가이드'[4] 및 '소프트웨어 보안약점 진단가이드'[5]를 참고할 수 있다.
- 알려진 보안 취약점과 대응 방안이 게시된 사이트를 참고할 수 있다.
  - SWC registry, CVE 등
- 보안 취약점 진단 도구 등을 활용하여 취약점을 진단하고 보완할 것을 권고한다.

2.7. 데이터베이스

Guideline 7-1

하나의 이벤트에서 발생하는 여러 데이터를 블록체인 솔루션 내 다수의 저장소에 기록하는 경우, 일부 저장소에 장애가 발생하여도 기록된 데이터의 신뢰성을 보장할 수 있어야 한다.

가이드라인 적용 범위

ⓘ 원장 관리(7), 합의 프로토콜(9), 블록체인 솔루션 간 인터페이스(13), 블록체인 외부 시스템 인터페이스(14), 앱 데이터 관리(16), 운영 정책(22), 오프체인 저장소(25)

미준수 시 위협

⚠ 하나의 이벤트에서 발생하는 여러 데이터를 다수의 저장소에 기록하는 과정에 장애가 발생하면 데이터의 충돌 또는 손실, 서비스 장애 등의 피해 발생 가능

※ 블록체인 솔루션 내 저장소는 블록체인 시스템 내·외부의 블록체인을 비롯하여 데이터를 보관할 수 있는 모든 형태의 저장소를 포함한다.

하나의 이벤트에서 발생하는 여러 데이터를 다수의 블록체인에 저장할 때, 저장되는 데이터는 다를 수 있다.

예 1 (계좌 거래 이력을 멀티체인으로 관리하는 경우) :

- 철수가 영희에게 만 원을 이체하는 경우,
  A(이체 기록) 저장소에는 '철수 계좌에서 영희 계좌로 만 원 이체',
  B(출금 기록) 저장소에는 '철수 계좌에서 만 원 출금',
  C(입금 기록) 저장소에는 '영희 계좌에 만 원 입금' 기록

예 2 (스마트 의료 시스템을 온·오프체인 저장소로 관리하는 경우) :

- 병원에서 진료를 받은 경우,
  상세 진료 기록은 개인정보 보호를 위해 오프체인 저장소 A에 기록하고,
  기록의 무결성을 보장하기 위해 진료 기록의 해시값과 메타 데이터를
  온체인 저장소 B에 기록

가이드라인 준수 방안

블록체인은 데이터를 저장하고 관리한다는 측면에서 데이터베이스와 유사한 기능을 제공하므로, 데이터베이스가 장애 발생 시에도 데이터의 신뢰성을 보장하기 위해 가져야 하는 성질인 ACID(Atomicity, Consistency, Isolation, Durability)를 만족할 것을 권고한다.

※ 블록체인은 합의 과정에서 일시적으로 ACID 성질을 만족하지 못할 수 있다.

- (원자성, Atomicity) 기록하려는 저장소에 모두 기록해야 한다. 일부 저장소에만 부분적으로 기록해서는 안 된다.
- (일관성, Consistency) 기록하려는 여러 데이터는 하나의 이벤트를 정확히 나타내야 한다.
- (고립성, Isolation) 하나의 이벤트를 기록하는 작업이 완료되기 전까지 다른 이벤트는 기록 중인 어떤 데이터에도 접근할 수 없어야 한다.
- (지속성, Durability) 한 번 기록된 데이터는 취소될 수 없어야 한다.
  ※ 이 성질은 블록체인이 제공하는 고유 성질 중의 하나이다.

예 1 에서의 ACID 성질

- **원자성** (Atomicity) : 저장소 A, B, C에 모두 기록되어야 한다.
- **일관성** (Consistency) : 저장소 A, B, C에 기록하려는 여러 데이터에서 출금 계좌는 철수 계좌, 입금 계좌는 영희 계좌, 금액은 만 원을 나타내야 한다.
- **고립성** (Isolation) : 저장소 A, B, C에 기록이 완료되기 전까지 철수 계좌나 영희 계좌에서 입 · 출금을 할 수 없어야 한다.
- **지속성** (Durability) : 저장소 A, B, C에 기록이 완료되면, 이체 기록은 취소될 수 없어야 한다.

3
용어 정의

개인키 private key

공개키 암호 체계(public key cryptosystem)에서 각 사용자가 독립적으로 소유한 암호키의 하나로, 체계의 다른 사용자에게 공개하지 않고 비밀로 관리하여 사용하는 키

- 참고 1: 개인키는 전자 서명 생성과 같이 개인키를 소유한 사용자임을 증명해야 하는 암호학적인 작업을 위해 사용된다.

개체 entity

정보·통신 기술 시스템 내부 또는 외부의 사람, 기관, 기기, 프로세스 또는 이들의 집합

계정 account

시스템에 등록된 개체를 관리할 수 있는 식별자

- 참고 1: 블록체인 솔루션에서 계정은 블록체인 노드(blockchain node), 서비스 제공자(service provider), 최종 사용자(end-user), 기기(device), 프로세스(process) 등 다양한 형태의 개체가 소유할 수 있다.

공개키 public key

공개키 암호 체계(public key cryptosystem)에서 각 사용자가 독립적으로 소유한 암호키의 하나로, 체계의 모든 사용자에게 공개하여 사용하는 키

- 참고 1: 사용자의 공개키는 해당 사용자의 고유 정보이다.
- 참고 2: 각 사용자의 공개키는 해당 사용자의 개인키와 특수한 수학적인 관계성이 존재한다.
- 참고 3: 공개키는 전자 서명 검증과 같이 특정 사용자(또는 사용자 정보)를 확인하는 암호학적인 작업을 위해 사용된다.

공개키 기반 구조 PKI, Public Key Infrastructure

사용자 공개키에 대한 인증서를 공신력을 가진 인증 기관이 전자적으로 생성하고 발급 및 관리함으로써 공개키 암호 체계의 안전성과 신뢰성을 보장하기 위한 보안 인프라

- 참고 1: 인증서 형식을 비롯하여 PKI의 인증 서비스를 구현하기 위한 대표적인 인증 프레임워크로 ITU-T의 X.509[13]가 많이 사용된다.

공개키 암호 public key cryptography

공개키 암호 체계(public key cryptosystem)에서 공개키를 사용하는 기능과 개인키를 사용하는 기능을 제공하는 함수로 구성되어, 공개키와 개인키의 비대칭적인 특성에 기반하여 암호화, 전자 서명 생성 · 검증, 키 교환 등의 기능을 제공할 수 있는 암호기술

기밀성 confidentiality

인가되지 않은 개체(unauthorized entity)에 의해 발생할 수 있는 특정 데이터의 정보 노출을 방지하는 특성

- 참고 1: 기밀성은 정보에 대한 암호화를 통해 보장할 수 있다.
- 참고 2: 암호화에 사용되는 대표적인 암호기술로 블록 암호, 스트림 암호, 공개키 암호 등을 들 수 있다.

디렉터리 서비스 directory service

네트워크 내에 분산된 디렉터리를 하나로 관리하여, 사용자나 사용자 프로그램이 요구하는 디렉터리의 정보 검색, 변경, 추가, 삭제 등의 서비스를 제공하는 기능 단위

- 참고 1: 디렉터리는 논리, 계층 방식 속에서 조직화 된, 비슷한 특성을 가진 객체들의 모임이다.
- 출 처: 국립국어원

멀티체인 multi-chain

블록체인 시스템에서 논리적으로 분리된 체인으로 구성된 특성 또는 이러한 특성을 가지는 다수의 체인

무결성 integrity

특정 데이터가 위 · 변조되지 않았다는 것을 보장하는 성질

- 참고 1: 무결성은 메시지 인증 코드, 전자 서명 등의 방법으로 보장할 수 있다.

분산 원장 distributed ledger

합의 프로토콜을 사용하여 네트워크에 분산된 개체들이 공유 · 복제 · 동기화하는 원장

블록 block

트랜잭션의 묶음과 블록 헤더로 이루어진 블록체인의 자료 구조

블록 암호 block cipher

특정 크기의 데이터를 대상으로 암호키(cryptographic key)의 작용에 의해 같은 크기의 다른 데이터로 변환하는 암호기술

- 참고 1: 블록 암호의 기본 처리 단위로는 주로 64비트 또는 128비트를 많이 사용한다.
- 참고 2: 블록 암호에 사용되는 암호키는 허가된 사용자 이외에는 비밀로 관리되는 것을 가정한다. 암호키의 크기(비트)는 128 이상이어야 한다.

블록 헤더 block header

블록의 메타 데이터를 포함하는 자료 구조

- 참고 1: 일반적으로 블록 헤더는 생성 시각과 이전 블록의 해시값을 포함한다.

블록체인 blockchain

합의된 블록을 암호학적 해시 함수를 이용하여 덧붙이기만 가능하도록 차례로 연결한 분산 원장

블록체인 노드 blockchain node

블록체인 네트워크에 참여하는 기기 또는 프로그램

블록체인 솔루션 blockchain solution

블록체인 시스템을 이용하여 블록체인 기반 서비스를 제공하는 데 필요한 모든 기능을 통합 구현한 솔루션([그림1-3] 참조)

- 참고 1: 블록체인 솔루션은 블록체인 시스템을 기반으로 블록체인 오라클, 오프체인 저장소, 블록체인 외부 애플리케이션 등 블록체인 외부 시스템을 포함한 개념이다.

블록체인 시스템 blockchain system

블록체인 SW 플랫폼을 탑재한 노드들로 사전에 정의된 정책에 따라 네트워크를 구성하고 노드들이 블록체인을 공유할 수 있도록 구현한 시스템([그림1-3] 참조)

블록체인 오라클 blockchain oracle

블록체인 시스템 외부에서 생성된 데이터를 이용하여 블록체인에 정보를 제공하는 서비스

- 출 처: ITU-T Technical Specification FG DLT D1.1, Distributed ledger technology terms and definitions

블록체인 SW 플랫폼 blockchain software platform

블록체인 노드가 블록체인 시스템에 참여할 수 있도록 제공되는 프로세스, 저장소, 통신 기능의 집합([그림1-3] 참조)

비잔틴 장애 허용 BFT, Byzantine Fault Tolerance

분산 환경에서 비잔틴 장애(단순 장애뿐만 아니라 담합, 거짓 응답 등 프로토콜의 규칙을 의도적으로 위반하는 행위)가 발생해도 정상적으로 합의를 도출할 수 있는 성질

- 참고 1: 단, 전체 분산 개체 중 1/3 이상의 비잔틴 장애를 허용하는 프로토콜은 존재할 수 없다는 것이 증명되었다.

비허가형 블록체인 permissionless blockchain

블록체인을 유지 · 관리하는 합의 절차에 허가 없이 누구나 참여할 수 있는 블록체인

서비스 거부 공격 denial of service attack

정보 시스템에 과도한 부하를 일으켜 시스템의 데이터나 자원을 정당한 사용자가 적절한 대기 시간 내에 사용하는 것을 방해하는 공격

스마트 컨트랙트 smart contract

모든 실행 결과가 블록체인에 기록되는 블록체인 시스템상의 컴퓨터 프로그램

식별자 ID, Identifier

서로 다른 개체를 구별할 수 있는 정보

신뢰 실행 환경 TEE, Trusted Execution Environment

독립된 보안 영역이 제공하는 안전한 실행 환경

- 참고 1: 일반 영역과 보안 영역이 따로 분리된 프로세서에서, 보안 영역에는 생체 정보, 결제 정보, 기업 보안 문서 등의 중요한 정보가 저장된다. 일반 영역과의 정보 교환이 통제되고 보안 소프트웨어가 안전하게 실행될 수 있다.
- 출 처: TTA 정보통신용어사전

신뢰 플랫폼 모듈 TPM, Trusted Platform Module

암호화된 키, 패스워드, 디지털 인증서 등을 저장하는 안전한 저장 공간을 제공하는 보안 모듈

- 출 처: TTA 정보통신용어사전

암호모듈 검증제도 KCMVP, Korean Cryptographic Module Validation Program

행정기관 등 국가·공공기관 정보통신망에서 소통되는 자료 중 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도

오프체인 off-chain

블록체인 시스템과 연관이 있지만, 블록체인 시스템 외부에 위치, 수행, 또는 운영되는 특성

온라인 인증서 상태 프로토콜 OCSP, Online Certificate Status Protocol

특정 인증서의 현재(폐지) 상태를 실시간으로 인증 기관(CA, Certificate Authority)을 통해 확인하는 프로토콜

- 참고 1: 상세 명세는 RFC 6960[11]에 기술되어 있다.

온체인 on-chain

블록체인 시스템 내부에 위치, 수행, 또는 운영되는 특성

완결성 finality

원장에 기록된 트랜잭션이 삭제되지 않음을 보장하는 성질

- 참고 1: 블록체인 기술에서의 완결성은 트랜잭션의 묶음인 블록이 삭제되지 않는다는 것을 의미한다.

원장 ledger

완결성과 불변성이 요구되는 트랜잭션의 기록을 위한 저장소

응용 프로그래밍 인터페이스 API, Application Programming Interface

응용 소프트웨어와 소프트웨어 플랫폼 사이에 존재하며, 플랫폼상에서 실행하는 애플리케이션 개발을 용이하게 하는 소프트웨어 라이브러리 집합

인증 authentication

개체의 식별 정보의 유효성을 확인하거나 주어진 데이터의 출처를 확인할 수 있는 특성

인증서 certificate

전자 서명을 생성하기 위하여 이용하는 전자적 정보가 해당 사용자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보

- 출 처: 전자서명법(법률 제17359호, 2020. 6. 9.) 제2조제7항

인증서 폐기 목록 CRL, Certificate Revocation List

인증서를 발급한 인증 기관(CA)이 특정 공개 저장소에 관리하는 "현재" 폐지된 인증서 목록

- 참고 1: 상세 명세는 RFC 5280[6]에 기술되어 있다.
- 참고 2: CRL에 등재된 각 인증서는 시리얼 번호로 식별한다.

자기 주권 신원 self-sovereign identity

기존 신원 확인 방식과 달리 분산 네트워크 기술을 활용하여 중앙 시스템에 의해 통제되지 않으며 개개인이 자신의 정보에 완전한 통제권을 갖도록 하는 기술

재전송 공격 replay attack

이전에 전송된 유효한 메시지를 다시 사용하는 공격

전자 서명 digital signature

서명자를 확인하고 서명자가 해당 전자 문서[1]에 서명을 하였음을 나타내는데 이용하기 위하여 해당 전자 문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보

- 참고 1: 전자 서명의 생성과 검증을 위해 각각 서명자가 가진 개인키와 해당 개인키에 대응하는 공개키를 사용함으로써, 서명자의 확인과 부인 방지가 가능하다.
- 출 처: 전자서명법(법률 제17359호, 2020. 6. 9.) 제2조제2항

중간자 공격 man-in-the-middle attack

통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 통신 내용을 바꾸거나 도청하는 공격 기법

- 출 처: TTAK.KO-12.0002/R3 정보 보호 기술 용어

최초 블록 genesis block

블록체인 시스템의 초기 상태를 기록한 블록체인의 첫 번째 블록

크리덴셜 credential

신원이나 자격을 주장하면서 증거로 제출된 데이터 집합

- 출 처: ISO/IEC TS 29003:2018

1) 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보(출처: 전자서명법(법률 제17359호, 2020. 6. 9.) 제2조제1항)

탈중앙화 애플리케이션 DApp, decentralized application

블록체인 솔루션에 참여하는 개체가 블록체인 시스템을 활용할 수 있도록 블록체인 시스템상에서 운영되는 애플리케이션

트랜잭션 transaction

자산의 이동 또는 생성과 같이 블록체인에서 발생하는 이벤트의 기록

하드웨어 보안 모듈 HSM, Hardware Security Module

개인키 등의 비밀 정보를 안전하게 저장, 보관할 수 있고 기기 내부에 프로세스 및 암호 연산 장치가 있어 전자 서명 키 생성, 전자 서명 생성·검증 등이 가능한 하드웨어 장치

- 참고 1: 기기 내부에 저장된 전자 서명 개인키 등 비밀 정보는 장치 외부로 복사 또는 재생성되지 않으며 스마트카드, 유에스비(USB) 토큰 등 다양한 형태로 제작 및 구현이 가능하다.
- 출 처: TTA 정보통신용어사전

합의 consensus

모든 참여자가 하나의 결과에 동의하는 것

합의 프로토콜 consensus protocol

모든 참여자가 합의에 도달하기 위해 약속한 규칙과 절차

- 참고 1: 일반적으로 블록체인 기술에서는 블록체인에 추가할 블록을 결정하는 규칙과 절차를 의미한다.

해시 함수 hash function

임의 길이의 메시지를 일정 길이의 출력값으로 압축하는 알고리즘

- 참고 1: 해시 함수의 출력값을 해시값(hash value)이라 한다.
- 참고 2: 본 가이드라인에서는 역상 저항성, 제2 역상 저항성, 충돌 저항성을 만족하는 암호학적 해시 함수를 가정한다.

허가형 블록체인 permissioned blockchain

블록체인을 유지 관리하는 합의, 계정 관리 등의 절차에 참여하려면 사전 허가가 필요한 블록체인

협정 세계시 UTC, Coordinated Universal Time

국제 협정에 따라 국제 사회가 사용하는 과학적 시간의 표준

- 참고 1: 한국은 UTC+9 시간대를 사용하고 있다.

DTLS Datagram Transport Layer Security

TLS를 UDP(User Datagram Protocol) 통신상에서 활용할 수 있도록 수정한 프로토콜

- 참고 1: DTLS는 데이터 전송에 대한 신뢰성을 보장할 수 있는 전송계층 프로토콜(예: TCP)상에서 동작하도록 설계된 보안 프로토콜인 TLS를 수정하여, 데이터 전송 신뢰성을 보장할 수 없는 UDP 통신에 대한 TLS 수준의 정보보호 서비스를 제공하기 위해 설계되었다.
- 참고 2: DTLS는 UDP의 통신 특성(데이터 누락, 순서 비보장 등)을 반영하여 TLS를 최소한의 수준으로 수정하였다.
- 참고 3: 버전 1.2의 상세 명세는 RFC 6347[10]에 기술되어 있다.

TLS Transport Layer Security

TCP/IP 계층의 서버-클라이언트 통신에 대해 기밀성, 무결성, 인증과 같은 정보보호 서비스를 제공하는 프로토콜

- 참고 1: TLS는 cipher suite와 키 교환 및 사용자 인증을 수행하는 핸드셰이크 단계(handshake layer)와 데이터 암호화 및 메시지 인증을 수행하는 레코드 단계(record layer)로 구성된다.
- 참고 2: TLS는 SSL(Secure Socket Layer) 프로토콜보다 보안성이 강화되었으며, 2020년 현재 1.3 버전이 공개되었다.
- 참고 3: 버전 1.2의 상세 명세는 RFC 5246[7], 버전 1.3의 상세 명세는 RFC 8446[9]에 기술되어 있다.

X.509

ITU-T 표준으로 인증서 구조 명세와 인증 서비스 활용을 위한 관리 메커니즘을 제시하는 공개키 기반 구조(PKI) 프레임워크

- 참고 1: 상세 명세는 ITU-T X.509[13]에 기술되어 있다.

4. 약어

3GPP	3rd Generation Partnership Project
ACID	Atomicity, Consistency, Isolation, Durability
API	Application Programming Interface
BFT	Byzantine Fault Tolerance
CRL	Certificate Revocation List
CVE	Common Vulnerabilities and Exposures
DApp	Decentralized Application
DID	Decentralized Identifiers
DPoS	Delegated Proof of Stake
DTLS	Datagram Transport Layer Security
ETSI	European Telecommunications Standards Institute
FIDO	Fast Identity Online
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
iPIN	Internet Personal Identification Number
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union Telecommunication Standardization Sector

KCMVP	Korean Cryptographic Module Validation Program
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
P2P	Peer-to-Peer
PBFT	Practical Byzantine-Fault Tolerance
PKI	Public Key Infrastructure
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
SSL	Secure Socket Layer
SWC	Smart Contract Weakness Classification
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
UTC	Coordinated Universal Time
W3C	World Wide Web Consortium

5. 체크리스트

번호	점검항목	점검결과
암호 사용기준		
1-1	암호 알고리즘 사용 시, 암호모듈 검증제도 검증대상 암호 알고리즘을 사용할 것을 권고한다.	
계정 관리		
2-1	계정을 관리할 수 있는 시스템을 제공해야 한다.	
2-2	계정을 생성하려는 개체와 계정을 관리하는 시스템은 상호 인증을 수행해야 한다.	
2-3	계정을 생성하려는 개체는 개인키와 공개키 쌍을 안전하게 생성한 후, 공개키를 계정을 관리하는 시스템에 등록하고, 개인키를 안전하게 저장해야 한다.	
2-4	계정의 개인키와 공개키 쌍은 교체할 수 있어야 한다.	
2-5	계정은 폐기할 수 있어야 하며, 폐기된 계정은 폐기 즉시 사용할 수 없어야 한다.	
데이터 전송 보안		
3-1	블록체인 시스템 내의 개체와 데이터를 주고받으려는 개체는 상호 인증을 수행해야 한다.	
3-2	블록체인 솔루션에서 전송되는 모든 데이터를 안전하게 보호해야 한다.	
합의 프로토콜		
4-1	제공하려는 서비스 환경에 요구되는 안전성 · 효율성 특성(장애 허용, 처리 속도 등)을 만족하는 합의 프로토콜을 사용해야 한다.	
4-2	합의에 참여하는 노드 수는 서비스 환경과 합의 프로토콜을 고려하여 결정해야 한다.	

번호	점검항목	점검결과
원장		
5-1	트랜잭션에는 트랜잭션의 생성 과정에 참여한 모든 개체의 식별자 및 전자 서명, 재전송 공격을 방지하기 위한 데이터가 포함되어야 한다.	
5-2	블록을 생성하는 개체는 블록에 포함할 트랜잭션 생성에 참여한 개체의 권한과 전자 서명을 검증해야 한다.	
5-3	블록 헤더에 직전 블록의 해시값이 포함되어야 한다.	
5-4	블록에는 블록을 생성한 개체의 식별자 및 전자 서명, 생성 시각이 포함되어야 한다.	
스마트 컨트랙트		
6-1	스마트 컨트랙트의 실행 결과는 검증할 수 있어야 한다.	
6-2	스마트 컨트랙트에는 알려진 소스코드 보안 취약점이 존재하지 않아야 한다.	
데이터베이스		
7-1	하나의 이벤트에서 발생하는 여러 데이터를 블록체인 솔루션 내 다수의 저장소에 기록하는 경우, 일부 저장소에 장애가 발생하여도 기록된 데이터의 신뢰성을 보장할 수 있어야 한다.	

6. 참고문헌

1. 과학기술정보통신부, 한국인터넷진흥원, “암호 알고리즘 및 키 길이 이용 안내서”, 2018년 12월, <https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=82&ST=&SV=>.

2. 국가정보원, 암호모듈 검증, <https://www.nis.go.kr:4016/AF/1_7_3_1.do>.

3. 행정안전부, “행정 · 공공기관 민간 클라우드 이용 가이드라인”, 2019년 12월, <https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=75072>.

4. 행정안전부, 한국인터넷진흥원, “전자정부 SW 개발 · 운영자를 위한 소프트웨어 개발보안 가이드”, 2019년 11월, <https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=6&mode=view&p_No=259&b_No=259&d_No=88&ST=T&SV=>.

5. 행정안전부, 한국인터넷진흥원, “전자정부 SW개발보안 진단원을 위한 소프트웨어 보안약점 진단가이드”, 2019년 6월, <https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=6&mode=view&p_No=259&b_No=259&d_No=52&ST=T&SV=>.

6. Copper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

7. Dierks, T., and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

8. Neuman, C., Yu, T., Hartman, S., and K. Raeburn, “The Kerberos Network Authentication Service (V5)”, RFC 4120, DOI 10.17484/RFC4120, July 2005, <https://www.rfc-editor.org/info/rfc4120>.

9. Rescorla, E., “The Transport Layer Security (TLS) Protocol Version 1.3”, RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

10. Rescorla, E. and N. Modadugu, “Datagram Transport Layer Security Version 1.2”, RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

11. Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, RFC 6960, DOI 10.17487/RFC6960, June 2013, <https://www.rfc-editor.org/info/rfc6960>.

12. Sermersheim, J., Ed., “Lightweight Directory Access Protocol (LDAP): The Protocol’, RFC 4511, DOI 10.17487/RFC4511, June 2006, <https://www.rfc-editor.org/info/rfc4511>.

13. ITU-T Recommendation X.509. Information technology - Open systems interconnection - The directory: Public-key and attribute certificate frameworks (October 2019)

14. NIST, SP 800-57 Part 1 Rev. 5, “Recommendation for Key Management: Part 1 - General”, May 2020, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>.

15. W3C World Wide Web Consortium Working Draft, Decentralized Identifiers (DIDs) v1.0, 8 November 2020, <https://www.w3.org/TR/did-core/>.

16. W3C World Wide Web Consortium Recommendation, Verifiable Credentials Data Model 1.0, 19 November 2019, <https://www.w3.org/TR/vc-data-model/>.

7. 부록

암호기술	특 성	활용 사례
다중 서명 multi-signature	같은 메시지에 대한 여러 개체의 서명을 집계한 서명을 만들 수 있어 서명 검증의 효율성 높음	Openchain, MultiChain
임계 서명 threshold signature	다중 서명과 유사하나 서명 생성 시 미리 정해진 최소 인원 이상 필요	Libra
은닉 서명 blind signature	서명자와 사용자가 다를 때, 사용자의 문서를 가린 후 서명자가 서명할 수 있어 전자 화폐와 전자 투표에 사용 가능	Hyperledger Fabric
환 서명 ring signature	구성원 누구나 그룹을 생성하여 서명할 수 있고 그룹 원 중 하나의 서명이라는 사실만 드러나서 서명자의 익명성 보장 가능	CryptoNote
영지식 증명 zero-knowledge proof	어떤 문장에 대해 그 문장의 참 · 거짓 여부를 제외한 어떤 것도 노출하지 않고 증명할 수 있으며 익명성 보장에 활용 가능	Zcash, Monero
안전한 다자간 계산 secure multi-party computation	여러 개체가 각자의 정보 공개 없이 어떤 함수의 결과를 공동으로 계산 가능 예) 두 개체가 각자의 수입을 공개하지 않고 누가 더 수입이 많은지 확인 가능	Enigma, Hawk, Wanchain
비밀 분산 기법 secret sharing	비밀값을 여러 개체가 분산하여 저장한 후 미리 정해진 일정 수 이상의 개체들이 모여야 비밀값 복구 가능	SHARVOT, Wanchain
위탁 방식 commitment scheme	어떤 값을 보여주지 않은 상태로 위탁한 후, 필요하면 위탁한 값 공개 가능	Zcash, Monero
불확정 전송 oblivious transfer	송신자가 보낸 여러 개의 정보 중 일부의 정보를 수신자가 받고, 수신자가 어떤 정보를 받았는지에 대해서 송신자는 알 수 없음	Searchain
검증 가능한 랜덤 함수 verifiable random function	비밀키와 공개된 입력을 사용하여 검증 가능한 의사 난수 생성 가능	Algorand, Ouroboros praos
Accumulator	집합에 대한 짧은 위탁으로 특정 원소가 집합에 속하는지 아닌지의 증명 가능	Zerocoin

[표 7-1] 블록체인에서 활용되는 암호기술

블록체인 암호기술 가이드라인

발행일 2020년 12월

발행처 국가정보원

과학기술정보통신부

국가보안기술연구소

한국정보통신기술협회