이 재 원 교수 지도
박사학위 청구논문

블록체인 기반의 신뢰할 수 있는 스마트 컨트랙트 모델 연구

2018

성신여자대학교 대학원
컴퓨터학과
김 혜 리

블록체인 기반의 신뢰할 수 있는 스마트 컨트랙트 모델 연구

이 재 원 교수 지도

이 논문을 박사학위논문으로 제출함

2018년 4월

성신여자대학교 대학원

컴퓨터학과

김 혜 리

인 준 서

김혜리의 박사학위 논문으로 인준함

2018년 4월

심사위원장 김 태 훈 (인)

심 사 위 원 변 혜 원 (인)

심 사 위 원 김 학 경 (인)

심 사 위 원 김 재 중 (인)

심 사 위 원 이 재 원 (인)

성신여자대학교 대학원

논 문 개 요

블록체인을 비롯한 빅데이터, 사물인터넷, 인공지능으로 대표되는 4차 산업 혁명이라는 시대의 변화 속에서 기술의 발전으로 대용량의 정보의 분석이 가능해졌다. 그리고 그 정보가 직접적으로 수익과 연관성을 갖게 되면서 특히 개인정보의 활용과 보호에 대한 조화가 점점 더 중요해 지고 있다.

블록체인은 모든 네트워크 참여자가 거래가 저장된 원장(ledger) 전체를 보관하고 새로운 거래를 반영하는 작업도 공동으로 수행한다. 그 과정에서 원치 않게 블록체인에 등재된 기밀데이터 및 개인정보가 공개될 위험이 있다. 또한 블록체인 기술 자체는 데이터의 무결성과 가용성을 확보함으로써 보안성이 뛰어나다는 평가를 받고 있으나, 데이터의 기밀성을 보장해주는 것은 아니기 때문에 이에 대한 고려가 필요하다.

최근에는 블록체인을 기반으로 한 스마트 컨트랙트를 활용하여 소유권 이전, 상속, 증여, 물품구매 등 다양한 분야에 도입하기 위한 시도가 크게 증가하고 있다. 특히 이러한 분야에서는 개인정보나 민감한 정보들이 다수 포함되기 때문에 이들에 대한 고려가 필수적이며, 블록체인 네트워크에서는 기존과는 다른 접근 방식의 개인정보 보호를 위한 기술 적용과 프로세스가 필요하다. 스마트 컨트랙트가 프로그램이기는 하지만, 기존 어플리케이션의 정보보호와 블록체인이기에 지켜야 할 정보보호를 모두 고려해야 하기 때문이다.

그리하여 본 연구에서는 블록체인 기반 스마트 컨트랙트 실행 시 포함되는 개인정보와 민감정보 관련한 정보보호 이슈를 분석해보고, 분석한 이슈에 대한 해결 방안으로 신뢰할 수 있는 스마트 컨트랙트 모델(TSCM : Trusted Smart Contract Model)을 제안하고자 한다. TSCM은 Smart

Contract가 한번 배포된 프로그램에 대해서는 되돌릴 수 없다는 점을 고려하여 작성된 계약 내용의 법적 지위를 보장하고, 프로그램으로써의 스마트 컨트랙트 신뢰성을 검토한다. 또한, 계약 내용 중에 포함되는 개인정보나 민감정보에 대한 보호조치를 적용하고, 권한이 부여된 사용자만이 내용을 확인할 수 있도록 접근제어를 적용한다. 제안한 설계 방안에 대해서는 개인정보나 민감정보가 많이 포함되게 되는 부동산 계약 사례에 적용하여 실현 가능성에 대한 타진을 해 보았다.

목 차

표 차 례

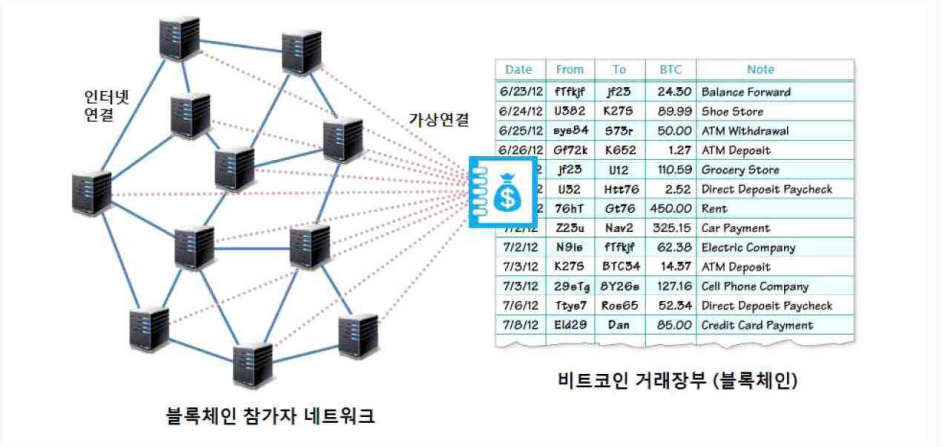
그 림 차 례

제 1 장 서론

1. 연구의 필요성 및 목적

블록체인은 2008년 사토시 나카모토라는 가명의 개발자가 발표한 <Bitcoin : A Peer-to-Peer Electronic Cash System> 논문에 의해 세상에 등장했으며, 블록체인은 이렇게 만들어진 가상화폐 비트코인의 성공에서 비롯됐다[1]. 블록체인은 거래 정보를 기록한 원장을 모든 참가자가 분산(distributed) 보관하고 신규거래가 발생하거나 기존 거래에 편집이 실행되면 암호인증으로 새로운 블록이 체인처럼 연결되는 방식으로서 특정의 제3기관(trusted third party)의 중앙서버가 아닌 온라인 P2P(Peer-to-Peer) 네트워크에 분산하여 참가자가 공동으로 거래정보를 기록・관리하고, 주기적으로 갱신되는 디지털 공동분산원장(mutual distributed ledger)을 의미한다[2].

4차 산업혁명의 기반 기술이자 핵심 기술로 평가받고 있는 블록체인은 다수의 노드들이 거래내역을 검증하여 블록 형태로 보관하기 때문에 위·변조가 매우 어렵고 데이터의 신뢰성을 기반으로 제3자 없이 거래가 가능하다. 또한, 참여하고 있는 모든 구성원이 네트워크를 통해 서로 데이터를 검증하고 저장함으로써 특정인의 임의적인 조작이 어렵도록 설계된 저장 플랫폼이라고도 할 수 있는데, 다음의 (그림 1)과 같이 블록체인 데이터구조는 거래가 담겨 있는 블록이 그 이전 블록과 연결되어 있는 형태의 정돈된 목록이며, 블록체인은 플랫(flat) 파일의 형태로 저장되거나 단순한 데이터베이스 내에 저장될 수 있다[3].



Date	From	To	BTC	Note
6/23/12	fffkjf	jf23	24.50	Balance Forward
6/24/12	U382	K275	89.99	Shoe Store
6/25/12	eys84	873r	50.00	ATM Withdrawal
6/26/12	Gf72k	K652	1.27	ATM Deposit
	jf23	U12	110.59	Grocery Store
	U32	Htt76	2.52	Direct Deposit Paycheck
	76hT	Gt76	450.00	Rent
	Z25u	Nav2	325.15	Car Payment
7/2/12	N9ie	fffkjf	62.38	Electric Company
7/3/12	K275	BTC54	14.37	ATM Deposit
7/3/12	29eTg	8Y26e	127.16	Cell Phone Company
7/6/12	Ttye7	Ros65	52.34	Direct Deposit Paycheck
7/8/12	Eld29	Dan	85.00	Credit Card Payment

(그림 1) 블록체인 개념도[3]

블록체인은 이렇듯 비트코인의 기반기술로 소개되었지만 최근에는 다양한 목적으로 발전되고 있으며, 그 중 가장 주목할 만한 것이 블록체인 상에서 합의 프로토콜에 의해 강제적으로 실행되는 프로그램인 스마트 컨트랙트(Smart Contracts)이다. 스마트 컨트랙트는 1994년 Nick Szabo에 의해 고안되었으며, 최초 발안자가 말하는 스마트 컨트랙트의 목적은 신뢰할 수 없는 컴퓨터 네트워크 환경에서 고도로 발달된 자동 계약 이행 방법을 제시하는 것이다[4]. 스마트 컨트랙트에서는 주어진 계약 조건은 프로그램화 되어 자동적으로 수행되면서 계약 조건이 만족되면 예외없이 강제적으로 실행이 된다. 조건에 의해 거래가 자동적으로 성립되므로 중간관리자에 의한 사기 피해를 막을 수 있으며, 거래정보 기록이 보존되기 때문에 계약서 위조·사고기록 조작 등과 같은 악의적 행위의 방지가 가능하므로 소유권 이전, 상속, 증여, 물품구매 등 다양한 분야에 도입하기 위한 시도가 증가하고 다. 반면에 이러한 거래 계약에는 거래 주체를 확인할 수 있는 개인정보와 민감한 정보들을 다루게 될 수 있는데, 블록체인 네트워크라는 특성상 참여자들의 합의 과정에서 거래내역이

공개가 될 수 있어 개인정보보호 문제가 매우 중요한 문제로 급부상하고 있다.

사실, 기존 디지털 화폐 기능의 비트코인에서는 서로간의 송금에 대한 정보만이 필요했기 때문에 이러한 문제에 대한 고려가 필요하지 않았다. 그러나 이더리움을 기반으로 스마트 컨트랙트로 기술이 진화하면서 더 많은 정보들을 담게 되었고, 블록체인이 가진 기술의 문제점으로 스마트 컨트랙트를 기존과 같이 적용했을 때에는 개인정보보호 및 정보보호 측면에서 많은 문제점을 가질 수 있게 되었다.

특히, 블록체인은 모든 데이터가 서로 연결된 체인과 같은 형태로 데이터의 선택 삭제가 불가능하기 때문에 데이터에 대한 관리와 설계가 중요하다. 또한 한번 배포된 스마트 컨트랙트는 복구가 어렵기 때문에, 문제가 발생하면 이에 대한 손실이 막대하므로 배포전 설계에 대한 부분이 가장 중요하다고 볼 수 있겠다. 그리하여 본 연구에서는 블록체인 기반의 스마트 컨트랙트에서 발생할 수 있는 개인정보보호 이슈를 컴플라이언스 준수와 기술적 측면에서 정리해 보았으며, 이슈 분석을 기반으로 신뢰할 수 있는 스마트 컨트랙트 설계와 적용 방안을 제안하고자 한다.

2. 연구의 범위 및 논문 구성

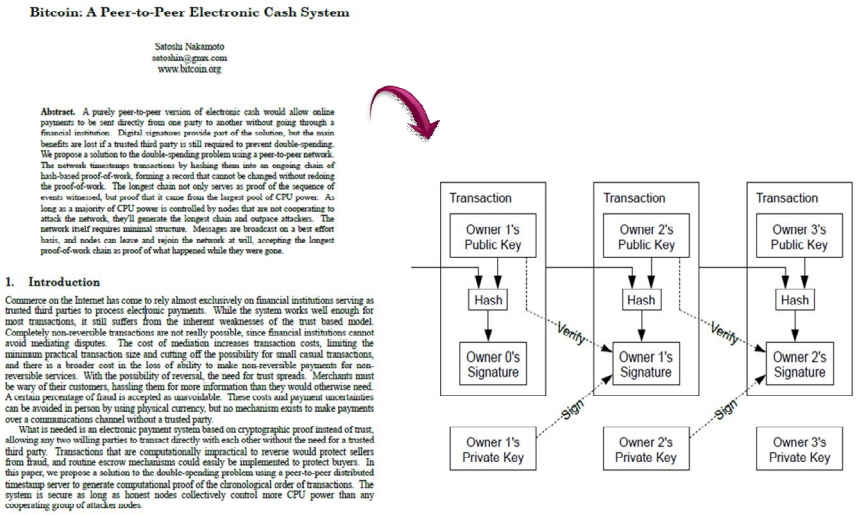
본 논문의 목표는 개인정보보호 및 정보보호를 고려한 블록체인 기반의 신뢰할 수 있는 스마트 컨트랙트 모델을 설계하는 것이다. 우선 본 연구의 목를 달성을 위해 기존의 블록체인이나 스마트 컨트랙트가 가지고 있는 개인정보보호 및 정보보호 관점의 문제점을 분석하고, 문제점을 해결하기 위한 요구 사항을 정의 하였다. 정의된 요구사항을 기반으로 최종적으로 블록이 생성되기 전에 트랜잭션에 포함되는 개인정보와 민감정보에 대해 보호 적용한 스마트 컨트랙트를 설계 하였다. 설계 방안에 대해서는 부동산 거래 계약을 사례로 선정하여 가능성을 확인해 보고자 하였다. 부동산 거래 계약은 블록체인 기반의 스마트 컨트랙트를 활용하면 온라인에서도 신뢰할 수 있는 실물 자산을 거래할 수 있게 된다는 점에서 좋은 사례가 될 수 있으며, 부동산 거래 계약에는 신분 확인과 계약서 작성 과정에서 많은 개인정보와 민감정보들이 포함되기 때문에 본 설계 방안을 적용해 보기 위한 사례로 선정하였다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인과 스마트 컨트랙트, 개인정보보호에 대한 이론에 대해 정리해 보고 3장에서는 블록체인 기반의 개인정보보호를 중심으로 선행 연구와 문제점을 분석 해 보았다. 4장에서는 블록체인 환경에서 발생할 수 있는 개인정보보호 및 정보보호 이슈를 기반으로 신뢰할 수 있는 스마트 컨트랙트 모델을 제안한다. 5장에서는 제안한 모델에 대해 사례를 통한 검증을 진행하였으며, 6장에서는 연구에 대한 결론을 맺는다.

제 2 장 이론적 배경

1. 블록체인

블록체인은 2008년 사토시 나카모토라는 가명 개발자가 발표한 <Bitcoin : A Peer-to-Peer Electronic Cash System> 논문에 의해 세상에 등장했으며, 블록체인은 이렇게 만들어진 가상화폐 비트코인의 성공에서 비롯됐다[1].



(그림 2) 사토시 나카모토의 논문 및 제안한 블록체인 트랜잭션 구조[1]

사토시 나카모토가 제안한 비트코인의 거래 과정을 살펴보면, 각 암호키 소유자들은 그 전까지의 거래내역에 다음 소유자의 공개키를 덧붙인 뒤에 자신의 비밀키로 암호화하는 디지털 서명을 하고 넘긴다. 돈을 받는 사람은 서명 소유자들의 체인과, 서명을 검증할 수 있다. 블록 안에는 거래 주체의 주소와 금액, 시간 등 거래에 관한 모든 내역이 기록되고 10분간의 모든 기록들이 모여 블록을 형성하고 공신력이 부여된다[5].

블록은 블록체인의 기본단위로서 일정 시간 동안의 거래 내역을 순서대로 저장해 놓은 데이터베이스를 말한다. 각각의 블록은 거래정보를 포함하고 있고, 블록은 블록크기(4byte)와 메타 정보를 가지고 있는 헤더(80byte), 그리고 블록에 기록된 거래에 대한 정보로 구성된다[6].

[표 1] 블록의 구조[6]

분류	내용	크기
블록 크기 (Blocksize)	블록헤더, 거래건수, 거래내역들에 대한 전체 크기	4Byte
블록 헤더 (Blockheader)	이전 블록의 해시 값, 거래내역의 머클루트 등 총 6개의 정보로 구성되며 블록 간의 연결 및 무결성 확보 등의 역할을 수행하는 블록에 기록된 메타정보	80Byte
거래 건수 (Transaction Counter)	블록에 포함되어 있는 거래내역의 전체 건수	1~9Byte
거래 내역 (Transactions)	실제 발생한 거래정보, 블록에 기록된 거래	Transaction Count

블록체인은 거래 내역을 암호화한 뒤 해당 네트워크 구성원 간에 공유 및 대조함으로써 위·변조를 불가능하게 함으로써 보안성과 신뢰성을 보장한다. 보안성과 신뢰성을 보장하되 기존과 같이 거래를 중개하는 제3의 기관의 개입없이 개인이나 기관 간 직접 거래가 가능하다는 탈중개성이 블록체인 기술의 대표적인 장점이다.

적은 비용으로 안전한 거래를 할 수 있다는 점에서 효율성 또한

뛰어나다. 블록체인에 기반한 거래는 제3의 기관 없이 운영되기 때문에 수수료를 절감할 수 있다. 거래 시간 단축과 비용 절감으로 자금 조달·운용 효율성을 높인다. 이러한 특징으로 금융을 중심으로 공공분야와 의료, 물류, 콘텐츠 등 다양한 산업 분야에서 주목받고 있으며 인공지능, 사물인터넷, 빅데이터 등과 함께 4차 산업혁명을 이끄는 핵심 기술로 꼽힌다.

(그림 3) 블록체인 개요도[7]

1) 합의 알고리즘

블록체인은 기본적으로 분산 시스템이다. 분산 컴퓨팅으로 이루어진 비행기 예매 시스템에 합의 알고리즘이 없다고 가정해 보자. 손님 A와 손님 B가 같은 자리a를 동시에 예매 하였을 때 합의 알고리즘이 없다면 들어온 시스템에 따라 자리 a를 예매한 사람이 달라진다. 이러한 시스템적인 오류를 방지하고 무결성 보장을 위하여 합의 알고리즘이 생겨났다.

블록체인에서는 각 노드에서 만든 블록의 트랜잭션을 검증하고, 네트워크 전체에서 공유하는 블록체인에 반영하기 위하여 합의 알고리즘을 사용한다. 블록체인에서 사용되고 있는 대표적인 합의 알고리즘에는 다음과 같은 것들이 있다[8].

[표 2] 블록체인 합의 알고리즘 종류

합의 알고리즘	주요 내용
PoW (Proof of Work)	- 비트코인을 시작으로 많은 블록체인 기반 기술이 채택하고 있는 합의 알고리즘 - 거래 승인 과정에서 많은 컴퓨터 파워를 필요로 하는 어려운 작업을 하는 노드를 신뢰할 수 있다고 판단함
PoS (Proof of Stake)	- 이더리움이 채택한 합의 알고리즘 - 사용자의 소유 지분이 블록 생성의 우선권을 가짐 - 기본적인 구조는 PoW와 다르지 않지만 화폐량에 따라 해시 계산의 난이도가 낮아지기 때문에 PoW와 비교하여 자원 소비가 작아지는 장점이 있음
DPoS (Delegated Proof of Stake)	- 위임된 지분 증명 - 투표에 의해 선출된 대표자들의 신뢰를 바탕으로 블록을 생성하기 때문에 합의에 걸리는 시간과 비용이 적게 소요되고 단위 시간동안 생성되는 블록의 개수도 PoW와 PoS에 비해 상대적으로 많음[9]
PoI (Proof of Importance)	- NEM과 같은 가상화폐에서 사용하는 새로운 해시 알고리즘 - 네트워크의 참여도를 통해 평가등급을 결정, 많은 양의 코인을 통해 거래를 하면 더 많은 보상을 가짐
PBFT (Practical Byzantine Fault Tolerance)	- PoW나 PoS와 마찬가지로 Byzantine Fault[1] 모델이지만 PoW와 PoS의 단점인 결과의 불확실성과 성능 문제를 해결 - Hyperledger Fabric과 Eris 등 컨소시엄형에서 이용하고 있는 블록체인 기반 기술에 많이 채택

1) 비잔틴 장군 문제(Byzantine General Problem) : 분산 컴퓨팅 환경에서 악의적인 노드가 분산 시스템에 참여한 상황을 모델링한 문제. 비잔틴 장군 문제를 해결한 시스템은 악의적인 노드가 분산 시스템에 참여한 상황에서도 전체 시스템은 신뢰도 있는 서비스를 제공할 수 있다는 것을 보장한다.

블록체인의 가장 기본적인 합의 알고리즘인 PoW(Proof of Work)는 거래승인 과정에 많은 컴퓨팅 파워가 필요한 어려운 작업(반복 연산 문제 풀기 등)을 포함시키고[8], 이 과정을 통해 가장 많은 구성원들이 가지고 있는 블록체인을 진짜로 인식해 다른 기록은 폐기하는 것이다. 결국 블록체인의 조작을 위해서는 전체 참여노드의 과반수보다 많은 컴퓨팅 파워를 보유해야 하기 때문에 거의 불가능한 일이라 할 수 있다. 그러나 이러한 방식은 전력 소모가 많고 특정 세력이 네트워크의 51%를 장악하면 검증 결과를 왜곡할 수 있다는 문제가 존재한다. PoW는 데이터 무결성은 보장하지만 채굴풀의 집중화와 독점화, 과도한 에너지 소비와 같은 단점이 있다.

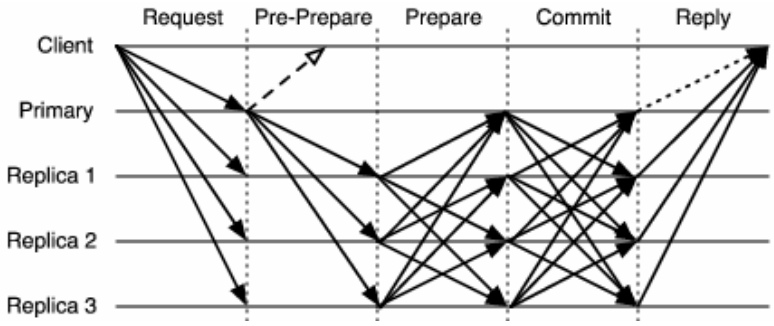
이러한 Pow의 단점을 보완하고자 나온 PoS(Proof of Stake) 방식은 채굴 대신 시스템에서 사용자의 소유 지분이 블록 생성권 지분율이 되며 블록의 생성 주기가 매우 짧아 질 수 있다는 장점이 있으나 전체 네트워크의 노드 상태를 알아야한다는 점과 빈익빈 부익부 현상이 나타날 수 있다는 단점이 있어 연구가 진행되고 있는 상황이다.

DPoS(Delegated Proof of Stake)는 위임된 지분 증명 방식이다. PoS와 비슷하지만 PoS는 일정 지분을 가진 모든 노드에게 블록 생성 권한을 주는 반면, DPoS는 네트워크를 구성하는 모든 노드들의 투표 결과에 의해 선출된 대표자들의 신뢰를 바탕으로 블록을 생성한다[8]. 투표에 의해 선출된 대표자들의 신뢰를 바탕으로 블록을 생성하기 때문에 합의에 걸리는 시간과 비용이 적게 소요되고, 단위 시간동안 PoW와 PoS에 비해 많은 블록을 생성할 수 있다. 대표자들은 매 차수마다 임의로 배정되는 순서에 따라 블록을 만들어 블록체인에 추가할 수 있는 권한을 가진다[9]. 또한,

대표자들의 투표로 악의적인 사용자라고 지목된 노드는 블록체인 네트워크에서 추방시킬 수 있으나, 블록 내의 발신자, 수신자, 잔고 등은 바꿀 수 없다[9].

PoI(Proof of Importance)는 디지털통화인 NEM에서 처음 제안 되었으며 네트워크 참여도로 평가등급이 결정된다. PoI는 PoS와 유사하지만 계정의 잔액규모에만 의존하지 않는다는 점이 다르다고 할 수 있으며 PoS에서 제기되었던 빈익빈 부익부 현상을 막고자 계정의 잔액규모가 아니라 많은 양의 코인을 빈번하게 거래할수록 더 많은 보상을 갖게 된다[2].

PBFT(Practical Byzantine Fault Tolerance)는 PoW나 PoS와 마찬가지로 Byzantine Fault 모델이지만 PoW와 PoS의 단점인 파이널리티의 불확실성과 성능 문제를 해결한 것이다. Hyperledger Fabric과 Eris 등 컨소시엄형에서 이용하고 있는 블록체인 기반 기술에 많이 채택되고 있다. 다음은 PBFT 알고리즘의 동작 방식을 나타낸 그림이다.



(그림 4) PBFT 알고리즘 동작방식[10]

PBFT는 네트워크의 모든 참여자를 미리 알고 있어야 한다. 참가자 중 1명이 프라이머리(Primary, 리더)가 되며, 이 노드는 클라이언트의 요청 순서를 정렬하고, 요청에 대한 결과를 기입하며 다른 노드들에게 뿌려주는

역할을 한다. 프라이머리는 자신을 포함한 모든 참가자에게 요청을 보낸다. 그 요청에 대한 결과를 집계한 뒤 다수의 값을 사용해 블록을 확정한다. 부정한 노드 수를 f개라고 하면 노드 수는 3f+1개여야 하며, 확정을 위해서는 f+1개 이상의 노드가 필요하다. PoW/PoS는 남은 1개에서도 동작을 계속하지만 PBFT는 필요 수를 충족하지 못하면 정지한다[10].

2) 블록체인의 종류

블록체인은 노드의 참여방식, 노드의 식별 가능성 등의 기준을 통해 퍼블릭(public) 블록체인, 프라이빗(private) 블록체인, 컨소시엄(consortium) 블록체인으로 유형을 분류할 수 있다. 대표적인 퍼블릭 블록체인은 비트코인, 이더리움 등이 있고 컨소시엄 블록체인과 프라이빗 블록체인은 노드를 식별할 수 있다는 점에서 금융권, 사내 블록체인으로 활용한다[7]. 각각의 특징을 정리하면 다음의 표와 같다.

[표 3] 블록체인의 종류[7],[14]

구분	퍼블릭(Public)	프라이빗(Private)	컨소시엄(Consortium)
관리주체	모든 거래 참여자	한 중앙기관이 모든 권한 보유	컨소시엄에 소속된 참여자
거버넌스	한 번 정해진 법칙을 바꾸기 매우 어려움	중앙기관의 의사결정에 따라 비교적 쉽게 법칙을 바꿀 수 있음	컨소시엄 참여자들의 합의에 따라 상대적으로 용이하게 법칙을 바꿀 수 있음
거래속도	네트워크 확장이 어렵고 거래 속도가 느림	네트워크 확장이 매우 쉽고 거래 속도가 빠름	네트워크 확장이 쉽고 거래 속도가 빠름
데이터 접근	누구나 접근 가능	허가받은 사용자만 접근가능	허가받은 사용자만 접근가능

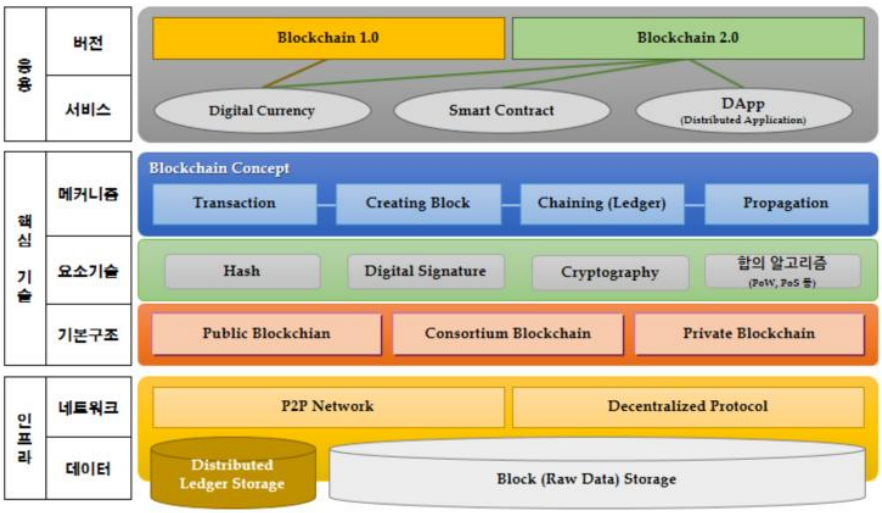
식별성	익명성	식별 가능	식별 가능
거래증명	검증 알고리즘에 따라 거래 증명자가 결정되며 거래 증명자가 누구인지 사전에 알 수 없음	중앙기관에 의하여 거래증명이 이루어짐	거래 증명자의 인증을 거쳐 알려진 상태이며 사전에 합의된 규칙에 따라 거래검증 및 블록생성이 이루어짐
활용사례	Bitcoin, Ethereum 등	나스닥 링크(Linq) 등	R3CEV, Tendermint, CASPER 등

3) 블록체인 2.0

블록체인은 공인된 제3자 없이도 거래 기록의 무결성 및 신뢰성을 확보하기 위해 해시(Hash)[2], 전자서명(Digital Signature)[3], 암호화Cryptography) 등의 보안 기술을 활용한 분산형 네트워크 인프라를 기반으로 다양한 응용서비스를 구현할 수 있는 구조를 가지고 있다.

비트코인의 핵심기술로써 디지털통화(Digital Currency)의 발행·유통·거래가 주 기능이었던 기존의 블록체인 1.0은 기존 비트코인의 한계를 극복하고 다양한 영역으로의 확장을 목표로 하는 블록체인 2.0으로 진화 · 발전해나가고 있다[2].

2) 임의의 길이의 입력 메세지를 고정된 길이의 출력 값으로 압축시키는 기술로 데이터의 무결성 검증 및 메시지 인증에 사용된다.
3) 전자 서명은 작성자로 기재된 자가 그 전자문서를 작성하였다는 사실과 작성내용이 송·수신과정에서 위변조 되지 않았다는 사실을 증명하는 기술이다.

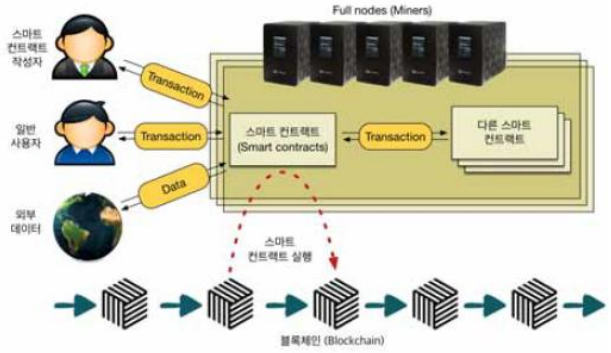


(그림 5) 블록체인의 요소[2]

블록체인 2.0의 대표적인 기술로는 이더리움(Ethereum)이 있으며, 디지털통화의 기능과 더불어 비트코인의 거래 스크립트를 다양한 형태로 프로그램 가능하게 만든 스마트 컨트랙트(Smart Contract)를 구현한다. 이더리움은 블록체인 기반 위에서 부동산 계약, 온라인 투표 등 다양한 분산 어플리케이션을 개발하고 구동할 수 있는 플랫폼으로 확장되었다. 여기서 이야기하고 있는 블록체인 플랫폼이란 블록체인 서비스를 개발, 테스트할 수 있도록 블록체인 시스템의 구성요소(분산 네트워크, 통신 프로토콜 등) 및 필요기능(거래정보 검증, 합의, 노드관리 기능 등)을 제공하는 환경을 말한다. 블록체인 서비스 개발 시 플랫폼을 활용함으로써 개발 편의성과 서비스 간 상호 호환성, 안정성을 확보할 수 있다[8].

2. 스마트 컨트랙트

초기 블록체인은 암호화화폐를 저장하는 기술로 주목을 받았지만 블록체인을 플랫폼으로서 활용하기 위한 기술로 주목을 받은 것은 블록체인의 스마트 컨트랙트이다. 스마트 계약은 Nick Szabo에 의해 소개된 개념으로 신뢰할 수 있는 컴퓨터 인터넷 환경에서 “고도로 발달된” 계약을 준수하는 프로토콜로 정의할 수 있다[4]. Nick Szabo는 가장 단순한 스마트 컨트랙트의 형태를 자판기에 비유하였다. 조건에 따라 동작하는 스마트 컨트랙트는 자판기가 주어진 금액과 선택이 있으면 조건에 맞는 제품을 제공하는 것과 유사하다고 설명한 것이다. 기술적으로 정확하게 표현하자면 스마트 컨트랙트는 블록체인에서 동작하는 프로그램이고, 블록체인에서 동작하기 때문에 실행의 신뢰성이 보장이 되는 방식이다[15].



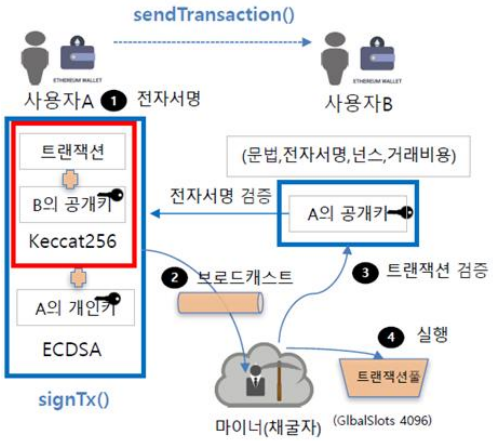
(그림 6) 스마트 컨트랙트와 블록체인[15]

비트코인은 Script 함수를 사용하여 스마트 컨트랙트 코드를 작성할 수 있다. 하지만 함수가 많지 않아 정교한 계약을 수행하기 힘들다는 특징을 가지고 있다. 또한 Script 언어는 대부분의 프로그래밍 언어에서 제공하는 기능을 가지고 있기는 하지만, 무한루프의 위험성 때문에 반복 기능은

제외되어 있어, 튜링 완전성을 보장하고 있지 않다. 이러한 개념을 기반으로 더 완전한 기능을 제공하기 위하여 Vitalik Buterin은 이더리움에서 튜링완전성이 보장된 코드 개발을 통해 더 고도화된 형태의 스마트 컨트랙트를 개발할 수 있도록 하였다. 기존의 비트코인이 분산 환경에서의 안전한 디지털 화폐의 사용을 위한 신뢰성에 초점을 맞추었다면 이더리움은 스마트 컨트랙트와 같은 기능을 모두 내포할 수 있는 프로그래밍 능력에 초점을 맞추어 개발되었다[15].

1) 스마트 컨트랙트 구현 기술 및 이더리움

스마트 컨트랙트는 특정 조건을 실행 가능한 코드로 구현한 일종의 계약으로, 이더리움에서는 트랜잭션을 통해서 블록체인에 배포한다[14]. 또한 이더리움(Ethereum)은 블록체인을 기반으로 한 암호화폐 시스템의 한 종류이기도 하며, 스마트 컨트랙트를 효율적으로 배포, 실행시킬 수 있는 환경을 구축하고 있다. 사용자 A가 사용자 B에게 송금하는 과정을 통해 이더리움에서 블록이 생성되는 과정을 살펴보면 다음과 같다.



(그림 7) 이더리움 블록 생성 과정[16]

① A는 트랜잭션 내역과 B의 공개키를 가져와서 암호해싱을 한다 그리고 자신(A)의 개인키를 사용해서 전자서명(Sign, ECDSA)을 한다.

② 서명된 트랜잭션을 현재 연결되어 있는 전체 노드에 브로드캐스팅 한다.

③ 마이너는 A의 공개키로 개인키를 해제하여 전자서명 검증 등 트랜즉션의 유효성을 검증하고 이상이 없을 시 트랜잭션 풀에 이를 등록한다.

④ 이후 마이너는 트랜잭션풀에서 가장 비싼 수행대가의 트랜잭션을 꺼내서 EVM을 생성하여 실행하고 블록 행성 후 마이닝 작업을 하여 블록체인에 추가한다.

이더리움에는 비밀키에 의해 통제되는 외부 소유 계정(EOA, Externally Owned Account)과 코드에 의해 통제되는 컨트랙트 계정(Contract Account)이 존재하며, 사용자는 외부 소유 계정을 통해 트랜잭션을 생성하여 스마트 컨트랙트를 배포하거나, 스마트 컨트랙트에 포함된 코드를 실행할 수 있다[13]. 각각 계정의 특징은 다음과 같다.

- 외부 소유 계정(EOA, Externally Owned Account)

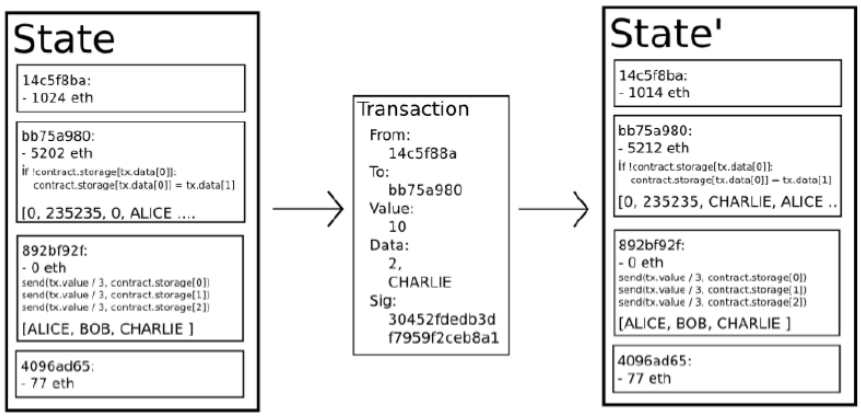
사용자가 갖는 계정. 고유 주소가 있으며, 연결된 잔액과 비밀키가 있다.

- 컨트랙트 계정(CA, Contract Account)

계약(contract)과 연결된 계정이다. EOA와 마찬가지로 주소가 있고 연결된 잔액이 있다. EOA에서 거래를 거쳐 만들어지며, EOA가 발신하는 거래가 트리거가 되어 계약 코드가 실행된다. CA에서 다른 CA를

생성하거나 코드를 실행할 수도 있다. EOA와는 달리 비밀키가 없다.

스마트 컨트랙트는 고유 주소를 가지고 있다고 이야기 하는데, 여기에서 이야기하는 주소는 CA이며, 해당 주소로 메시지를 전송하면 컨트랙트 코드가 실행된다. 별도의 주소로써 존재하기 때문에 블록체인 시스템 내에서 독립되어 있는 개체로 동작할 수 있는 장점을 가지며, 코드를 실행함으로써 이더리움의 상태(State)를 변경하거나 다른 스마트 컨트랙트로 메시지를 전송할 수 있다.



(그림 8) 이더리움 상태 변환 함수 [17]

이더리움 컨트랙트를 구성하는 코드는 “이더리움 버추얼 머신 코드” 또는 “EVM 코드”로 불리는 로우-레벨, 스택 기반의 바이트코드 언어로 작성된다. 이 코드는 연속된 바이트로 구성되어 있고, 각각의 바이트는 연산(operation)을 나타낸다[17]. 보통, 코드 실행은 0부터 시작하는 현재 프로그램 카운터를 하나씩 증가시키면서 반복적으로 연산을 수행하도록 구성된 무한 루프이고, 코드의 마지막에 도달하거나 오류, STOP, RETURN 명령을 만나면 실행을 멈추게 된다[17]. 코드는 또한 블록 헤더 데이터뿐만

아니라 특정 값이나, 발송자 및 수신되는 메시지의 데이터에 접근할 수 있고, 결과값으로 데이터의 바이트 배열을 반환할 수도 있다[13].

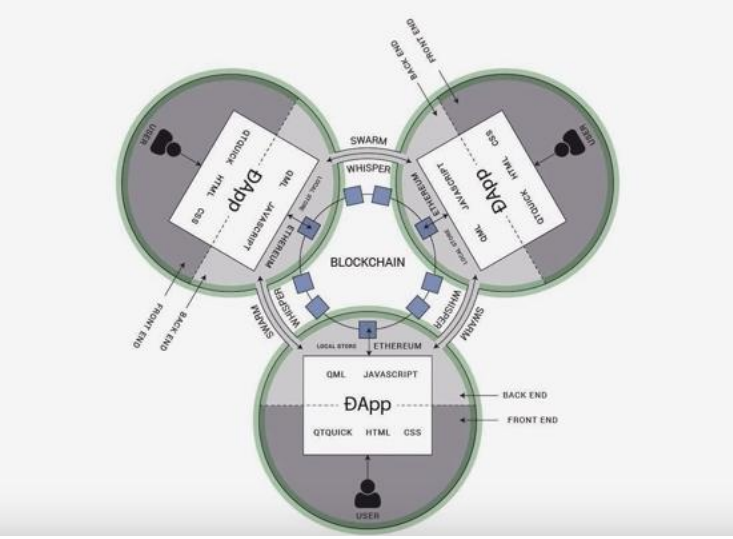
2) 분산 어플리케이션(Distributed Application, DApp)

DApp(Distributed Application)은 분산 어플리케이션은 오픈소스로 정의되어 있는 자율적으로 작동하는 응용 프로그램이며, 탈중앙화된 애플리케이션이라고도 정의된다. 대부분의 DApp은 플랫폼에 기반하여 만들어지며, 어떤 플랫폼을 기반으로 하고 있는가에 따라 이더리움 DApp, 퀀텀 Dapp, 네오 Dapp 등으로 불리고 있다. 본 연구에서는 이더리움을 기반으로 설계 및 구현하였으므로, 이더리움 App을 기반으로 알아보았다.

이더리움은 블록체인을 사용해 참여자들끼리 공유된 합의를 통해서 다양한 분산 어플리케이션을 가능하게 하는 플랫폼이다. 분산 어플리케이션은 데이터를 블록체인에 저장하기 때문에 데이터를 보호할 수 있고 국경 간 서비스에 용이하다. 어플리케이션 내의 변화는 참여자들의 합의를 통해 어플리케이션 내의 규칙을 지정하고 변경되기 때문에 민주적인 모델을 만들 수 있어 투명한 서비스를 제공할 수 있는 장점이 있다.

또한 중앙 서버가 없기 때문에 서버 운영비용이나 보안 비용이 절감되고 DDoS 공격에 대한 근본적인 방어가 가능하다. 기존의 웹 어플리케이션과 비교했을 때도 분산 어플리케이션은 HTML, Javascript를 이용하여 비교적 개발하기 쉬운 구조를 가지고 있다[2]. 최근, 이더리움에서는 Web 3.0 기반 기술의 에코시스템에 포함되기 위해 브라우저 내장 지갑인 Mist, P2P 메시지 프로토콜인 Whisper, 웹 컨텐츠 호스팅을 위한 P2P 데이터

스토리지인 Swarm을 지원하고 있다[19].



(그림 9) DApp 구조도[18]

3. 개인정보보호

기술의 발전으로 대용량의 정보의 분석이 가능해 지고 있다. 그리고 그 정보가 직접적으로 수익과 연관성을 갖게 되면서 특히 개인정보의 활용과 보호에 대한 조화가 점점 더 중요해 지고 있다. 블록체인 기술은 금융 분야에서 우선적으로 활용이 시도되었으며, 최근에는 소유 증명, 인증, 전자 기록 등의 분야에서 신뢰도를 확보할 수 있는 기술로써 잠재력이 매우 높은 기술로 평가 받고 있다. 그러나 블록체인 네트워크에 참여하고 있는 노드들이 거래내역을 검증하는 과정에서 거래내역이 공개가 되는 등 프라이버시 문제가 매우 중요한 과제로 부상하고 있다. 그리하여 블록체인 기반 개인정보보호 이슈 분석에 앞서 개인정보보호에 대한 이론적 정의와 동향에 대해 정리하였다.

1) 개인정보보호 컴플라이언스

국내·외를 막론하고 비즈니스를 위한 기업들은 정보보호뿐만 아니라 개인정보보호 관련 법률의 컴플라이언스 활동을 적극적으로 추진하고 있다. 컴플라이언스란 기업이 비즈니스 연속성과 경영 투명성을 확보하기 위해 관련 법률, 규정, 규칙 등 다양한 외부 규제와 표준에 대한 준수 여부를 확인하고 발견된 문제점들을 지속적으로 개선시켜 나가는 일련의 활동을 의미한다[20].

국내 개인정보보호법에서는 개인정보에 대해 “살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게

결합하여 알아볼 수 있는 것을 포함한다)"라고 정의하고 있다. 또한 개인정보 "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말하며, "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다. 따라서 정보통신망에서 각 노드에 공개되고 분산된 데이터베이스 형태로 운용되는 블록체인 기술을 통하여 분산원장으로 개인정보를 보유 및 활용하고 있는 경우 개인정보처리자에 해당됨에 따라, 개인정보보호법에 관련된 내용을 준수할 수 밖에 없다. 따라서 평문으로 저장된 개인정보를 안전하게 "처리"해야 하며 특히 정보주체의 요구가 있거나 보유기간이 끝난 개인정보에 대해서는 파기의 의무가 있다. 또한 블록체인에서는 신뢰성 확보를 위해 분장을 서로 공유하기 때문에 블록체인의 분산된 노드는 위탁자의 역할도 수행한다고 봐야 하겠다.

2) Privacy by Design

"Privacy by Design"은 1990년대 후반, 캐나다 온타리오주의 정보프라이버시 위원회(Information & Privacy Commissioner)의 Ann Cavoukian 박사에 의해 소개 된 개념이다[21]. Ann cavoukian 박사는 온라인 서비스를 포함하는 IT 기술의 발전에 따라, 정보 통신 분야에 있어 "Privacy by Design"의 개념과 이에 관한 7가지 원칙을 제시하였는데, 서비스 기획 단계에서부터 폐기 단계까지의 전체 생애주기에 걸쳐 프라이버시 보호 및 기술 조치를 포함시켜야 한다는 개념이다.

“Privacy by Design”은 모든 정보기술 및 그 시스템의 설계, 초기 상품 개발이나 서비스 기획 단계에서부터 프라이버시의 보호 및 강화를 위한 조치를 확립하는 포괄적인 절차를 의미한다고 볼 수 있으며, Ann cavoukian 박사가 제안한 7가지 원칙은 다음과 같다.

① 사후 대응이 아니라 사전 대비. 문제점을 고치는 것이 아니라 “예방”(Proactive not Reactive; Preventative not Remedial)
② 프라이버시 보호를 기본 설정값(Defaults)으로(Privacy as the Default Setting)
③ 기획 단계서부터 프라이버시 고려(Privacy Embedded into Design)
④ 포괄적 기능성 보장 - Zero Sum이 아니라 Positive Sum을 추구(Full Functionality – Positive-Sum, not Zero-Sum)
⑤ 전체 수명주기의 보호(End-to-End Security – Full Lifecycle Protection)
⑥ 가시성과 투명성의 확보(Visibility and Transparency – Keep it Open)
⑦ 개인의 프라이버시 존중 -사용자 중심의 설계와 운영(Respect for User Privacy – Keep it User-Centric)

“Privacy by Design”은 개인정보보호 분야의 일반법인 개인정보보호법이나 정보통신서비스 제공자등이 이용자의 개인정보를 취급함에 있어 준수해야 할 내용을 담고 있는 정보통신망법상의 일반원칙으로 자리 잡고 있다.

제 3 장 선행 연구

1. 블록체인 기반 개인정보보호 문제점

1) 개인정보보호 컴플라이언스 문제

블록체인 기술 기반에서 개인정보보호 컴플라이언스 준수와 관련하여 가장 기본적인 것은 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)이다. 블록체인 기술을 통하여 분산원장으로 개인정보를 보유 및 활용하고 있는 경우 개인정보보호법에 따라 각 노드들은 모두 개인정보처리자에 해당되므로 개인정보보호법에 관련된 내용을 준수할 수밖에 없다. 또한 정보통신망법에서는 “정보통신망”이란 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말하므로, 블록체인 네트워크 역시 이에 해당된다.

블록체인에 저장된 정보는 기본적으로 네트워크에 참여하고 있는 참여자들에게 공개되므로 원하지 않게 블록체인에 등재된 기밀데이터 및 개인정보가 공개될 수 있는 위험이 있다. 블록체인 네트워크에서 발생할 수 있는 정보 생명주기별 개인정보보호 이슈를 개인정보보호법과 정보통신망법을 기반으로 다음과 같이 분석 해 볼 수 있다[22].

- 수집

개인정보보호법을 기준으로 개인정보를 수집하는 단계에서는 수집·이용

기준(15조), 최소 수집(16조), 14세 미만 법정 대리인 동의(22조), 민감정보(23조), 고유식별정보(24조), 주민번호(24조의 2)의 처리 제한 사항을 준수하도록 하고 있다. 이 중에서 블록체인 네트워크이기 때문에 문제가 되는 부분은 수집·이용 기준이라 할 수 있겠다. 개인정보를 수집하는 경우 반드시 정보주체의 동의를 받도록 하고 있으며, 동의를 받을 때에는 정보의 수집·이용 목적, 수집 항목, 보유·이용 기간, 동의거부 권리 및 동의거부 시 불이익 내용에 대해 고지하도록 하고 있다.

정보통신망법을 기준으로 개인정보 수집 시에는 수집·이용 동의(제22조), 수집 제한(제23조), 주민번호의 사용 제한(제23조의 2), 만 14세 미만 아동의 법정대리인 동의(제31조)의 사항을 준수하여야 한다. 개인정보를 수집하는 경우 개인정보의 수집·이용 목적, 수집하는 항목, 개인정보 보유·이용 기간 등을 이용자에게 알리고 동의를 받아 최소한의 개인정보만을 수집해야 한다.

수집 단계와 관련한 블록체인 개인정보보호 이슈는 블록체인 기술을 활용하는 경우 데이터가 생성되는 과정에서 정확한 수집·이용의 목적과 보유·이용 기간을 고지하고 동의를 받기는 어렵다는 문제가 있다.

- 이용 및 제공

개인정보보호법에서는 이용 및 제공 단계와 관련하여 목적외 이용·제공 제한(18조), 제3자 제공(17조), 처리 위탁(26조), 영업 양도 양수(27조), 국외 이전(17조) 등의 내용을 검토해야 한다. 개인정보보호법에 따르면 개인정보처리자는 정보주체의 동의를 받은 경우나 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우에 개인정보를 제공받는자, 이용 목적,

제공하는 항목 및 보유 기간 등의 정보를 알린 후에 동의를 받고 제공하도록 하고 있다.

정보통신망법에서는 개인정보 이용 단계에서는 이용 제한(제24조), 제공 동의(제24조의 2), 처리위탁(제25조), 영업 양수 등에 따른 개인정보 이전(제26조) 등의 조항을 준수하여야 한다. 이용자에게 수집 시 동의 받은 목적과 다른 목적으로 이용할 수 없으며, 수집한 개인정보를 제3자에게 제공 혹은 업무 위탁 시 해당 사실을 이용자에게 알리고 동의를 받아야 한다.

그러나 거래정보가 담긴 블록을 생성하는 과정에서 함께 저장될 수 있는 개인정보가 포함된 채로, 거래 타당성 검증을 위해 해당 네트워크 구성원들에게 전달 및 공유될 수 있다. 또한 블록체인 기술을 기반으로 하고 있는 스마트 컨트랙트에서는 익명성을 보장하기 위해 개인정보를 직접적으로 기록하지는 않지만 거래된 내용이 블록체인 노드 참여자들에게 공개되는데, 스마트 컨트랙트 및 거래에 사용된 지갑 주소(wallet address)를 알면 계약 당사자가 아닌 다른 사람들도 조회가 가능하다는 문제점이 있다.

- 관리

개인정보보호법 상의 “개인정보처리시스템”은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 뜻하며, 이는 기존의 중앙집중화 형태의 데이터베이스관리시스템을 기반으로 제정되어 있어 분산화된 블록체인 환경에서 이를 적용하기에는 관리주체가 누구인지 판단하기 어렵다. 이더리움과 같은 퍼블릭 블록체인 기반에서는 모든

노드가 거래와 관련된 정보를 기록·관리하므로 더욱 그러하다. 또한 “개인정보의 안전성 확보조치 기준에서는 개인정보 침해사고 방지를 위하여 취급중인 개인정보가 P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람 권한이 없는 자에게 공개되지 않도록 하고 있다. 이는 블록체인 노드들이 P2P 기반으로 운영되고 블록체인 네트워크에 참여하고 있는 모든 노드들이 거래에 대한 기록을 공유하는 특성을 갖고 있다는 점에서 개인정보보호법에는 명백히 위배되는 사실이다.

정보통신망법에서는 개인정보 관리 시에는 개인정보 보호조치(제28조), 이용자의 권리(제30조)의 조항을 준수하여야 한다. 정보통신서비스 제공자는 개인정보 처리 시 개인정보의 안정성을 확보하기 위해 내부관리계획 수립, 접근 통제장치 설치 등 적절한 기술적·관리적 조치를 취하여야 하는데, 개인정보보호법에서와 마찬가지로 블록체인 네트워크에서는 참여하는 모든 참여자가 개인정보를 관리하기 때문에 이를 모두 준수해야 한다.

- 파기

개인정보보호법에서는 목적 달성이 된 개인정보는 데이터가 복원되지 않도록 초기화 또는 덮어쓰기를 수행하여 파기하도록 하고 있다. 또한 정보통신망법에서도 개인정보 파기와 관련하여 개인정보의 파기(제29조) 조항이 있으며, 정보통신서비스 제공자는 이용 목적을 달성하거나 보유 및 이용 기간이 끝난 경우 해당 개인정보를 복구할 수 없도록 파기하여야 한다고 규정하고 있다.

그러나 블록체인의 구조 상 한번 블록에 기록된 정보에 대한 파기는 사실상 불가능하다. 블록체인에 한번 올라간 데이터는 이론적으로 조작이

불가능하며 저장된 기록이 영구적으로 남을 수 있다는 특징이 있다. 블록체인에서 데이터의 신뢰성은 과거의 내역을 지울 수 없는 비가역성에 근거하고 있으므로 한 번 시도된 거래에 대해서는 삭제를 하는 것이 어렵다. 이러한 특징으로 데이터의 무결성을 보장하는 측면이나, P2P 서비스에서의 신용을 보장할 수 있다는 장점으로 많이 활용되고 있지만, 다른 측면으로는 한 번 올라간 데이터에 대한 변경 및 삭제가 거의 불가능하므로, 개인정보보호 컴플라이언스 관점에서는 파기가 불가능하다는 문제가 존재한다.

2) 기술적 문제

전자 계약 분야에서 스마트 컨트랙트를 이용하는 경우에는, 법적 효력을 갖는 계약이 성사되기 위해 계약 당사자간의 개인을 확인할 수 있는 정보, 즉 개인 인적 정보를 필요로 하며, 이 경우 블록에 개인정보를 저장한다. 그러나 블록체인에 이러한 개인정보가 평문으로 기록이 되면, 블록체인에 저장된 정보는 기본적으로 해당 네트워크에 참여하고 있는 참여자 모두에게 공개되므로 의도하지 않게 블록체인에 등재된 기밀데이터 및 개인정보가 공개될 수 있는 위험이 있다. 블록체인 기술 기반에서 발생할 수 있는 개인정보보호 측면의 이슈는 다음과 같다.

- 거래 내역 검증 및 합의

거래가 완료되면 invoke를 통해 해당 원장은 블록에 저장되며, 블록체인은 각 노드에서 만든 블록의 정당성을 검토하고 네트워크 전체에서 공유하는 블록체인에 반영하기 위해 합의의 과정을 거치게 된다[4]. 합의를 위해 거래내역이 공유되는 과정에서 정보의 기밀성이 보장되지 않을 수

있다. 블록체인에서 보장하는 것은 데이터의 부결성과 가용성이지 기밀성에 대해서는 보장이 되지 않는다. 그러나 블록체인에서는 모든 노드에서 실시간으로 알아야 하는 거래에 필요한 정보들이 관리되는데, 이 정보들 중에는 개인을 식별할 수 있는 개인정보나 자산정보, 결제 정보 등과 같은 민감한 정보들이 포함될 수 있는데 이러한 과정에서 민감정보의 기밀성이 보장되지 않는다는 문제가 있다[23].

또한, 블록체인에 저장된 거래내역의 공개키 주소를 이용하면 과거에 발생한 거래내역을 추적하는 것이 가능하다. 이러한 추적이 가능한 거래내역들을 수집하여 통계적으로 분석하면 특정 공개키 주소에 대한 패턴이 드러나게 되며, 이를 지속적으로 모니터링하면 본인 인증 또는 개인정보를 필요로 하는 행위를 하게 되는데, 이 때부터 노드의 개인정보 확인이 가능해진다. 또한, 여러 블록에서 값을 가져오는 경우 정보의 조합이 가능해지므로 식별성이 발생할 수 있다. 따라서 거래 데이터가 완전한 익명성을 갖는다고 보기 어렵다.

실제로 대표적인 퍼블릭 블록체인 플랫폼인 이더리움에서 생성된 블록체인에 포함된 트랜잭션의 일부를 추출하여, 16진수를 ASCII 문자열로 변환하는 함수를 사용하면 다음의 그림과 같이 평문으로 정보를 확인할 수 있음을 확인했다.

(그림 10) 트랜잭션의 ASCII 문자열 변환 결과

- 참여자 권한 관리

퍼블릭 블록체인에서는 참여자 누구나 네트워크에 공유되고 있는 거래 정보를 확인할 수 있으므로 개인정보 침해가 발생할 수 있게 된다. 프라이빗 블록체인은 권한이 있는 참여자만 거래 내역을 확인할 수 있으나, 네트워크를 운영하고 있는 운영 주체가 권한을 도용당하는 경우 거래 내역을 확인할 수 있게 되어 블록체인 네트워크 전체에 대한 신뢰성이 문제가 될 수 있다. 블록체인은 분산 구조로 인해 참여자 권한 관리 등 거버넌스 통제가 모든 노드들에게 일관성 있게 적용되는 것이 어려운 부분이 존재한다[24]. 그러므로 이로 인한 보안 사고의 발생 가능성을 배제할 수 없다.

- 블록체인 네트워크 관리(Governance) 구조의 문제

블록체인 소프트웨어는 일반적으로 오픈 플랫폼으로서 보안에 다소 취약하기 때문에, 보안 취약점으로 인한 거래 유효성 조작, 참여자 권한 조작, 개인정보 침해 등 다양한 보안 위협에 노출이 가능하며, 분산 구조로 인해 보안 패치가 모든 참여자에게 적용되었음을 보장하기 어려운 부분이 있다. 그러나 모든 블록체인은 버그 생성, 취약점 발생, 업그레이드 등의 이유로 프로토콜을 변경해야 하는 일이 발생한다[24]. 이러한 경우 소프트웨어 개발자들의 주도 하에 업그레이드가 진행되어, 많은 네트워크

참여자들의 동의가 필요하고 실패 시 블록체인이 분리되는 결과를 초래한다[24].

또한, 분산 네트워크 환경에서는 관리주체가 부재하므로, 사고 발생 시 침해사고에 대한 즉각적인 인지가 어렵다. 그러나 정보보호 측면에서, 발생할 수 있는 사고 측면에서 사고를 최소화 하고 빠른 해결이 가능한 탐지(Detection)와 조치(Correction)방안의 마련은 매우 중요한 일이기 때문에 이에 대한 고려가 필수적이다. 또한 분쟁이 발생하였을 경우에는 문제가 발생한 경우 그 모든 책임을 거래 당사자에게만 물을 수는 없으므로, 분쟁이 발생한 경우 중재할 수 있는 역할이 필요하다.

2. 관련 연구 동향

국내 학위논문에 블록체인 기술이 등장한 것은 2016년도부터이다. 그만큼 기술 연구는 초기 단계로 기술 자체에 대한 연구와 활용에 대한 연구가 먼저 이루어지고 있었는데, 블록체인 활용과 관련해서 황경락의 연구[5]를 살펴보면, 비트코인에 적용된 기술을 분석하고 비트코인 기반 기술의 한계점에 대한 개선 방안 연구를 진행하였다. 유헌우의 연구[25]에서는 블록체인 방식을 활용한 전자 투표 시스템을 제안한 것으로 앞선 이 연구들은 블록체인 기술 자체에 대한 연구와, 그 기술의 특징을 이용한 인증 방안에 대한 연구이며 기술 활용 측면의 연구라 볼 수 있겠다. 이루다의 연구[26]에서도 블록체인을 전자투표 시스템에 적용한 사례를 확인할 수 있으며, 양민희의 연구[27]에서는 블록체인을 보험사 건강체 특약 할인에 적용한 사례를 확인할 수 있었다. 또한 블록체인 기술을 정보보호 분야에 적용한 사례들도 있었다. 이상민의 연구[28], 이찬혁의 연구[29]

논문들이 그러하며 최근들어 다양한 분야에서의 블록체인 기술 적용과 함께 블록체인을 활용한 정보보호 적용 방안에 대한 연구는 이루어지고 있었으나, 블록체인 자체의 보안에 대한 연구는 이제 막 시작하는 단계임을 확인할 수 있었다. 앞선 연구들은 모두 블록체인 기술에 대해 알아보고 활용 측면에서 고민해 본 연구들이라 할 수 있다.

블록체인 기술 활용에 대한 연구 이후 블록체인 기술 자체가 가진 문제점을 분석하고 성능을 향상시키려는 시도를 확인할 수 있었다. 이러한 연구는 국내보다는 해외에서 많이 진행되고 있었으며, 그 중 한 분야로 블록체인 자체가 가진 보안 문제에 대한 것이 있었다. Jaume Barcelo의 논문[30]에서는 비트코인 거래 시 주소의 반복적인 재사용으로 인해 발생하는 사용자의 프라이버시 누설(Privacy Leakage)에 대해 지적하고 있다. 비트코인 주소는 익명이고 사용자의 실제 신원 정보와 연결되어 있지 않지만, 실제적으로 여기서의 익명은 프라이버시를 지키기 위한 '매우 얇은 선(very thin line)'에 불과하기 때문에 거래 정보를 누적하여 분석하면 결국 거래에 사용하는 주소와 해당 주소의 소유주를 연결할 수 있을 가능성이 충분히 존재한다는 것이다. 그 이유는 거래 시 사용하는 주소는 특정 소유주와 연결되어 있고 이 주소와 관련된 모든 거래 내역은 결국 이 소유주와 관련된 것이라고 볼 수 있기 때문이다.

블록체인 네트워크의 프라이버시 문제와 관련하여 Ahmed Kosba이 발표한 Hawk 모델[31]에서는 블록체인 기술의 데이터 정확성 또는 가용성에 대해서는 신뢰할 수 있지만 프라이버시에 대해서는 문제가 있다는 것을 지적하며, 블록체인과 스마트 컨트랙트의 표현력과 이들 기술이 가진 힘에도 불구하고 현재의 형태로는 스마트 컨트랙트에서 발생하는 모든

일련의 액션들이 네트워크를 통해 전파되고 블록체인에 기록되어지며 이를 네트워크상의 모든 참여자가 볼 수 있기 때문에 거래 프라이버시(transactional privacy)의 누출이 발생한다고 말하고 있다. Hawk에서는 블록체인을 사용하기는 하지만 거래 당사자들이 자발적으로 정보를 노출하지 않는 한 거래에 참여하지 않는 공공에게는 거래 내역이 공개되지 않는데, 블록체인 상에 정보를 전달할 때 $\varnothing_{priv}$ 구역 내에서 거래되는 화폐의 흐름이나 거래량에 대해서는 암호화하고 zero-knowledge proof를 이용하는 방법으로써 프라이버시를 강화한다.

블록체인 기술이 가진 보안 문제에 대해 국내에서 가장 눈에 띈 연구는 전솔의 연구[32]였다. 이 연구에서는 기존 블록체인에서 나타나는 문제점을 기존 블록체인에서 나타나는 문제점을 무결성, 인증, 기밀성 측면으로 분석하고 해결 방안 제시하고자 하는 부분이 본 연구와의 방향의 출발은 가장 유사한 연구였다. 그러나 해결 방안은 인증과 합의 알고리즘을 강화한 프라이버시 블록체인을 제시한 부분에서 차이가 있었다. 본 연구에서도 일정 해결 방안으로 네트워크 참여 전 인증이 이루어져야 한다는 것에는 동의를 하지만 더 나아가 블록체인 기술 자체가 가지는 기밀성 측면에서 문제를 해결해보고자 했다는 점에서 다르다 할 수 있다. 또한 블록체인 기반 스마트 컨트랙트 역시 블록체인이 가진 기술의 문제점을 가지고 있으며, 그로 인해 프로그램 배포 전 설계의 중요성에 대해 강조하고자 하였다.

블록체인은 높은 신뢰성으로 인해 다양한 산업 분야에서 그 활용에 대한 연구가 활발하게 진행되고 있으며, 그 가능성을 매우 높이 평가하고 있지만 실적용 사례는 아직 드문 것 또한 사실이다. 최근에는, 블록체인 연구가

많이 진행되기 시작하면서 정보보호 및 개인정보보호 관련 이슈가 제기되고 있다. 블록체인을 활용하면 서비스 운영의 신뢰성과 투명성을 강화할 수 있지만, 기밀성에 대한 위협이 존재하며, 한 번 배포된 스마트 컨트랙트로 인해 문제가 발생하여도 돌이키고 복구하기까지 많은 자원과 부담이 필요하다. 그렇기 때문에 스마트 컨트랙트에서는 설계에 대한 부분이 특히 더욱 중요하다고 볼 수 있다.

3. 블록체인 기반 개인정보보호 문제점 도출

블록체인은 보안에 뛰어난 기술이라 평가받고 있다. 그러나 실제 블록체인을 비즈니스에 적용할 때에는 개인정보보호 측면에서 많은 문제가 있음을 확인할 수 있었다. 대표적인 컴플라이언스 관점 이슈는 개인정보 파기의 문제일 것이다. P2P 네트워크에서의 신뢰성 확보를 위한 비가역성은 개인정보보호 측면에서는 한번 저장된 개인정보의 파기가 불가하다는 큰 문제를 갖게 되었다. 파기가 불가능하다는 것은, 블록에 올라간 정보가 아무리 잘못된 정보일지라도 이에 대한 삭제가 불가능하기 때문에 블록에 올라가는 정보에 대한 확인 검증 또한 중요한 문제가 될 수 있다. 그리고 이러한 비가역성은 스마트 컨트랙트라는 프로그램 입장에서도 한 번 배포된 프로그램에 문제가 있는 경우 복구가 어렵다는 것이 문제가 된다. 또한 개인정보보호의 기술적인 측면에서는 투명성 확보를 위한 블록의 공유가 트랜잭션에 포함된 개인정보를 누구나 확인할 수 있다는 문제를 갖게 하였다. 마지막으로 블록체인이 가지는 가장 큰 특징인 탈중앙화는 P2P 거래에서의 신뢰 문제를 해결하였지만 분쟁 발생 시 책임소재가 모호하다는 문제를 배제할 수 없다. 그리하여 본 연구에서는 다양한 개인정보보호 관점의 문제가 있겠지만 위에서 제시한 5가지 문제를 해결하고자 하였다.

제 4 장 신뢰할 수 있는 스마트 컨트랙트 모델

1. TSCM(Trusted Smart Contract Model)

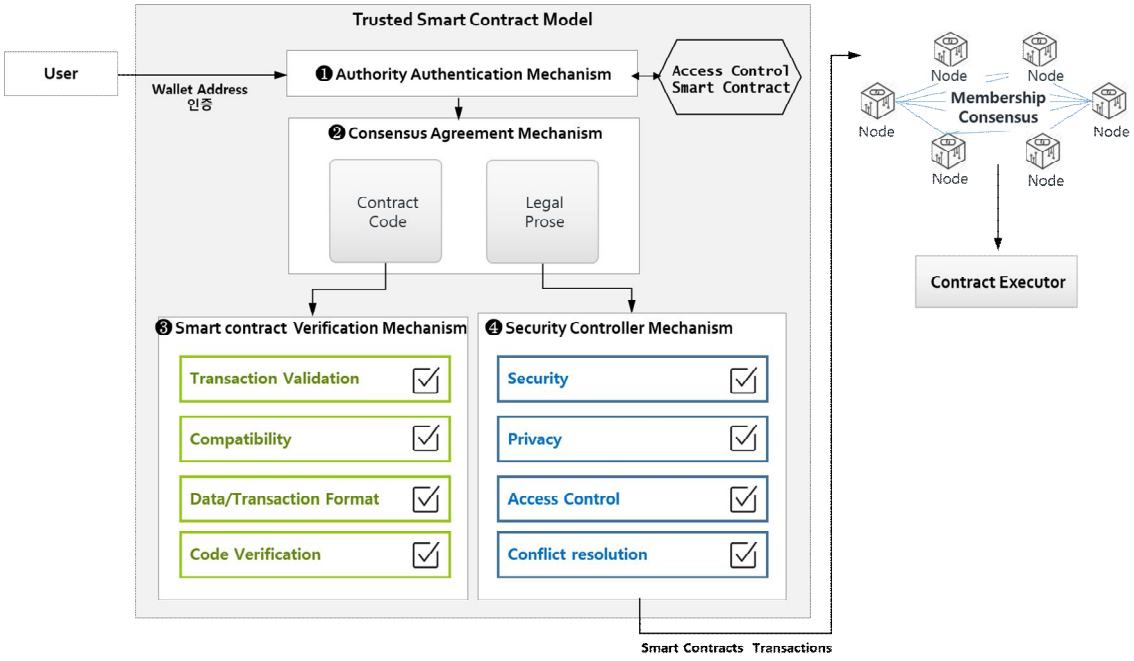
1) 구현 목표

본 연구의 목표는 신뢰할 수 있는 스마트 컨트랙트의 구현이며, 앞에서 언급한 문제점 중에서 본 시스템에서 해결하고자 하는 부분은 크게 다섯 가지이다. 1) 개인정보 및 민감정보가 포함된 계약 전체의 내용은 계약의 당사자만 확인 가능해야 하며, 2) P2P 네트워크를 통해 작성되는 계약의 법적 유효성을 최대한 보장하고자 한다. 3) 블록에 최종 올라가면 수정이 어렵다는 점을 고려하여 계약 내용에 대한 합의가 이루어졌음을 보장할 수 있도록 하고, 4) 개인정보는 본인이 원하지 않거나 보관의 의무가 종료되면 확인 할 수 없도록 논리적 파기의 방안을 적용하고자 한다. 마지막으로 5) 분쟁이 발생하는 경우 중재할 수 있도록 한다.

그리하여 이러한 시스템을 구현하기 위해 스마트 컨트랙트 기능을 갖고 있는 이더리움 플랫폼을 기반으로 구현하고자 한다. 본 연구에서는 참여자들의 형태를 사용자 노드는 자유롭게 네트워크에 참여하게 하되 계약의 법적 검토를 위한 검증 노드를 두고자 한다. 사용자와 검증자 노드를 분리하여 운영한다는 점에서, 완벽한 퍼블릭 블록체인의 형태라 볼 수는 없으나, 한정적으로 탈중앙화를 구현하면서 안정성을 확보할 수 있는 형태의 블록체인을 목표로 한다.

2) 제안 모델

앞에서 제시한 블록체인 기반 스마트 컨트랙트 실행시 발생할 수 있는 정보보호 이슈를 해결하고자 본 논문에서는 TSCM(Trust Smart Contract Model)을 제시하고자 하며, 제안하는 모델은 다음과 같다.

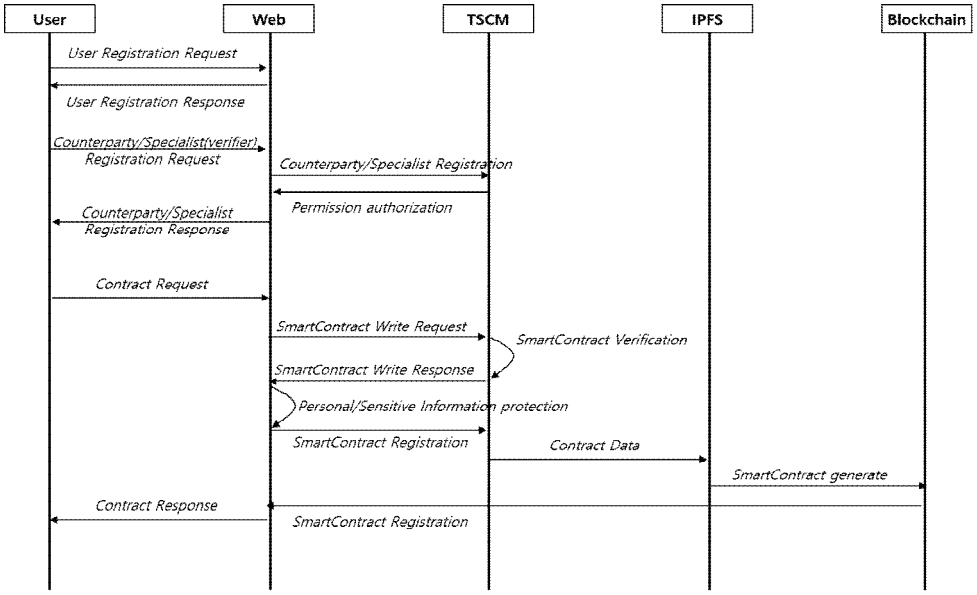


(그림 11) Trust Smart Contract Model(TSCM)

제안된 시스템은 퍼블릭 블록체인을 기반으로 한다. 그렇기 때문에 기본적으로 사용자는 누구나 자유롭게 참여가 가능하되 검증자 노드들은 허가를 통하여 네트워크에 참여시키고자 하므로 반허가 블록체인의 형태라 할 수 있다. 그러므로 사용자가 누구인지에 대한 식별이 아닌 일반 사용자인지 혹은 검증자 노드인지에 대한 식별을 위한 권한 인증 메커니즘(AAM : Authority Authentication Mechanism), 계약 내용에 대한

협상을 지원하고 디지털 계약서가 법적 지위를 보장받게 하기 위한 합의 메커니즘(CAM : Consensus Agreement Mechanism), 스마트 컨트랙트 코드에 대한 유효성을 보장하고 트랜잭션을 검증하는 스마트 컨트랙트 코드 검증 메커니즘(SVM : Smart contract Verification Mechanism), 계약 내용에 포함되는 데이터들을 보호하고, 개인 간의 지급/결제 거래에서 이용자를 보호할 수 있도록 하는 기능을 실행하는 정보보호 메커니즘(SCM : Security Controller Mechanism)으로 구성된다.

본 연구에서 제안하는 모델에 대한 시퀀스 다이어그램은 다음과 같다.



(그림 12) 시퀀스 다이어그램으로 표현한 TSCM 프로세스

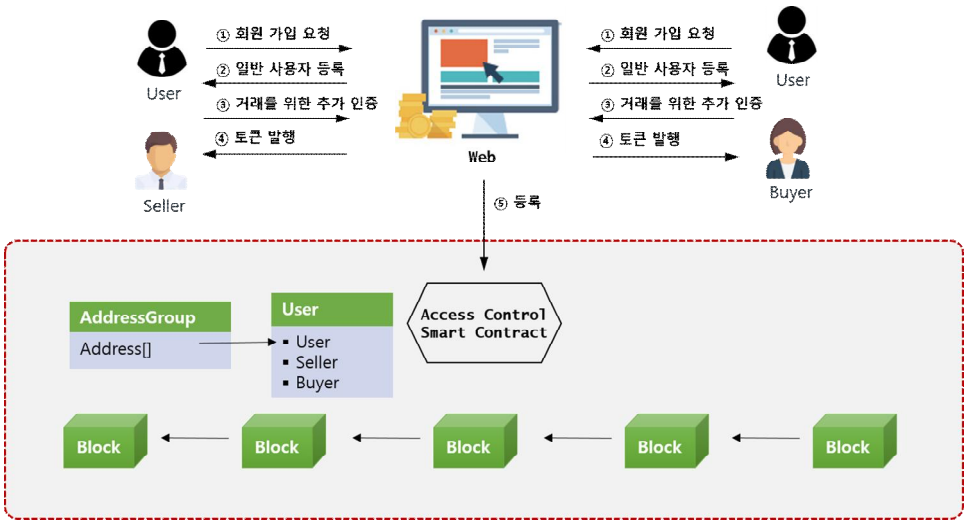
실제 계약에 참여하기 위해서는 AAM(Authority Authentication Mechanism)을 통해 사용자 지갑 주소로 추가 인증을 하도록 하여 각 역할에 맞는 R&R(Role&Responsibility)을 부여 받아 거래에 참여하도록 하였다.

거래 당사자들은 계약의 내용을 작성 후에 CAM(Consensus Agreement Mechanism)을 통해 계약 조건의 내용을 확인하고 상호간의 협의를 하며 법적 효력 여부를 검증한다. 그 다음 SVM(Smart contract Verification Mechanism)을 통해 작성된 Smart Contract의 상호 호환성과 트랜잭션 및 코드 유효성을 점검하고, 계약에 포함되는 데이터를 parsing 한다. 추출된 데이터는 SCM(Security Controller Mechanism)을 통해 정보보호 및 개인정보보호 메커니즘을 적용하여 식별이 가능한 정보에 대해서는 비식별화를 적용하고, 민감한 정보들에 대해서는 암호화를 적용한다. 모든 절차가 완료된 계약에 대해서는 합의알고리즘을 통해 블록에 저장되고, 스마트 컨트랙트는 해당 계약을 실행함으로써 종료한다.

2. 세부 메커니즘

1) AAM(Authority Authentication Mechanism)

본 설계에서는 거래와 무관한 제3자의 접근을 통제하기 위해 AAM(Authority Authentication Mechanism)에서 검증된 노드만이 블록체인 네트워크에 참여할 수 있게 한다. 일반 사용자는 사용자 지갑 주소 등록만으로 웹에서 정보 검색이 가능하지만, 실제 계약에 참여하기 위해서는 사용자 지갑 주소를 등록하고 추가 본인 인증 후에 토큰을 발급받도록 한다.



(그림 13) Authority Authentication Mechanism

스마트 컨트랙트를 활용한 전자 계약에는 많은 민감한 정보가 포함될 수 있으므로 정확한 역할에 따른 권한 할당이 필요하다. 그러므로 본 논문에서는 역할 기반의 접근 통제를 설계 및 적용하였다. 노드의

지갑주소를 기반으로 일반 사용자와 계약 참여자, 계약에 대한 검증 노드를 구분하였으며 자세한 내용은 다음과 같다.

[표 4] 서비스 참여 노드 역할 정의 예

분류	세부 사항
일반 사용자 (user)	- 블록체인 네트워크를 이용하는 일반 유저 - 네트워크에 지갑 주소를 등록하고 1차적인 노드 인증만 완료 - Seller가 등록한 내용을 확인할 수 있음
계약 참여자 (Seller)	- 거래에 참여하고 싶은 user에게 추가 인증을 통해 Seller 역할 부여 - 새로운 서비스 및 매물에 대한 등록이 가능 - 거래에 대한 세부 협의 요청 가능 - 문제가 발생하는 경우 Controller 호출 가능
계약 참여자 (Buyer)	- 거래에 참여하고 싶은 user에게 추가 인증을 통해 Buyer 역할 부여 - 매물에 대한 거래 의사 등록 가능 - 거래에 대한 세부 협의 요청 가능 - 문제가 발생하는 경우 Controller 호출 가능
검증 노드 (Specialist)	- 거래를 중재, 감사(Audit)하는 제3자 - 전문가 회원으로 법률 자문, 계약 내용의 검토 등이 필요한 경우 거래에 참여 가능 - 계약의 내용에 대한 검토만 가능하며 직접 수정은 불가 - 분쟁 발생 시 중재의 역할 수행

참여 노드의 지갑주소를 이용해 검증한 후, 참여 역할(User, Seller, Buyer, Specialist)별로 계약에 참여할 수 있도록 한다. 노드를 역할에 할당한 후 사용자가 Contract 정보에 접근할 때 민감한 정보까지 포함되어 있다면, 사용자가 접근가능한지에 대한 검증을 한 후, 접근 여부 및 이용할 수 있는 연산에 대한 알맞은 권한을 부여한다. 여기서 데이터를 이용할 때 사용자가 Seller 혹은 Buyer와 같이 계약 당사자라면, 정보에 접근 및 읽고 쓰기가 가능하다.

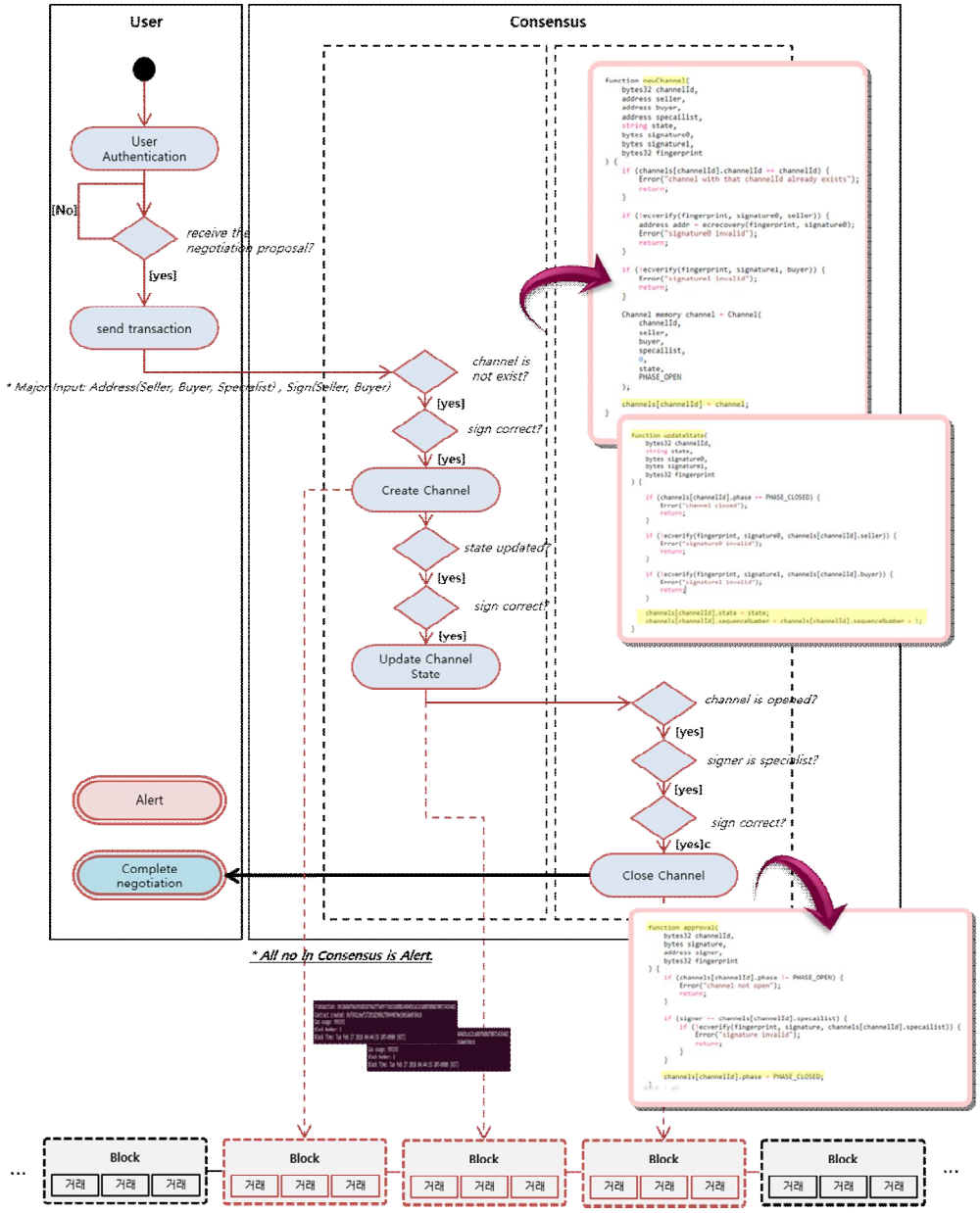
2) CAM(Consensus Agreement Mechanism)

스마트 컨트랙트는 법적인 부분의 내용(Human Readable)과 프로그램을 실행하는 부분(Machine Readable)으로 나눌 수 있다. CAM(Consensus Agreement Mechanism)에서는 계약 생성자가 설정한 조건이 법적 타당성을 갖추는가에 대해서 검증하고, Human Readable 계약서를 완료하는 데 목적이 있다. CAM에서 다루고 있는 합의(Consensus)는 계약 당사자간의 계약 내용에 대한 합의 및 법적인(legal) 합의를 의미한다.

전통적인 계약에는 통상 청약과 승낙에 의해 계약이 체결되고, 체결된 계약의 이행에 있어 당사자는 일정 금원을 지급하고 반대 당사자는 재화 등을 제공하며, 금원과 재화는 특정의 장소로 이전하면서 계약 이행이 종료된다. 스마트 컨트랙트도 디지털로 구현되어 있는 계약이기 때문에 이러한 절차 및 내용이 모두 포함되어야만 법적인 효력을 인정받을 수 있다. 법적인 부분에 대해서는 사용자가 코드를 작성하지 않아도 쉽게 계약을 생성할 수 있도록 변수 형태로 내용을 입력 받아서 작성한다. 예를 들면, 당사자간의 신원 확인 정보, 계약 조건과 내용(금액, 날짜 등)과 같은 부분이 그러하다.

그러나 이러한 계약 내용에 대한 합의의 내용 중에는, 특히 기업의 경우, 사업 기밀의 내용을 포함하는 민감한 정보들이 다수 포함되어 있을 수 있기 때문에 이러한 transaction을 모든 참여자가 있는 메인 채널에서 주고받는 것은 정보보호 측면에서 문제가 있을 수 있다. 그렇기 때문에 이러한 의견 합의 과정을 안전하게 진행하고, 과정 중에 주고받은 transaction 전체를 저장하여 최종 계약이 이루어진 후에 부인방지가 보장될 수 있도록 다음의

(그림15)와 같이 설계 하였다[34].

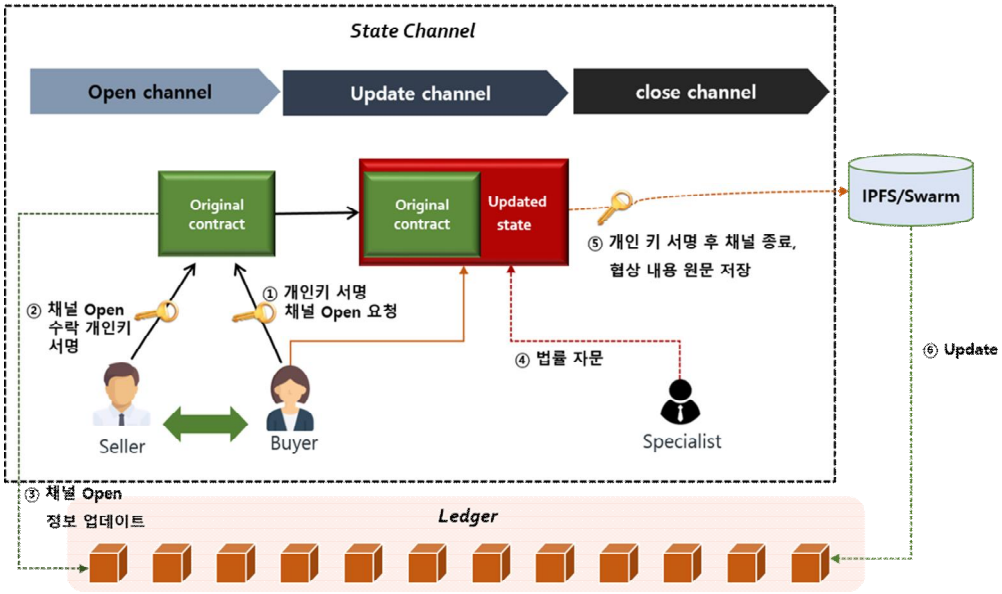


(그림 14) Consensus Agreement Mechanism

CAM에서는 원활한 계약서 작성과 법률적인 부분에 대한 전문가 자문을 위하여 전문가 노드인 Specialist Node를 구성하였다. Specialist는 법적 자문을 할 수 있는 전문가로, 거래 당사자들의 계약 내용 협상에서 문제가 발생하거나, 계약 내용에 대한 법률 자문이 필요한 경우 도움을 줄 수 있게 하였다. Specialist Node는 모든 계약에 참여하게 되는 것은 아니며, 비영리, 친분 등을 기반으로 계약서가 작성되어 Compliance 이슈가 크지 않은 계약에 대해서는 그림에서처럼 생성된 스마트 컨트랙트의 법률 언어(legal prose)에 대해 상호 동의 검증을 하고, 스마트 계약 코드와 연결하여 계약을 실행 하여 코드를 통해 계약의 유효성을 보증해주도록 한다.

전문가의 추가적인 법률 자문이 필요한 경우에는 Specialist를 포함시켜 계약에 대한 협상을 주고받을 수 있게 한다. 이러한 협상은 민감한 내용일 수 있기 때문에, 전체 노드가 참여하고 있는 메인 네트워크에서 일어날 필요는 없다. 그러나 둘 사이의 대화가 오프라인 기반으로 이루어진다면 추후에 문제 발생 시에 이를 뒷받침 해 줄 근거가 없다. 그리하여 본 설계에서는 메인 Channel과는 별개의 State Channel에서 이러한 협상이 이루어 진 후에, 협상 내용 전문은 Hash하여 저장함으로써 무결성을 보장하고자 하였다.

추후 발생할 수 있는 법적 문제에 대한 대비를 위해, 중요한 계약에 대해서는 메인 Channel이 아닌 State Channel을 통해 신뢰할 수 있는 제3자(Specialist)를 거래에 일정부분 참여시켜서, 분쟁 발생 시 해결 할 수 있게 한다.

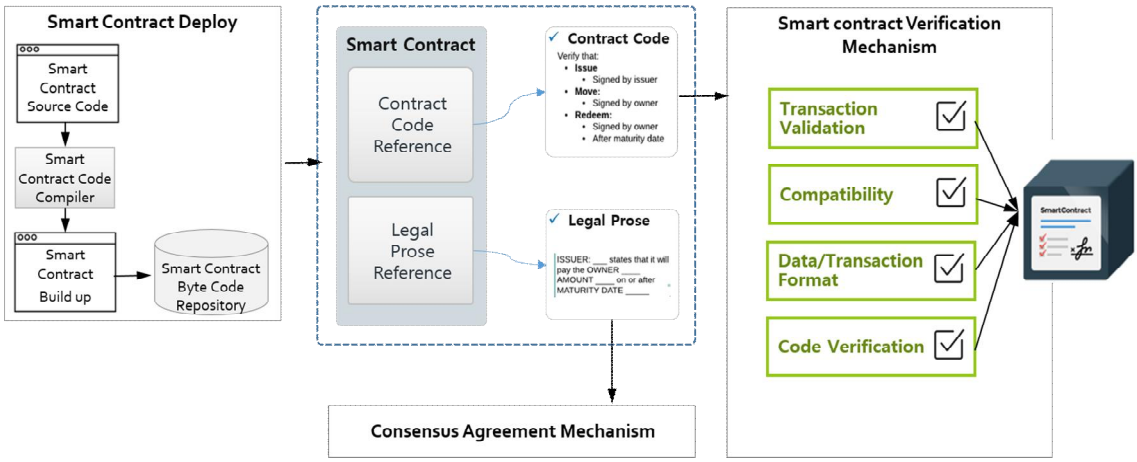


(그림 15) State Channel을 이용한 계약 내용 합의 과정

State Channel을 이용하는 이유는 크게 2가지가 있다. 네트워크 상의 모든 노드들이 그 내용을 알 필요가 없거나 민감정보인 경우, 당사자들과 Specialist Node 만이 State Channel을 통해 내용을 확인할 수 있고, 이야기된 내용은 참가자의 개인키로 서명하기 때문에 데이터의 무결성과 부인방지 기능을 기대할 수 있다. 협상 내용의 전문은 분산데이터 저장소인 IPFS 및 Swarm에 저장된다. 또한 트랜잭션 발생으로 인한 불필요한 수수료를 줄일 수 있다는 장점이 있다.

3) SVM(Smart contract Verification Mechanism)

스마트 컨트랙트 코드 신뢰성을 보장하기 위한 스마트 컨트랙트 코드 생성과 관련한 메커니즘이다. SVM(Smart contract Verification Mechanism)에서는 작성된 스마트 컨트랙트가 오류 없이 다양한 환경에서 운영될 수 있도록 상호 호환성을 체크하고, 실행 코드와 트랜잭션의 유효성, 데이터 포맷을 검증한다.



(그림 16) Smart contract Verification Mechanism

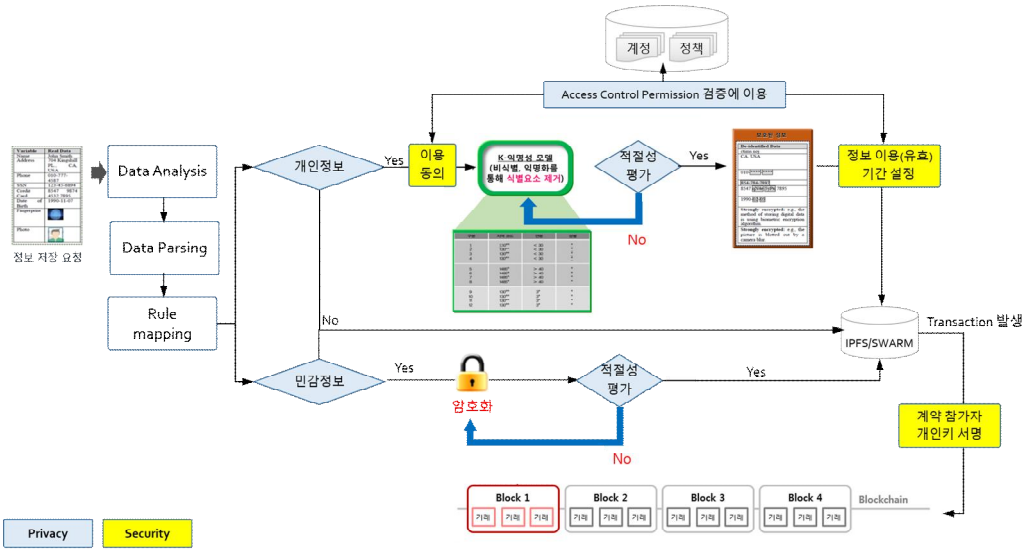
이러한 절차가 필요한 이유는 실제 계약에 참여하는 당사자가 프로그래밍이 불가능 하더라도 쉽게 이용할 수 있도록 하기 위함이다. 본 시스템에서는 표준 계약서를 Smart Contract 형태로 구현해 놓고, 계약서 형태로 작성된 HTML 페이지에서 입력받은 데이터를 변수로 받아 전자 계약의 형태로 작성될 수 있게 하였다.

각각의 계약서는 Smart Contract로 매번 배포 되지 않고, 입력받은

데이터들은 무결성 확보를 위해 블록체인에 저장한다. 각각의 계약마다 Smart Contract를 직접 배포한다는 것은, 사용자가 어느 정도 프로그래밍이 가능하다는 것을 전제로 한다. 또한 실제 서비스에서 스마트 컨트랙트를 매번 배포 하는 것은 비용적인 측면이나 관리의 측면에서 비효율적이다. 그러므로 각각의 계약은 사전에 배포된 스마트 컨트랙트를 불러와 그 안에 저장된다. SVM에서는 이 입력값으로 들어온 데이터들로 인해 Smart Contract 코드가 실행 시 코드상의 오류가 일어나지 않는지 등에 대한 데이터 포맷과 트랜잭션 및 코드 유효성 등을 검증하는 것이다.

4) SCM(Security Controller Mechanism)

스마트 컨트랙트에 포함될 내용에 대한 작성이 완료되면 SCM(Security Controller Mechanism)을 통해 계약에 포함되는 개인정보와 민감정보에 등에 대한 데이터 보호 방안, 데이터 접근에 대한 접근 제어 기능을 실행하고자 하며, 메커니즘에 대한 프로세스는 다음과 같다.



(그림 17) Security 및 Privacy 기능 적용 프로세스

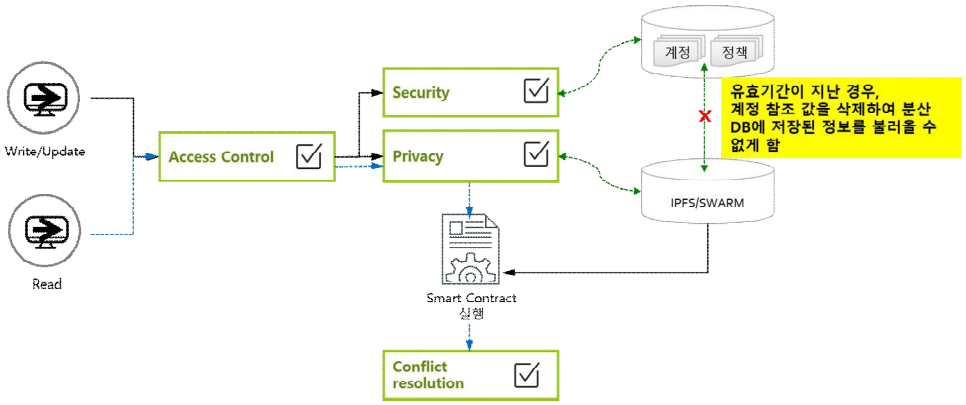
우선, 데이터 보호 방안을 위해 개인정보와 민감정보 등에 대한 보호조치를 적용하고자 한다. 이를 위해서는 거래 내용에 대한 거래당사자(Buyer, Selelr) 및 Specialist의 의견 합의가 이루어진 후에 최종 트랜잭션이 발생되기 전, 개인정보나 민감정보에 해당하는 정보를 추출한다.

트랜잭션이 발생 된다는 것은 합의 과정을 거친 후에 블록이 생성됨을 의미하므로 트랜잭션이 발생 한 이후에는 이러한 조치를 취하기 어렵다.

그러므로 트랜잭션이 발생하기 전에 개인정보나 민감정보에 대한 보호 조치를 적용해야 한다. 해당 식별 정보에 대해서는 비식별화를, 민감한 정보거나 개인정보에 대해서는 암호화를 적용하며, 이를 통해 블록체인 네트워크에 참여중인 다른 노드들이 계약서를 공유하게 되어도 중요한 정보는 알 수 없다. 또한 개인정보가 포함되어 있는 경우 정보주체에게 이러한 사실을 고지하고, 정보 이용에 대한 추가적인 동의를 받는다.

암호화 및 비식별화 된 정보에 대해서는 정보 적절성을 평가한 뒤 정보 이용에 대한 유효기간을 설정한다. 정보주체가 만약 유효기간을 별도로 설정하지 않으면, 법령에 의한 정보 보유기간을 정보 유효기간으로 설정한다. 개인정보의 보유 기간에 대한 유효기간을 설정하는 이유는 블록체인에서의 개인정보 파기 문제 해결을 위함이며, 블록체인 네트워크의 대표적인 개인정보보호 컴플라이언스 문제인 파기에 대한 부분을 일정 부분 해결하기 위하여 본 연구에서는 2가지의 논리적 파기 방법을 사용한다.

유효기간이 지난 이후에는 2가지 방법을 적용하였는데, 첫째, 이더리움에서 제공하는 delete 함수를 사용함으로써, 더 이상 해당 블록에 접근 할 수 없게 함으로써, 논리적인 파기가 이루어지도록 하였다. 둘째, 해당 계약서가 참조하고 있는 데이터에 대한 블록을 참조하는 값을 삭제함으로써, Smart Contract를 호출할 때 개인정보 값은 불러오지 못하고 계약 내용만 확인할 수 있게 하였다.



(그림 18) 개인정보 유효기간 설정을 통한 논리적 파기 적용 방안

작성된 계약서는 계약 참가자들의 최종 확인 후 각각의 개인키로 서명한 후 블록에 저장하기 위한 트랜잭션을 발생하여, 합의 절차를 거친 후 최종 블록에 업데이트 된다. 이렇게 저장된 계약서의 내용을 불러올 때에는 요청한 주체와 그 주체의 권한을 확인하고, 개인정보의 유효기간을 확인한 후 모든 조건이 충족되면 평문 형태로 다시 확인할 수 있게 한다.

제 5 장 사례를 통한 모델 검증

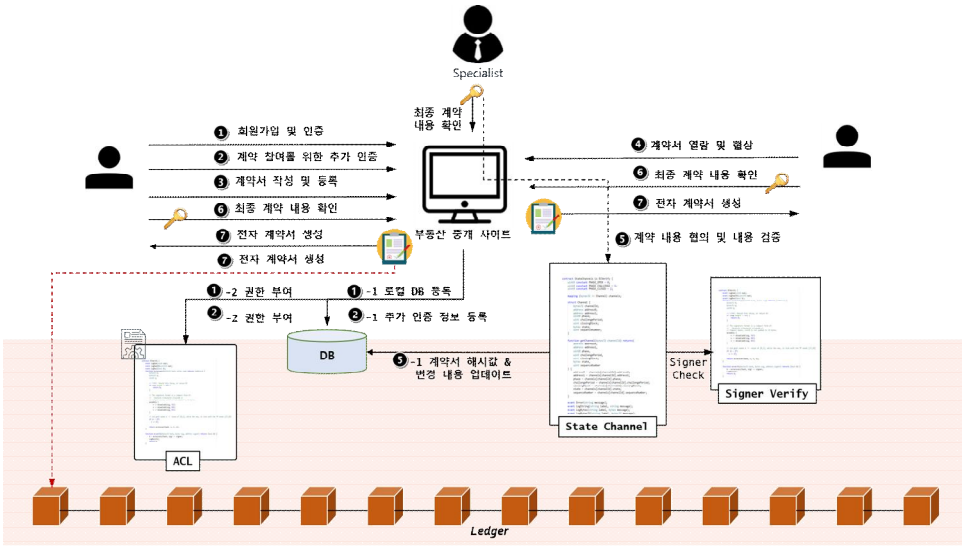
1. 적용 사례

본 연구에서 제안한 모델의 검증 방법으로는 사례연구를 진행하여 효과에 대해 분석하였다. 방법론 검증 사례로는 개인간 부동산 매매 거래 계약을 선정하였다. 부동산 거래는 실생활에서 비교적 많이 이루어지는 거래이며, 부동산 거래 및 소유자에 대한 정보는 변조가 돼서는 안되고 거래 기록이 남아 있어야만 하는 등 신뢰성이 중요하다. 최근 웹이나 앱을 통해 부동산 매물 정보를 검색하고, 거래하는 빈도가 급증하고 있는 반면, 실제 P2P 거래로 진행되기까지는 아직 보안에 대한 우려가 있는 것 또한 사실이다.

부동산 거래는 비교적 가격 규모가 큰 거래로써, High Risk라는 인식이 높다. 부동산을 거래할 때 그 부동산이 실제 그 사람 소유인지 확인하고, 판매자와 구매자의 신분을 확인해야 하며, 소유주가 변경됐다는 증거를 문서로 남기게 된다. 이러한 과정에서 보증과 신뢰를 필요로 하기 때문에 중개인, 보증기관 등 제3자가 개입하게 되므로 비용과 시간이 소요될 수 밖에 없다. 또한 부동산 계약과 관련해서는 세금을 줄이기 위한 다운 계약서, 업 계약서, 위장 계약서 등의 허위 계약서 작성 사례 등이 계속적인 문제가 되고 있다. 본 논문에서 제안한 모델의 적용은 이러한 문제들을 해결할 수 있는 좋은 대안이 될 수 있을 것이라 생각되어 P2P 부동산 거래 계약을 연구 대상으로 선정하게 되었다.

1) 적용 시나리오

부동산 거래 계약 사례를 적용하고자 하는 시나리오는 다음과 같다.



(그림 19) 부동산 사례 적용을 위한 시나리오

<사용자 등록 및 권한 인증>

① 부동산 중개 사이트 웹 회원으로 가입한다. → 일반 회원, *user*

② 매도자 혹은 매수자, 전문회원이 되기 위한 추가 인증 절차를 거친다. → 거래 참여 회원, *Buyer, Seller, Specialist*

<거래 시작 및 계약서 작성>

③ 매도자의 매물, 계약 내용 등록

④ 매수자 내용 확인, 협상 시도

⑤ 매도자, 매수자 간 계약 내용 협의 및 전문회원(공인 중개사, 법무사 등)을 통한 내용 검증

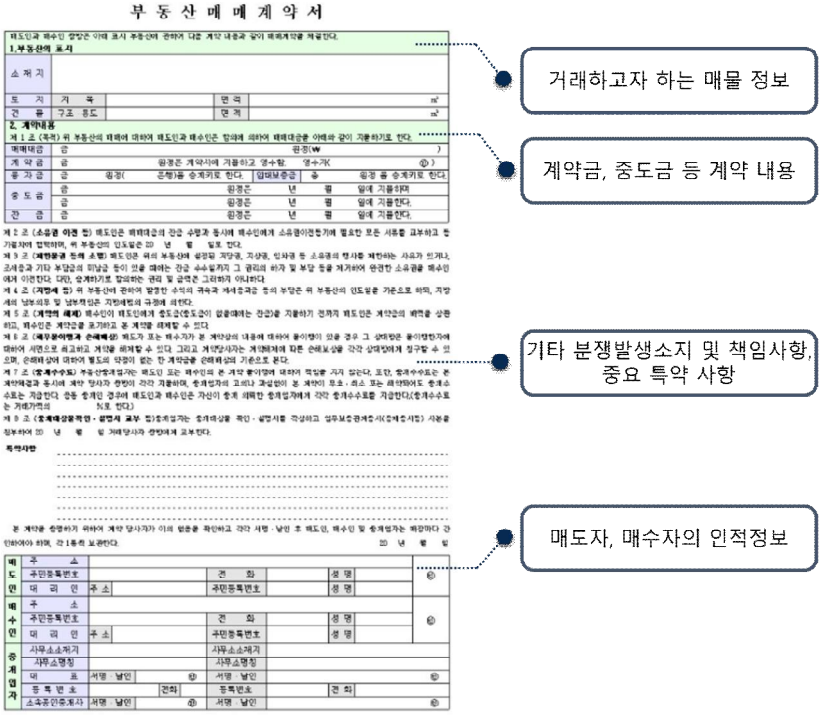
⑥ 최종 계약 내용에 대한 계약 당사자의 개인키 서명

⑦ 전자 계약서 생성(Human Readable)

⑧ 블록 생성을 위한 transaction 발생 및 블록 생성 완료(Machine Readable)

2) 계약서 작성을 위한 요구사항

국내 부동산 거래는 한국공인중개사협회에서 제공하고 있는 표준 계약서 양식을 사용하고 있으며, 부동산 거래 계약에 있어 필수적인 정보는 다음과 같다.



(그림 20) 표준 부동산매매계약서

이를 기반으로 계약 체결을 위해 본 시스템에서 필요한 정보는 다음과 같다.

[표 5] 부동산 계약 체결을 위해 필요한 최소 정보

분류	수집 정보	내용	개인정보
매물 정보	소재지	매물 소재지	
	토지	매물 토지 지목	

분류	수집 정보	내용	개인정보
		매물 토지 면적	
	건물	매물 건물 구조 및 용도	
		매물 건물 면적	
계약 내용	계약일	계약 체결일	
	매매대금	거래 전체 금액 정보	
	계약금	계약 체결을 위한 계약금	
		계약금 입금 기한	
	융자금	융자금액	
	중도금	중도금 금액 정보	
		중도금 입금 기한	
	잔금	잔금 금액 정보	
		잔금 입금 기한	
매도인 (Seller)	이름	매도인의 이름	○
	주소	매도인의 주민등록 상 주소	○
	주민등록번호	매도인의 신원확인을 위한 주민등록번호	○
	전화	매도인의 연락가능한 번호	○
	서명	개인 서명 데이터	○
매수인 (Buyer)	이름	매수인의 이름	○
	주소	매수인의 주민등록 상 주소	○
	주민등록번호	매수인의 신원확인을 위한 주민등록번호	○
	전화	매수인의 연락가능한 번호	○
	서명	전자지갑의 개인키 값	○
특약 사항	특약사항	기타 특약 사항 내용	

또한, 스마트 컨트랙트이기 때문에 시스템에서 추가적으로 수집하는 정보는 다음과 같다.

[표 6] 추가 수집 정보

분류	수집 정보	설명	개인 정보
매도자/ 매수자	이더리움 지갑 주소	스마트 컨트랙트를 위한 지갑 주소	○
	서명	이더리움 지갑 개인키 값	○

2. 실험환경 구성

본 논문에서는 위에서 제안한 부동산 계약 사례를 통한 프로타이핑 구현으로 연구의 타당성을 검증하고자 한다. 다음의 표는 각각 웹과 블록체인의 테스트 환경 구성을 표로 정리한 것이다.

[표 7] 웹 테스트 환경

구분	내용
OS	Ubuntu 16.04
Web Server	Apache tomcat 8.0.42
DB	IPFS
Language	Node.js

[표 8] 블록체인 테스트 환경

구분	내용
Platform	Ethereum 1.6.5
Solidity	0.4.0
Wallet	Metamask
Etheruem browser	Remix

각 노드는 Ubuntu 16.04 환경에서 구현 하였으며 이더리움 클라이언트인 Geth (Go-Ethereum) 1.8.5버전과 테스트를 조금 더 편리하게 도와주는 testRPC을 통해 테스트 및 개발하였다. Solidity를 이용하여 스마트 컨트랙트를 생성하고 지갑의 UI는 Javascript, HTML을 통해 사용자가 쉽게 사용할 수 있도록 계약서 포맷을 개발하였다. Solidity는 스마트

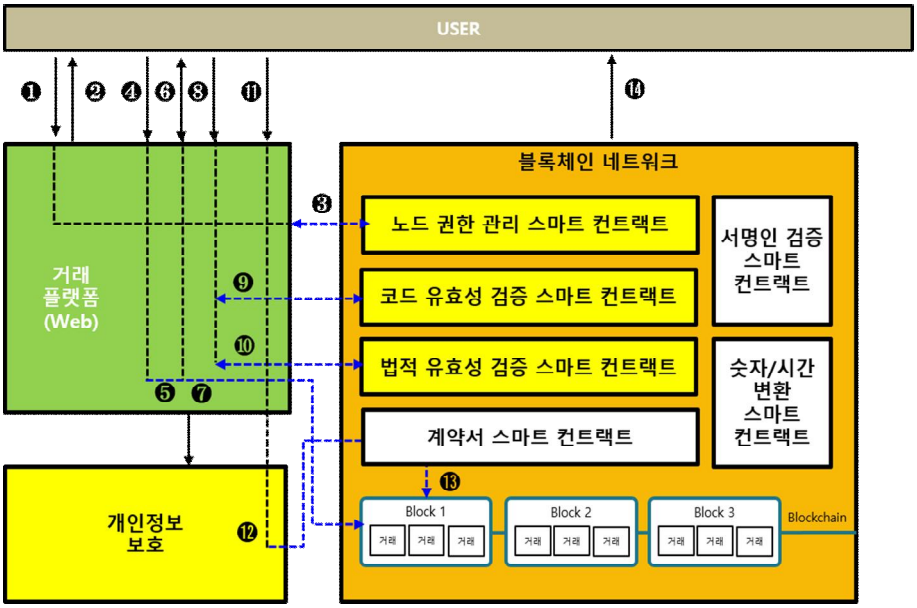
컨트랙트를 작성하는 데 쓰이는 프로그래밍 언어로, EVM을 통해 실행할 수 있다. Solidity는 high-level 언어로 JavaScript와 유사한 형태를 가지고 있다. Solidity로 작성된 스마트 컨트랙트는 입력되는 메시지의 값, 발신자 및 데이터, 블록 헤더의 데이터와 같은 메시지의 특정 속성에 접근할 수 있고, 상속, 라이브러리 및 다양한 기능을 지원하기 때문에 다양한 계약을 코드로 개발하는 것이 가능하다.

회원 가입이 이루어지고, 매물 정보를 등록하는 일은 부동산 중개 웹 사이트를 통해 이루어진다. 계약서에 작성되는 데이터들은 블록체인에 저장되기 때문에, 실제 계약서의 작성이 시작되는 순간부터 블록체인 네트워크를 이용하게 되며, 노드에 대한 접근 제어가 반드시 필요하므로 본 논문에서는 컨소시업 블록체인 구조를 채택했다. 원활한 계약 체결과 컨소시엄 망 구축을 위해 이더리움의 dev 옵션을 이용하여 테스트 네트워크에서 프로토타이핑을 수행하였다.

테스트 환경에서는 계약을 체결하는 계약 당사자인 A, B 노드(Counterparty)와 계약서의 법적 내용을 검토하고 문재 발생 시 중재자 역할을 할 수 있는 전문회원 노드(Specialist) 3개의 노드를 구성하여 진행하였다.

3. 모델을 적용한 P2P 부동산 계약 시스템 설계

제안 모델을 적용한 플랫폼의 모습은 다음의 그림과 같이 작동하며, 제안 시스템에서는 아래와 같이 전체 시스템 중 노란색으로 표시한 부분이 모델에서 제안한 내용의 구현이다.



(그림 21) 제안 모델을 적용한 플랫폼 설계

① 회원 가입 및 사용자 등록

② 실제 거래 참여를 위한 본인 인증

③ 블록체인 네트워크에 정보 등록 및 권한 부여

④ 웹에 거래 내용 등록

⑤ 거래 내용 등록 트랜잭션 블록에 저장

⑥ 거래 당사자 간 계약 내용 합의

⑦ 협상 내용 트랜잭션 블록에 저장

⑧ 계약서 작성 완료

⑨ 스마트 컨트랙트 실행을 위한 코드 유효성 검증

⑩ 법적 문제 최소화를 위한 전문인 합의

⑪ 계약서 초안 검토 및 승인

⑫ 계약서 내용 중 개인정보 추출/암호화/유효기간 설정

⑬ 계약 내용 트랜잭션 블록에 저장

⑭ 스마트 컨트랙트 실행

그리고 주요 기능은 다음의 표와 같이 스마트 컨트랙트로 구현되어 있다.

[표 9] 제안 시스템의 Smart Contract 구성 및 기능

Smart Contract	기능
PropertyContract.sol	계약서 등록 및 업데이트와 같은 부동산 계약이 이루어지는 로직을 처리하는 스마트 컨트랙트
ACL.sol	참여자 권한 관리에 대한 스마트 컨트랙트
ECVeify.sol	서명인을 검증하는 스마트 컨트랙트
DateTime.sol	블록체인은 기본적으로 블록의 숫자로 시간을 처리하기 때문에 블록의 숫자를 시간으로 바꾸어주는 스마트 컨트랙트
StateChannels.sol	계약에 대한 추가 협상이나, specialist의 법률 자문이 필요한 경우 State Channel을 이용하는 스마트 컨트랙트
CodeVerify.sol	계약서 스마트 컨트랙트의 코드 유효성을 검증하는 스마트 컨트랙트

4. 제안 모델의 구현

다음은 제안 모델을 적용한 P2P 부동산 계약 시스템을 구현한 모습이다. 본 연구에서는 거래와 무관한 제3자의 접근을 통제하고 관리의 효율성을 위하여 등록된 사용자만이 블록체인 네트워크에 참여할 수 있게 하였다. 웹에서만 활동하는 일반 사용자는 ID 등록만으로 사용이 가능하지만, 실제 계약에 참여하기 위해서는 이더리움 지갑 주소와 함께 추가 본인 인증을 받고 계약에 참여하도록 한다.

전자 계약에는 많은 민감한 정보가 포함될 수 있으므로 정확한 Role에 따른 접근제어가 필요하다. 본 연구에서는 이러한 사용자의 역할에 따른 권한을 하나의 Smart Contract로 구현하였다. 이렇게 하면, 예외 없이 설정한 규칙대로 적용이 가능하며, 상태의 변경이 필요한 경우 Contract 상태 Update를 통해 관리가 가능하다.

[표 10] 참여 역할별 권한

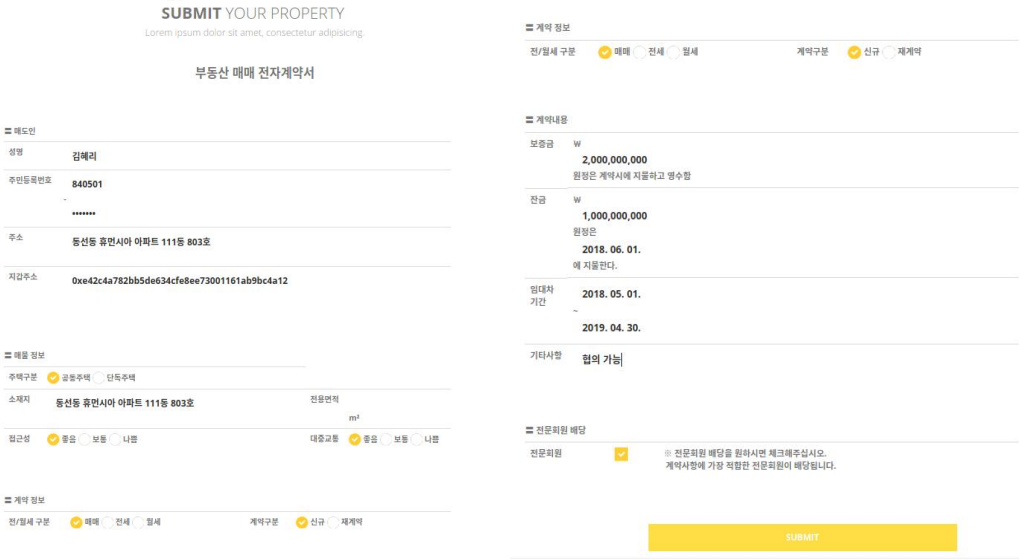
분류	권한
user	- 웹 회원 가입이 완료된 이용자 - Buyer가 등록한 매물 정보 Read 가능
Counterparty	- 실제 거래에 참여하는 Buyer와 Seller - 본인이 작성한 계약서를 Read, Write, Update가 가능
Specialist	- 전문가 회원 - 법률 자문, 계약 내용의 검토 등이 필요한 경우 거래에 참여 가능 - 계약의 내용에 대한 Read만 가능하며, 내용 수정은 State Channel을 이용하여 가능

노드를 검증한 후, 참여 역할(User, Counterparty, Specialist)별로 권한을 부여하여, 계약에 참여할 수 있도록 하였다. Access Control에 대한 Rule은

하나의 Smart Contract로 관리하며 참여자의 지갑 주소로 권한을 부여하고, Type은 블록체인 네트워크 내 노드의 등급을 분류하여 볼 수 있는 데이터를 접근제어를 위해 분류한다.

노드를 역할에 할당한 후 사용자가 Contract 정보에 접근할 때 민감한 정보까지 포함되어 있다면, 사용자가 접근가능한지에 대한 검증을 한 후, 접근 여부 및 이용할 수 있는 연산에 대한 알맞은 권한을 부여한다. 여기서 데이터를 이용할 때 사용자가 Seller 혹은 Buyer와 같이 계약 당사자라면, 정보에 접근 및 읽고 쓰기가 가능하다.

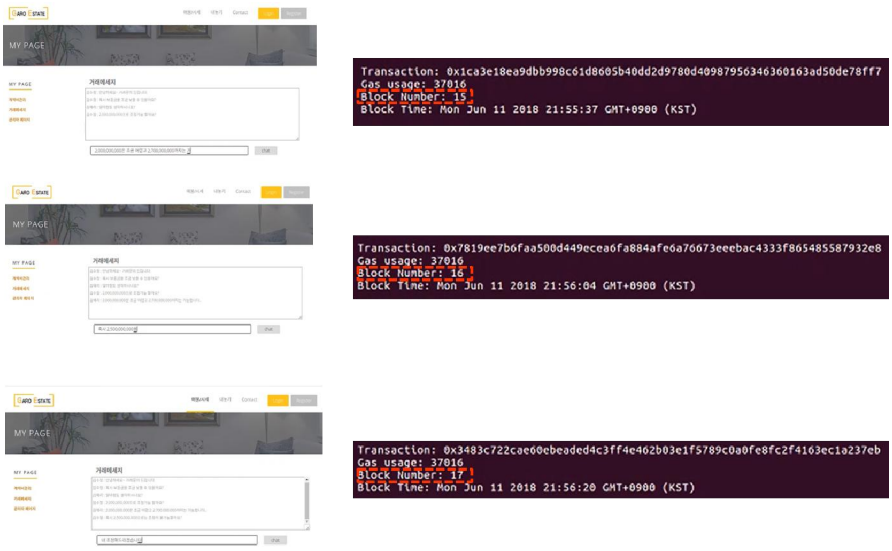
인증을 마친 사용자는 거래하고자 하는 매물을 검색하고 계약을 시도한다.



(그림 22) 계약서 작성 화면

계약서 작성이 시작되면 실제 계약의 내용에 대한 협상과 그에 대한 합의, 그리고 법적인 부분에서는 문제가 없는지에 대한 검증이 이루어진다.

비영리나 친분에 의한 간단한 계약서의 경우 법적 검토가 필요하지 않지만, 여기에서는 법률 자문이 필요하다는 가정 하에, Specialist를 State Channel에 포함시켜 계약에 대한 협상을 주고받을 수 있게 한다.



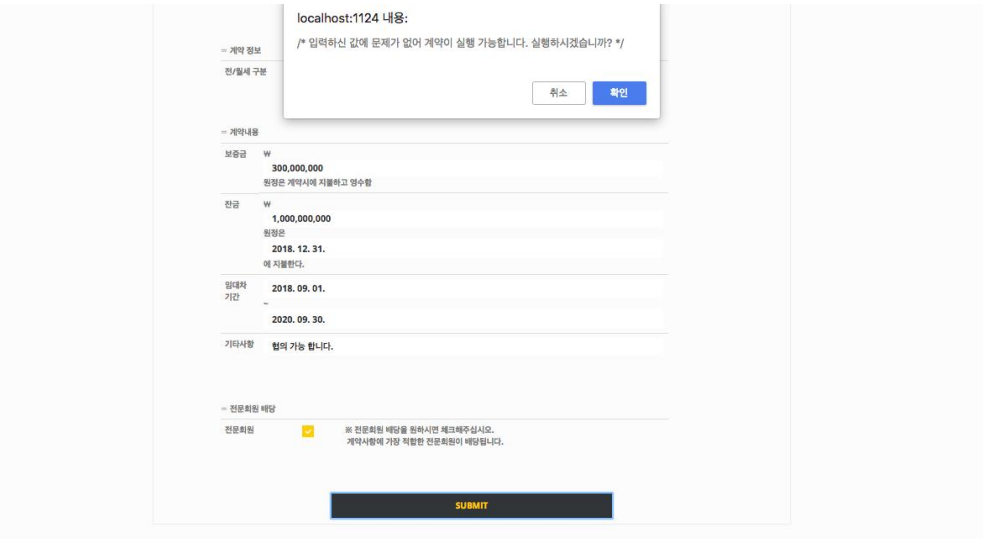
(그림 23) State Channel을 통한 협상 내용의 블록 저장

우선, 매도인이 처음 매물을 올려놓았던 정보대로 계약서 초안을 작성한다. 매수인은 내용을 확인 후에 계약 조건에 대해 추가적인 협상이 필요한 경우, 매도인에게 State Channel에 참가할 것을 요청한다.

계약 당사자들의 계약 내용 입력이 끝나면, 프로그램으로써의 스마트 컨트랙트의 프로그램으로서의 오류가 없이 실행됨을 보장하기 위해 다음과 같이 트랜잭션 유효성 체크가 먼저 이루어진다. 다음으로는 이용하고 있는 코드의 표준화 준수여부와 입력받은 데이터와 트랜잭션 포맷을 체크한다.

(그림 24) Transaction 유효성 검증

스마트 컨트랙트 코드에 이상이 없다면 다음 그림과 같이 스마트 컨트랙트의 생성 여부에 대해 한 번 더 확인을 거친 후에 프로그램을 생성하도록 한다.



(그림 25) 코드 유효성 검증 후 컨트랙트 생성 알림

다음으로는 협상이 완료되어 작성된 계약서 내용에 포함되는 개인정보 및 민감정보에 대한 정보보호 조치가 이루어진다. 현재 버전의 Smart Contract

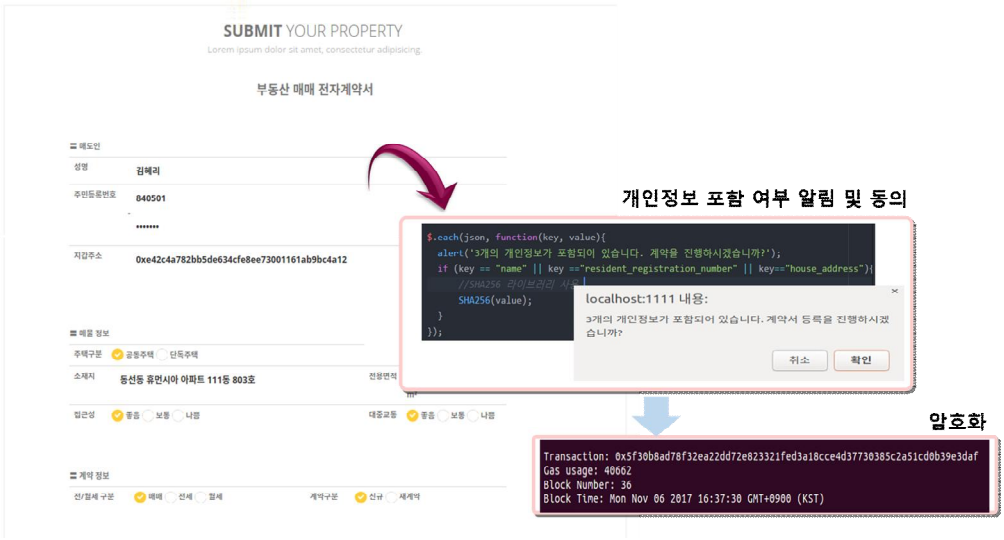
상에는 16개의 변수만이 실제로 입력될 수 있다. 그러므로 꼭 필요한 다음의 변수만을 Contract에 올리고, State Channel에서 오고간 대화들이나 법적 검토 사항, 계약을 위해 필요한 추가 다른 정보들은 모두 Hash 하여 트랜잭션에 포함시킨다. 실제 스마트 컨트랙트에 평문 형태로 저장되는 정보는 다음과 같다.

[표 11] Smart Contract 상에 실제 올라가는 정보

구분	변수명	개인정보
소재지	Location	
매매대금	SalesPrice	
계약금	ContractPrice	
계약날짜	ContractDate	
융자금	Loan	
잔금	Balance	
잔금 날짜	BalanceDate	
계약 당사자 이름	CounterpartyName	○
계약 당사자 지갑 주소	CounterpartyWalletAddress	○
계약 당사자 개인키 서명값	Identification	○

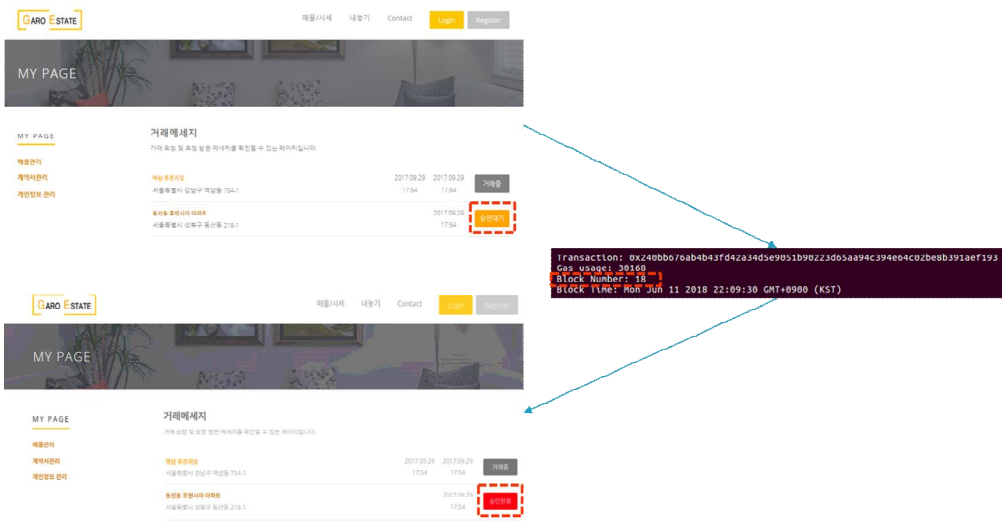
입력된 내용 중에 개인정보가 포함된 경우 사용자에게 이를 알리고, 개인정보 수집, 이용 및 제공에 대한 동의를 받는다. 또한 민감정보와 개인정보에 해당하는 데이터는 추출하여 암호화 및 비식별화 하고, 개인정보에 대해 정보 이용에 대한 유효 기간을 설정한다.

계약서에서 개인정보를 추출하고, 이를 알리는 화면이다. 실제 스마트 컨트랙트에 저장되는 데이터 중 개인정보에 해당하는 성명, 주민등록 번호, 지갑주소 등의 3개 개인정보가 포함되어 있음을 알리고, 정보주체로부터 계약을 위해 수집 및 이용한다는 내용에 동의를 받는다. 추출된 개인정보는 블록에 저장되기 전 암호화 한다.



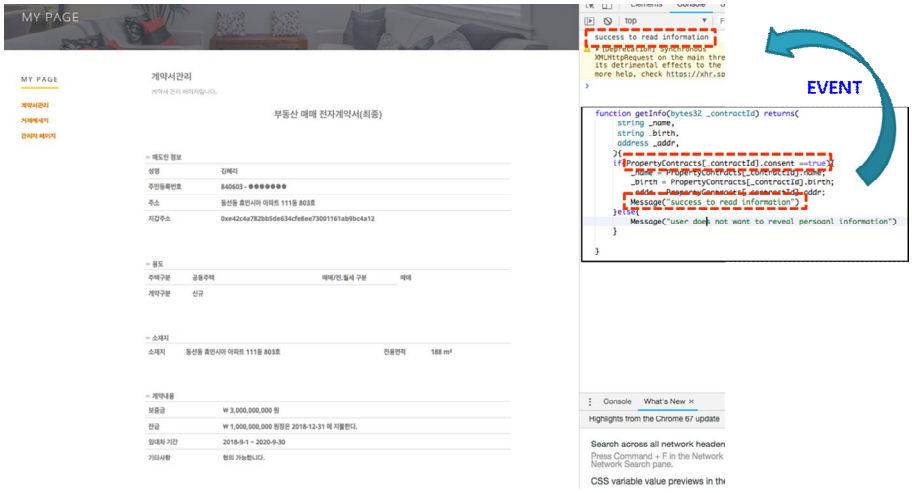
(그림 26) 개인정보 포함 여부 알림 및 동의 화면

이러한 과정을 거쳐 최종적으로 생성된 스마트 컨트랙트는 사람이 읽을 수 있는 형태(Human Readable)의 계약서로 화면에 보여지게 되며, 계약과 관련된 정보들은 transaction이 생성되어 블록에 저장됨을 확인할 수 있다.

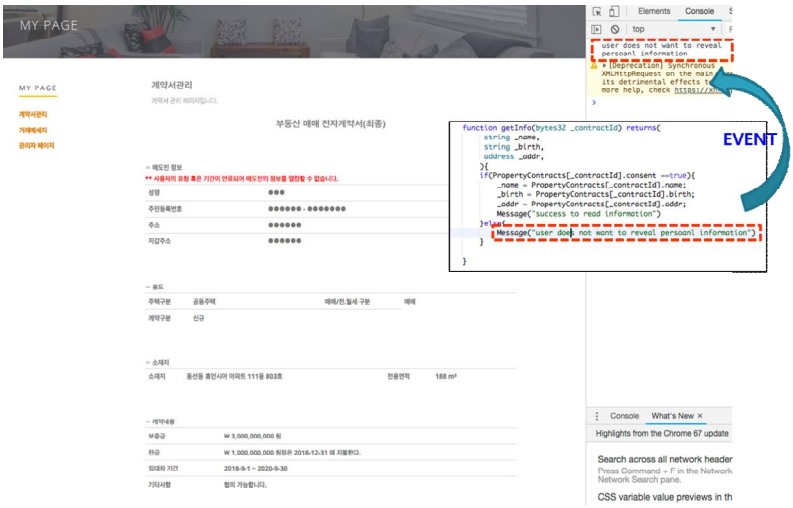


(그림 27) 계약서 블록 생성

계약서 내용 확인에 대해 권한이 있는 경우는 아래 첫 번째 그림과 같이 개인정보는 비식별화된 후 정보를 확인할 수 있으며, 계약 당사자가 아니거나 정보 삭제 후 정보의 읽기를 요청하는 경우 그 다음 화면과 같이 계약자의 개인정보를 확인할 수 없다.

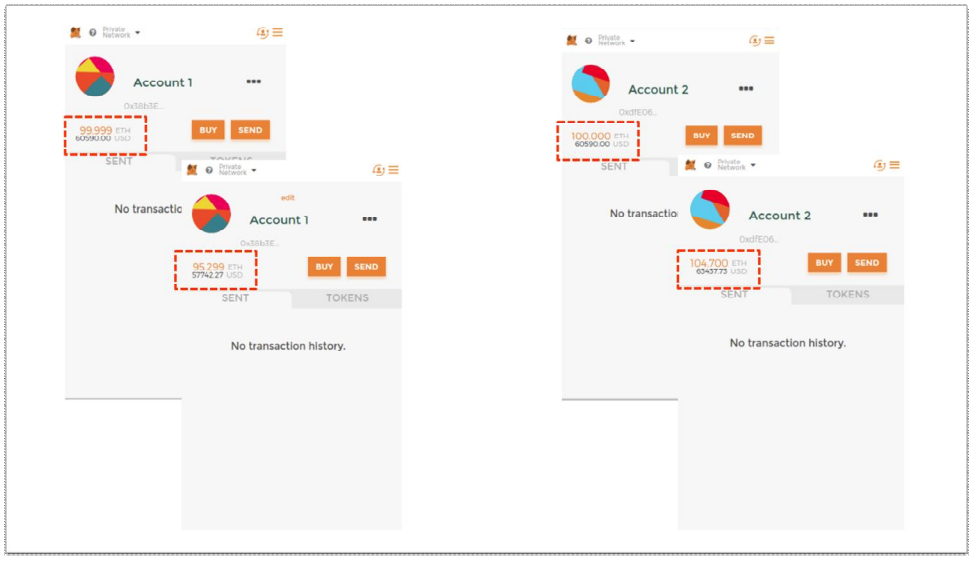


(그림 28) 유효한 계약서의 확인



(그림 29) 유효하지 않은 계약서의 내용 확인

계약 실행에 대한 확인은 아래와 같이 매도자와 매수자의 지갑 잔고 변화에서 확인할 수 있다.



(그림 30) 계약 실행 후 계정의 잔고 변화

5. 문제점 해결 및 보안성 평가

앞에서 제시했던 블록체인이 가지고 있는 문제점을 해결하고자 본 논문에서는 TSCM을 제안하였으며, 문제점 해결에 대한 결과는 다음과 같다.

[표 12] TSCM 보안성 평가

문제점	해결 여부	적용 메커니즘	문제 해결 방안
- 거래 내역이 공개돼 있어 원칙적으로 모든 거래 추적 가능(기밀성을 제공하지 않음)	✓	AAM /SCM	- 거래 내역이 공개되어도 개인정보나 민감정보에 대해서는 암호화/비식별화 하여 거래 당사자가 아니면 평문으로 된 정보를 확인할 수 없음 - 계약서 전체 내용을 확인하고자 할 때에는 거래 당사자 여부, 개인정보 보유기간 여부를 확인하여 Read 가능
- P2P 네트워크를 통해 작성되는 계약의 법적 유효성과 개인정보보호 컴플라이언스 준수를 보장	✓	CAM	- State Channel을 통해 계약 당사자간의 내용 확인 후 이에 대해 확인했음을 개인키 서명으로 보장 - 또한 대화 내용 전체를 저장함으로써 부인 방지 가능 - 법적 유효성에 대한 부분은 Specialist를 통해 검증
- 개인정보보호 컴플라이언스 관점의 파기 문제	✓	SCM	- 개인정보보호 유효 기간을 설정하여 기간이 지나거나 정보주체의 요청이 있는 경우 논리적 파기 방안 적용
- 스마트 컨트랙트 오류로 인한 네트워크 문제 발생 가능	✓	SVM	- 스마트 컨트랙트 배포 전 코드 유효성 검증을 통해 코드 자체의 기술적인 문제 해결
- 문제 발생 시 책임소재 모호	✓	CAM	- 검증자 노드(Specialist)를 배치하여 문제 발생 시 중재 가능

또한 본 논문에서 제안한 TSCM의 기능적인 측면과 관련하여, 정보보호의 3요소인 기밀성, 무결성, 가용성 측면에서 보안성을 평가해 보았다.

1) 기밀성

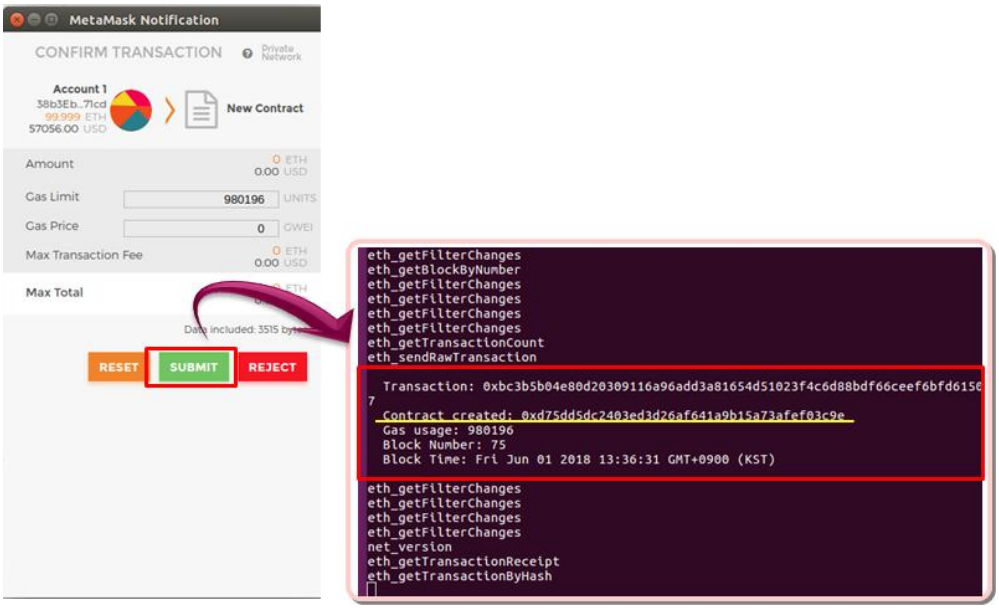
정보의 기밀성 확보는 정보보호 측면에서 매우 중요한 요소이나, 블록체인에서는 기밀성을 보장해 주지 않는다. 그러나 제안한 모델을 적용하면 중요한 정보는 비식별화 및 암호화를 적용하였기 때문에 내용을 확인할 수 없다. 기존 블록체인의 트랜잭션을 확인한 것과 제안 모델을 적용한 블록체인의 트랜잭션을 확인해 보면 다음과 같다.

(그림 31) 트랜잭션 기밀성 보장에 대한 확인

그림 위쪽의 일반적인 이더리움의 트랜잭션을 ASCII 코드로 변환하면 평문이 그대로 확인되는 것을 볼 수 있으나 아래 트랜잭션은 HASH 값만을 확인할 수 있다.

2) 무결성

P2P 기반에서의 거래에 대한 무결성을 보장하는 것은 블록체인이 지닌 고유 특징 중 하나이다. 제안 모델을 적용한 플랫폼에서는 실제 원거리에 있는 사용자들이 웹에서 작성한 계약서의 내용을 블록체인 기반 스마트 컨트랙트에서 생성하여 블록에 데이터를 저장하고 있다. 이렇게 블록에 저장된 정보는 네트워크에 참여하는 모든 사용자에게 공유되기 때문에 계약서 내용에 대한 무결성을 확보할 수 있다.

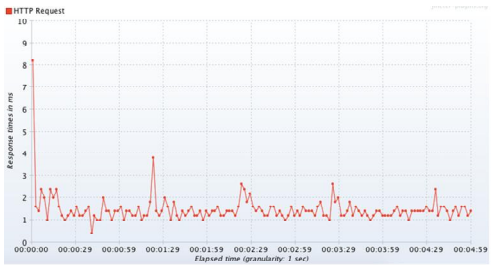


(그림 32) 전자지갑에서 생성된 스마트 컨트랙트 확인

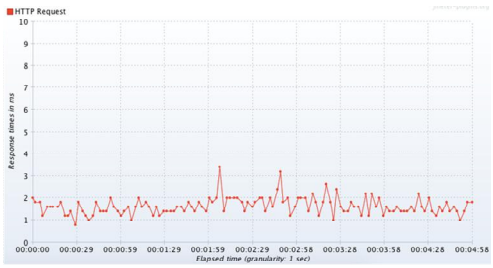
3) 가용성

가용성에 대한 확인은 여러번의 테스트를 통해 보안성이 적용된 TSCM과 TSCM이 적용된 시스템에서 개인정보보호 기능을 제거한 후 성능 테스트를

해 보았다. 성능 테스트는 각종 프로토콜에 부하를 거는 시험 테스트 유틸리티인 제이미터(JMeter)를 사용하였으며, 첫 번째 화면은 100명의 사용자를 기준으로 두 번 째 화면은 1000명의 사용자를 기준으로 테스트 한 결과이다.

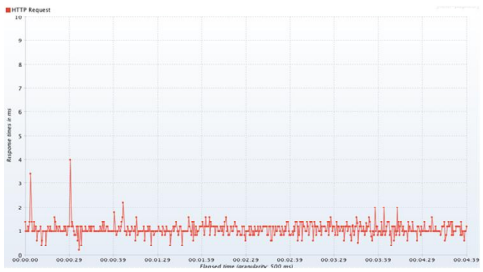


<TSCM 적용 트랜잭션>

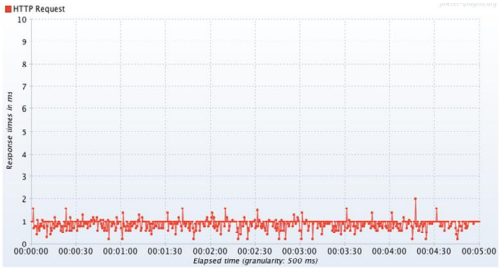


<일반 스마트 컨트랙트 트랜잭션>

(그림 33) 100명 기준 트랜잭션 비교



<TSCM 적용 트랜잭션>



<일반 스마트 컨트랙트 트랜잭션>

(그림 34) 1,000명 기준 트랜잭션 비교

TSCM에서는 정보보호 및 개인정보보호 기능을 한번 더 거친 후에 스마트 컨트랙트가 생성되는데, 초반에는 결과 처리 속도면에서 약간의 성능 저하가 있었으나, 트랜잭션 발생 수가 많아질수록 큰 차이가 없는

것으로 나타났다. 보안 기능을 적용해도 성능에 큰 차이가 없다는 것은 가용성 부분에서 크게 떨어지지 않음을 의미한다고 볼 수 있다.

제 6 장 결론 및 향후 연구

블록체인은 4차 산업혁명의 핵심 기술로 평가받으며, 블록체인의 장점을 이용한 새로운 서비스 개발이나 기술 활용 측면에서 활발하게 연구가 이루어지고 있다. 특히 디지털 화폐 기능이 강조되었던 블록체인 1.0에서 스마트 컨트랙트가 중심이 되는 블록체인 2.0으로 진화되면서 블록체인 기술은 각 산업군에서 더욱 주목받고 있다.

블록체인 기술에 실질적 가치를 더해 줄 수 있는 스마트 컨트랙트는 위·변조가 불가능한 블록체인을 이용해 지정된 조건이 일치할 경우에만 계약이 자동적으로 이행되도록 할 수 있게 하므로 계약에 기반한 다양한 분야에 적용할 수 있다. 그러나 계약이 이루어지는 과정에서 발생되는 개인정보와 민감한 정보들에 대해서는 블록에 그대로 올라가게 되면 개인정보보호 측면의 위험성이 존재한다. 블록체인 기술 자체는 무결성과 가용성을 보장하는 측면에서 보안에 뛰어나다는 평가를 받고 있지만, 데이터의 기밀성을 보장하지는 않기 때문이다. 그러므로 본 논문에서는 이러한 블록체인 기반의 스마트 컨트랙트에서 개인정보를 활용하는 경우에 대해 신뢰성을 고려하여 스마트 컨트랙트를 실행할 수 있는 설계 방안에 대해 제안하였다.

스마트 컨트랙트는 블록체인에서 실행할 수 있는 프로그램을 누구나 자유롭게 개발할 수 있다는 점에서 한층 보안 우려가 큰 분야이다. 또한 한번 작성되어 배포된 스마트 컨트랙트는 복구가 어려우며, 문제가 발생하는 경우 막대한 경제적 손실을 가져올 수 있다. 그렇기 때문에 스마트 컨트랙트가 실행되는 모든 단계에서 가장 중요한 부분은 “설계”라고

할 수 있다. 스마트 컨트랙트 설계 시에 이러한 정보보호 및 개인정보보호 측면의 취약점을 고려한다면, 다양한 산업 분야에서의 스마트 컨트랙트는 큰 성과를 낼 수 있는 기술이 될 것이다. 그러므로 본 연구에서는 스마트 컨트랙트 활용 시 발생할 수 있는 정보보호 이슈를 분석해 보고 해결 방안을 제시하고자 하였다. 제시한 모델을 부동산 계약에만 적용 해 본 점은 아쉬움으로 남는다. 향후에는 더 많은 사례 검증을 통해 더욱 안전하고 실효성 있는 블록체인 기반의 스마트 컨트랙트 기술 적용 방안 및 활용에 대해 연구하고자 한다.

참 고 문 헌

[1] Nakamoto, Satoshi. Bitcoin: “A peer-to-peer electronic cash system”, URL: http://www.bitcoinorg/bitcoin.pdf, 2008

[2] 금융위원회, “블록체인기술 금융분야 도입방안을 위한 연구”, 2016

[3] 정재원, 비트코인 악용 범죄 수사에 대한 제도 및 기술적 문제점과 해결 방안에 대한 연구, 서울대학교 융합과학기술대학원 디지털 포렌식 전공, 석사학위 논문, 2016

[4] Szabo, Nick. The idea of smart contracts. Nick Szabo’s Papers and Concise Tutorials, 1997

[5] 황경락, “비트코인 메커니즘 상세 분석 및 개선사항 연구”, 동국대학교 정보보호학과 석사학위논문, 2017

[6] 오세용, “블록체인을 활용한 전자거래에서 데이터 사전 유효성 검증 및 플랫폼 구현에 관한 연구”, 숭실대학교 대학원 IT정책경영학과, 2017

[7] TTA, “ICT 표준화 전략맵”, 한국정보통신기술협회, 2017

[8] 박수민, “디지털 비즈니스 환경 내 신뢰할 수 있는 블록체인 설계 방안”, 성신여자대학교 일반대학원 컴퓨터학과 석사학위논문, 2017

[9] 한국인터넷정보학회, “블록체인 방식을 활용한 온라인 투표시스템 적용 가능성 연구”, 2017년도 선거연수원 연구용역보고서, 2017

[10] 이부형, 임언주, 이종혁, “블록체인 플랫폼에서의 합의 알고리즘”, 한국통신대회 학술대회 논문집, pp386~387, 2017

[11] Miguel Castro and Barbara Liskov, “Practical Byzantine Fault Tolerance”, USENIX Technical Program - Paper - Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999

[12] https://tendermint.com/intro/consensus-overview

[13] 데일리 금융그룹(https://daylifg.blog.me/)

[14] 블록체인 구조와 이론, 위키북스

[15] 신다혜, 이종협, “핀테크를 위한 스마트 컨트랙트 보안”, 정보처리학회지 Vol.22 No. 5, 2015

[16] 박재현, 오재훈, 박혜영, “코어 이더리움 프로그래밍” 제이펍, 2018

[17] Vitalik buterin, Ethereum white paper: a next generation smart contract & decentralized application platform, Ethereumm.org, 2014

[18] https://ethereum.stackexchange.com/

[19] http://samse.tistory.com/465, dapp테스트를 위한 Swarm 실행하기

[20] 김영태, “기업의 정보보호 및 개인정보보호 컴플라이언스 평가 지표에 관한 연구”, 전남대학교 대학원 박사학위 논문, 2012

[21] 김나루, “Privacy by design′의 도입과 그 적용에 관한 소고”, 성균관법학. Vol.29 No.4, 2017

[22] 김혜리, 홍승필, “블록체인 네트워크에서의 개인정보보호 방안 연구 : 개인정보보호 컴플라이언스 중심”, 보안공학연구논문지 Vol15, No.2 (2018), pp81-92, 2018

[23] 이수현, 김혜리, & 홍승필. “개인정보보호를 고려한 블록체인 데이터 설계 방안 연구”. 한국통신학회 학술대회논문집, pp478-479. 2018

[24] 이수현, 김혜리, & 홍승필. “스마트 컨트랙트에서 개인정보 보호를 위한 설계 방안 연구”. 한국통신학회 학술대회논문집, pp604-605. 2017

[25] 유헌우, “블록체인 방식의 전자투표 시스템 구현 및 성능 개선 방안 연구”, 아주대학교 정보통신대학원 석사 학위 논문, 2016

[26] 이루다, “블록체인을 활용한 전자투표 시스템 구축”, 상명대학교 일반대학원 컴퓨터학과 석사 학위 논문, 2017

[27] 양민희, “블록체인을 활용한 보험사 건강체 특약 할인 시스템 설계 및 구현”, 한양대학교 전기 및 전자공학과 석사 학위 논문, 2018

[28] 이상민, “블록체인을 활용한 디지털 콘텐츠 저작권 보호 방법 연구”, 숭실대학교 정보과학대학원 석사 학위 논문, 2017

[29] 이찬혁, “블록체인을 활용한 IoT 데이터 보호 시스템 설계 및 구현”, 아주대학교 지식정보공학과 석사학위 논문, 2018

[30] Barcelo, Jaume. "User privacy in the public bitcoin blockchain." URL: http://www. dtic. upf. edu/~ jbarcelo/papers/20140704_User_Privacy_in_the_Public_Bitcoin_Blockchain/paper. pdf (Accessed 09/05/2016), 2014

[31] Ahmed Kosba, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”. Security and Privacy (SP), 2016 IEEE Symposium on, (2016) May22-26, San Jose, CA, USA, 2016

[32] 전솔, “안전하고 효율적인 그룹기반의 랜덤화된 메시 블록체인 시스템 연구”, 이화여자대학교 대학원, 2018

[33] 김광석, “4대 핀테크 동향과 금융산업의 파급 영향”, 정보통신기술진흥센터, 주간기술동향, 2016

[34] 김혜리, 강희정, 홍승필, “개인정보보호를 고려한 스마트 컨트랙트 설계 방안 연구”, 보안공학연구논문지 Vol15, No.3 (2018), pp139-154, 2018

[35] https://www.ethereum.org

[36] David Cerezo Sanchez, “Private and Verifiable Smart Contracts on Blockchains”, https://eprint.iacr.org/2017/878.pdf, 2015

[37] Buchman, Ethan , “Tendermint: Byzantine Fault Tolerance in the Age of Blockchains”, In partial fullment of requirements for the degree of Master of Applied Science in Engineering Systems and Computing,

2016

[38] Chrysoula Stathakopoulou, “On Scalability and Performance of Permissioned Blockchain”, EuroSys Doctoral Workshop ’18, April 23, Porto, Portugal, 2018

[39] Signe Rusch, “High-Performance Consensus Mechanisms for Blockchains”, EuroDW’18, April 23, Porto, Portugal, 2018

[40] Alysson Bessani et al. “A Byzantine Fault-tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform”. In: Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. SERIAL ’17. 2017.

[41] Vitalik Buterin et al. Casper the Friendly Finality Gadget. 2017. url: http://arxiv.org/abs/1710.09437

[42] Yossi Gilad et al. “Algorand: Scaling Byzantine Agreements for Cryptocurrencies”. In: Proceedings of the 26th Symposium on Operating Systems Principles. SOSP ’17. 2017.

[43] 국가법령정보센터(http://www.law.go.kr)

ABSTRACT

A Study on Trusted Smart Contract Model Based on Block Chain

Kim Hye Ri
Dept. of Computer Science
The Graduate School
Sungshin Women's University

In the era of the 4th industrial revolution represented by the block chain, big data, the Internet of things, and artificial intelligence, the development of technology has made it possible to analyze huge amount of information. And as the information directly relates to the profit, harmonization of the use and protection of personal information becomes increasingly important. In the block-chain technology, every participants hold all the ledgers which store the transactions between them and also carry out reflecting new transactions mutually. In the process, there is a risk that confidential data and personal information listed on the block chain will be disclosed unintentionally. In addition, the block-chain technology itself has been evaluated as having excellent security by securing the integrity and availability of data, but it is not guaranteed to confidentiality of data, so the lack need to be considered. In recent years, attempts that introduce smart contract based on block chains in various fields such as transfer of ownership, inheritance, bestowal, and

purchasing goods have been on the rise. Especially, in these fields, it is necessary to be considered because they contain numerous of privacy and sensitive information, so new accessing formula of applying technique for protecting private information and processing different from the existing one needs in such a block-chain network. Though smart contracts are programs, they need to take into account both information protection of existing applications and umbrella for information as a block-chain.

In this study, we analyze the information protection issues related to private and sensitive during activating the block-chain based smart contract, and propose a Trusted Smart Contract Model (TSCM) as a solution to the analyzed issues. TSCM assures the legal status of the contract contents, considering that the Smart Contract can not be reversed once the program has been distributed, and reviews the reliability of Smart Contract as a program. In addition, protection measures are applied to the personal information or sensitive information contained in the contract, and access control is applied so that only the authorized user can confirm the contents. The proposed method is applied to real estate contract cases which include many personal information and sensitive information.