www.osia.or.kr

OSIA S&TR Journal

ISSN 1738-9887 Vol. 32, No. 1, March 2019
• 발행인 : 이혁준 회장/OSIA • 편집위원 : 김형식 교수/성균관대학교

02 Editorial
블록체인의 보안 및 상호운용성 연구 동향
김형식/성균관대학교

Article
04 50%미만 이중지불 공격
장재혁, 이흥노/광주과학기술원
11 Inter-Chain 기술 동향
김준희, 김중헌/중앙대학교
16 블록체인 기반의 ID 관리 기술 동향
김석현, 조영섭, 김수형/ETRI
23 IoT 환경에 적합한 블록체인 및 스마트 컨트랙트 기술 연구
김베드로, 이대화, 지우중, 김형식/성균관대학교

(사)한국컴퓨터통신연구회
Open Standards and ICT Association

블록체인의 보안 및 상호운용성 연구 동향



성균관대학교
김 형 식

이미 “블록체인”이라는 용어는 더 이상 새롭거나 낯설지 않고, 인터넷과 웹처럼 친숙한 용어가 되고 있습니다. 2년 전의 암호화폐의 열기를 거쳐 학계와 산업계에서는 블록체인 기술을 둘러싼 많은 토론이 진행되고 있습니다. 그 중 일부는 블록체인 기술에 대한 무용론부터 시작하여 차세대 인터넷 플랫폼에 대한 가능성까지 논의하고 있습니다. 중요한 것은 블록체인 기술은 아직 현재 진행 중이며, 성능 및 보안성에 대한 많은 기술적인 난제들을 풀어야 하는 상황이라는 점입니다.

본 호에서는 현재 논의되고 있는 가장 중요한 블록체인 이슈인 보안성과 상호운용성에 대한 연구 결과를 소개하고 있습니다. 블록체인의 특성상 발생할 수밖에 없는 이중 지불 문제와 이기종 간의 블록체인 네트워크를 통합하기 위한 인터 체인 기술을 논의합니다. 블록체인의 중요한 응용 분야인 ID 관리 기술 및 IoT 관리 기술에 대한 최신 연구 동향을 소개하고 있습니다.

첫 번째 논문은 이중 지불이라는 블록체인의 고전적인 보안 문제에 대한 논문으로서 이중 지불에 대한 기존의 명제인 51% 이상의 컴퓨터 자원이 필요하다는 가정에 대한 의문을 제기하고 있습니다. 현실 블록체인 네트워크에서는 공격자의 컴퓨터 자인이 50% 미만인 경우에도 여전히 효과적인 이중 지불 공격이 가능하다는 것을 공격 성공률 및 공격자의 이윤을 모델링하여 몬테카를로 시뮬레이션을 통하여 증명하고 있습니다.

두 번째 논문은 이기종 간 블록체인 트랜잭션 및 데이터를 상호 교환 관리할 수 있도록 제안되고 있는 Inter-Chain 기술에 대해서 소개하고 있습니다. 현존하는 다양한 블록체인 네트워크 기술을 고려했을 때, 상호 운용성을 위하여 서로 다른 블록체인간 데이터 교환을 가능하게 해주는 Inter-Chain 기술은 향후 블록체인 기반 생태계를 구축하는데 중요한 이슈가 될 것이라 판단됩니다.

세 번째 논문은 블록체인을 이용한 사용자 계정 관리 기술을 소개하고 있습니다. 기존의 ID 관리 기술은 사용자의 개인 정보가 중앙의 특정 기관에서 관리되기 때문에 사용자의 자기 정보 통제 기능이 미흡하고, 개인 정보가 유출되는 사고 등이 발생할 수 있는 문제를 가집니다. 따라서 이러한 문제를 해결하기 위해서 사용자가 스스로 자신의 계정을 관리할 수 있는 방안이 필요합니다. 본 논문에서는 블록체인을 이용하여 어떻게 이러한 문제를 해결하고 탈중앙화된 사용자 계정 관리 시스템을 구축할 수 있는지를 소개하고 있습니다.

네번째 논문은 IoT 환경에서의 블록체인 기술에 대한 요구 사항을 분석하고, 요구 사항에 적합한 다양한 프로젝트를 소개하고 있습니다.

본 특집호 발간을 위해 소중한 시간을 내어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회 여러분께 깊은 감사를 드립니다.

50%미만 이중지불 공격

장재혁, 이흥노
광주과학기술원

Abstract

블록체인은 전 세계에 분포된 수많은 네트워크 노드들이 하나의 거래장부를 공동으로 기록, 관리하는 분산화 장부 시스템이다. 블록체인 기술은 합의와 분산화를 바탕으로 거래 기록의 위조가 불가능하도록 설계되었으나, 가상화폐 시장의 성장과 함께 이중지불 공격 (double-spending attack)을 통해 장부를 위조하여 부당이득을 취하려는 시도가 끊임없이 존재해 왔다. 본 논문에서는 이중지불 공격의 위험성을 분석한다. Satoshi Nakamoto는 2008년 비트코인에 대한 이중지불 공격의 성공을 위해서는 전 세계의 노드들이 보유한 컴퓨터 자원보다 더 많은 컴퓨터 자원, 즉 51% 이상의 컴퓨터 자원이 필요하다는 결론을 내렸다. 반면, 본 논문에서는 50% 미만의 적은 컴퓨터 자원을 사용하는 이중지불공격도 위협적임을 보였다. 이러한 결론은 이중지불 공격의 성공 확률이 아닌 기대 이윤을 분석함으로써 얻을 수 있었다. 구체적으로는, 대규모 시뮬레이션을 통해 실제 작동중인 블록체인 네트워크에 50% 미만의 이중지불 공격을 행할 경우에 대한 공격자가 얻는 기대 이윤을 측정하였으며, 이러한 공격을 방지 할 수 있는 방안을 제시한다.

I. 서론

블록체인은 비트코인과 이더리움 등 현존 가상화폐의 핵심 기술이며, 세계에 분포된 수많은 노드들이 하나의 거래장부를 공동으로 기록, 관리하는 분산화 장부 시스템이다. 분산화 장부는 은행, 국가 혹은 중개사가 거래를 관리 및 기록하는 중앙화 장부 시스템과 대조적이며, 중앙화 장부에 비해 해킹 혹은 위조 등에 강인하다. 그러나 거래내용을 전세계의 노드들에게 검증 받아야 하기 때문에 거래속도가 상대적으로 느리다는 단점이 있다. 블록체인과 비트코인은 2008년 Satoshi Nakamoto의 백서에서 소개되었으며 [1], 2019년 기준 약 60억 달러의 유통 규모를 보유한 거대 가상화폐로 성장하였다.

블록체인 기술은 합의와 분산화의 개념을 바탕으로 거래기록의 위 변조가 불가능하도록 설계되었다. 그러나 가상화폐시장의 성장과 함께 이중지불 공격 (double-spending attack)과 같은 보안성 공격을 통해 부당이득을 취하려는 시도가 끊임없이 존재해 왔다. 이중지불공격은 공격자가 서비스 혹은 재화의 대가로 지불한 가상화폐의 거래기록을 무효화하여 재사용하는 공격이다. 예를 들어, 가상화폐 거래소에게 가상화폐를 지불한 대가로 현금을 출금한 후, 이러한 거래 기록을 블록체인상에서 지워버리는 것이다. 실제로 지난 2018년에는 BitcoinCash, Zcash, ZenCash, LitecoinCash와 같은 대규모 가상화폐들이 이중지불 공격의 피해를 받았으며, 그 피해액은 수백만 달러에 달한다 [2], [3], [4].

이중지불공격은 블록체인 합의 알고리즘을 역이용하면 가능하다. 블록체인 합의 알고리즘은 통신지연 등의 이유로 노드들이 보유한 블록체인이 서로 다를 때, 어느 것을 유지하고 어느 것을 버릴지를 결정하는 알고리즘이다. 비트코인의 합의 알고리즘인 longest chain consensus는 길이가 더 긴 블록체인이 더 많은 노드들에게 검증 받았으며, 따라서 더 신뢰 할 수 있다고 결정한다 [1]. 결과적으로, 이중지불공격이 성공하려면 전 세계에 분포된 노드들이 공동으로 생성한 블록체인보다 길이가 더 긴 사기 블록체인을 생성하여 합의 알고리즘을 속여야 한다.

Nakamoto [1]와 Rosenfield [5]는 이러한 합의 알고리즘의 의의를 수학적으로 분석하였고, 이중지불 공격의 성공률이 100%가 되기 위해서는 전 세계의 노드들이 보유한 컴퓨터 자원보다 더 많은 컴퓨터 자원(51%)이 필요하다는 결론을 내렸다. 이중지불 공격이 51% 공격으로 불리는 이유이다. 개인 혹은 하나의 집단이 전 세계의 컴퓨터 자원보다 더 많은 자원(51%)을 보유하는 것은 현실적으로 매우 어렵고, 따라서 비트코인이 이중지불 공격으로부터 안전하다는 주장이다. 그러나 만약 50% 미만의 컴퓨팅 자원을 사용하는 이중지불 공격, 즉 50%미만 이중지불 공격이 공격자에게 큰 이윤을 가져다 줄 수 있다면, Nakamoto와 Rosenfield의 결론은 재검토되어야 한다.

본 논문은 IEEE Transactions on Information Forensics and Security 에 제출된 논문의 수학적 정리[6]를 바탕으로 50%미만 이중지불 공격의 가능성을 시뮬레이션을 통해 보여준다. 구체적으로는 이중지불 공격의 성공률이 아닌, 이중지

불 공격이 가져다 주는 기대 이윤을 분석하였다. 이러한 관점은 Nakamoto와 Rosenfield의 결론과는 전혀 다른 결론을 가져다 주었다. 시뮬레이션을 통해 50% 미만 이중지불 공격의 성공이 보장되지 않더라도, 공격의 대상이 되는 거래의 가치가 충분히 크면 공격자 입장에서 이중지불 공격의 기대 이윤은 크다는 것을 보였다. 만약 한번의 공격이 실패하더라도, 계속 시도하면 결국 그 동안의 지출을 모두 상쇄하고도 남는 이윤이 돌아온다는 것이 기대 이윤의 의미다. 공격자가 이중지불 공격을 수행하며 소요하는 지출은 공격시간 동안 소요한 컴퓨터 자원의 운용 비용뿐인데, 이를 상쇄할 만큼 가치가 큰 거래를 공격하면 결국 이윤을 기대할 수 있다는 것이다. 결론적으로, 상대적으로 적은 (50% 미만) 컴퓨터 자원을 이용하는 쉬운 이중지불공격도 위험하다는 것이다.

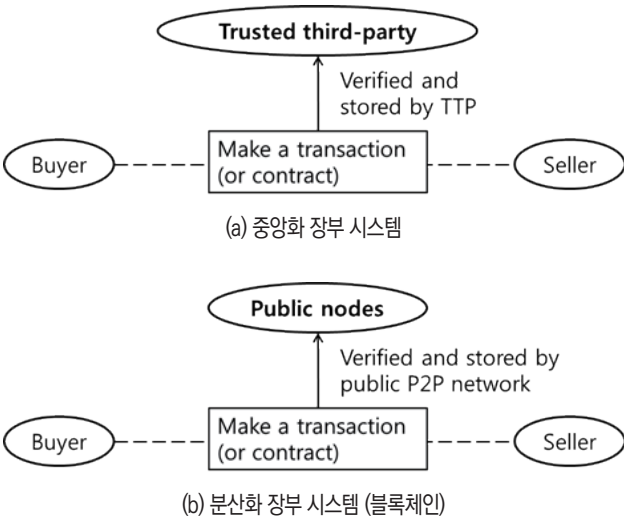
본 논문은 다음과 같이 구성되어 있다. 2장에서는 블록체인의 작동 원리를 소개한다. 3장에서는 이중지불 공격을 소개하고 공격의 성공 조건을 정의한다. 4장에서는 이중지불 공격의 성공률 분석에 관한 기존 연구문헌을 소개하고 분석의 한계점을 제시한다. 5장에서는 이중지불 공격의 이윤을 분석하고 50% 미만의 컴퓨터 자원을 이용하는 이중지불 공격도 위협적임을 실험을 통해 보인다. 마지막으로, 6장에서 요약과 함께 결론을 맺는다.

II. 블록체인

블록체인은 분산화 거래 시스템으로써, 기존 거래 시스템인 중앙화 거래 시스템과 대조적이다. 그림 1은 중앙화 거래 시스템과 분산화 거래 시스템을 비교하여 보여준다. 중앙화 거래 시스템은 공인된 3자인 trusted third-party (TTP)에 의해 거래내용이 검증 및 기록된다. 이러한 기존 방식은 TTP에 완전히 의존하고 있기 때문에, TTP가 부정한 행동을 취하거나 해킹당할 시 거래자는 금전적 피해를 받을 수 있다. 반면, 블록체인에 의한 분산화 거래 시스템은 전 세계에 분포한 풀 노드 (채굴자)에 의해 거래내용이 공동으로 검증 및 기록된다. 따라서 블록체인은 TTP에 의한 거래 시스템보다 더 신뢰할 수 있는 거래 시스템을 제안한다.

블록체인 네트워크를 구성하는 노드는 크게 거래자 노드와 채굴자 노드로 구분 할 수 있다. 거래자 노드는 거래(transaction)을 생성하여 채굴자 노드에게 공표한다. 채굴자 노드는 검증되지 않은 거래들을 모아서 검증하고, 블록에 담는다. 이후 채굴자 노드는 블록에 담긴 거래들이 수정되지 못하게 하기 위해 작업증명을 수행한다.

작업증명의 방식은 블록체인 프로토콜마다 차이가 있으며, 본 논문에서는 비트코인 프로토콜의 작업증명 (proof-of-work)를 소개한다. 비트코인의 작업증명은 블록의 특별한 해쉬 (hash) 값을 찾는 것이다.



(a) 중앙화 장부 시스템

(b) 분산화 장부 시스템 (블록체인)

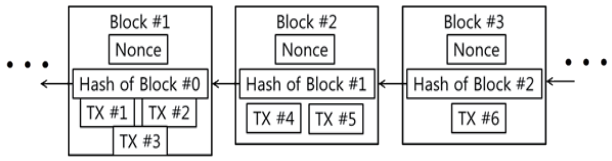
〈그림 1. 중앙화 장부 시스템과 분산화 장부 시스템〉

해쉬는 SHA-256 함수에 의해 1MByte 크기의 블록이 압축된 256bit 길이의 이진 문자열이다. SHA-256 해쉬 함수의 특성은 입력 블록의 이진 값 중 하나의 값이라도 수정되면, 출력되는 해쉬 값이 불규칙적으로 변한다는 것이다. 다시 말해, 누군가 악의적인 목적으로 블록의 거래내용을 수정하고 다시 해쉬 값을 계산하면, 이전에 계산된 해쉬 값과는 전혀 다른 결과를 얻는다. 이러한 SHA-256 해쉬 함수의 특성이 거래내용 위조 및 변조를 방지하기 위해 사용된다.

작업증명의 목적은 수 많은 채굴자가 하나의 블록을 함께 검증하였다는 사실을 증명하는 것이다. 이러한 목적을 달성하기 위해 비트코인 프로토콜은 채굴자에게 블록의 특별한 해쉬 값을 찾도록 요구한다. 구체적으로, 블록의 내용에 임시 값(nonce)을 추가한 후, 프로토콜이 요구하는 조건을 만족하는 블록의 해쉬 값이 출력될 때까지 임시 값을 변경하도록 지시한다. 특별한 해쉬를 찾으면 하나의 블록을 완성하는 것이며, 블록을 완성한 노드에게는 암호화폐가 보상으로 주어진다. 특별한 해쉬 값의 조건이 어렵기 때문에, 조건을 만족시키려면 SHA-256 함수를 수없이 많이 실행하여야 한다. 즉, 조건을 만족시키기까지 오랜 시간이 소요되며, 그 시간 동안 더 많은 채굴자가 거래들을 검증 하는데 참여 할 수 있다.

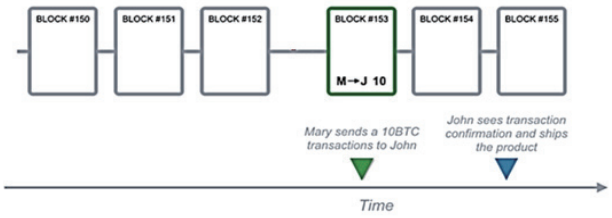
블록체인의 블록들은 서로 연결되어있다. 그림 2은 블록체인의 구조를 보여준다. 작업증명을 통해 하나의 블록이 완성되면, 그 다음 블록의 내용에는 이전 블록의 특별한 해쉬 값이 포함된다. 이러한 체인 구조는 누군가 악의적인 목적으로 이미 검증된 거래 내용을 위조 및 변조하는 것을 어렵게 만든다. 예를 들어 그림 2에서, 블록 #1에 들어있는 거래 #2를 수정하기 위해서는 먼저 블록 #1의 특별한 해쉬 값을 새롭게 찾아야

한다. 그리고 새롭게 찾은 블록 #1의 특별한 해쉬 값은 블록 #2의 해쉬 값에도 영향을 주기 때문에, 블록 #2의 특별한 해쉬 값도 새롭게 찾아야 한다. 이러한 일련의 과정을 가장 최신 블록까지 반복해야 한다. 특별한 해쉬 값을 찾는 작업증명 과정은 많은 시간을 소요한다. 따라서 혼자서 수 많은 작업증명을 완성하는 것은 매우 어렵다.



〈그림 2. 블록체인의 구조〉

거래가 포함된 블록 이후에 더 많은 블록이 연결된다면, 그 거래는 위-변조의 위험에 더욱 강인해진다. 이러한 이유로 거래자는 이체 확인 (block confirmation)라는 과정을 수행한다. 이체 확인은 거래를 완료하기 전에, 거래내용이 기록된 블록을 포함하여 몇 개의 블록이 더 생성되기까지 기다리는 것이다. 이때 생성을 기다리는 블록의 개수를 이체확인 수 (block confirmation number, N_{BC})라고 한다. 예를 들어, 그림 3은 Mary가 John에게 10 BTC의 암호화폐를 지불하고, John은 Mary에게 그 대가에 상응하는 제품을 제공하는 거래의 이체확인 과정을 보여준다. 이체확인 수 (N_{BC})가 2개이면, 거래가 포함된 블록과, 그 이후에 하나의 블록이 생성되는 것을 기다린다. 이체확인 수 N_{BC}가 클수록 위-변조의 위험에 더 강인해지지만, 거래처리 속도는 느려진다.



〈그림 3. 이체확인 과정의 예 (출처: Telemaximum.com)〉

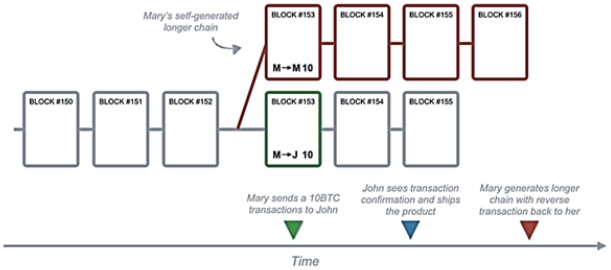
블록체인의 블록은 전 세계의 노드가 공동으로 형성하기 때문에, 네트워크 지연 등의 이유로 서로 연결되지 않는 블록들이 동시에 생성 될 수 있다. 구체적으로, 하나의 블록에 서로 다른 두 개 이상의 블록이 연결되어 체인의 갈래(fork)가 발생 할 수 있다. 비트코인 프로토콜은 여러 갈래가 존재하는 것을 허용하지 않는다. 다수의 갈래 중 하나의 갈래만 유지하는 과정을 합의 (consensus)라 한다. 합의는 여러 방식이 존재하며 [7], 비트코인의 경우 길이가 가장 긴 갈래를 유지시키는 longest chain 합의를 사용한다.

III. 이중지불 공격

이중지불 공격은 longest chain 합의를 악용하여 거래 내용을 변조하고 부당이득을 취하는 공격이다. 그림 4은 Mary (이하 M)가 John (이하 J)에게 이중지불 공격을 수행하는 과정을 보여준다. 공격에 앞서, M은 J에게 10 BTC의 암호화폐를 지급하고 재화를 공급받는 정상적인 거래를 작성 후 공표한다. 정상적인 거래는 채굴자들에 의해 검증된 후 정상블록 #153에 포함된다. 이후 채굴자들은 정상블록 #153을 잇는 또 다른 정상블록들을 지속적으로 생성한다. 한편, M은 정상적인 거래를 공표하자마자 정상적인 거래의 내용을 무효화하는 비정상적인 거래를 작성한다. 비정상적인 거래의 내용은, 예를 들어, "M이 M에게 10 BTC를 이체한다"가 될 수 있다. M은 비정상적인 거래를 채굴자들에게 공개하지 않는다. 채굴자들이 정상적인 거래가 포함된 정상블록을 생성하는 동안, M은 은밀하게 비정상적인 거래가 포함된 비공개블록 #153을 생성하고, 이를 잇는 또 다른 비공개블록들도 생성한다. M은 비정상적인 거래가 포함된 비공개 블록들의 갈래를 다음의 조건이 충족되면 공개한다.

i. 채굴자들의 정상블록의 개수가 이체확인 수 (N_{BC}) 보다 크고,
ii. 공격자의 비공개블록의 개수가 정상블록의 개수보다 많음

M이 비공개 블록들의 갈래를 공개하는 시점에서는, 첫 번째 조건에 의해 정상적인 거래는 완료되었고, 따라서 M은 J로부터 재화를 공급받았다. 그리고 두 번째 조건에 의해 네트워크 모든 노드의 lognest chain 합의는 M이 은밀하게 개발한 갈래를 선택한다. 즉, 두 번째 조건에 의해 M이 J에게 10 BTC를 지급한다는 거래가 무효화되기 때문에 M은 10 BTC를 재사용 할 수 있다.



〈그림 4. 이중지불 공격의 예 (출처: Telemaximum.com)〉

Ⅳ. 이중지불 공격의 성공률 분석

이중지불 공격의 성공확률은 Nakamoto [1]와 Rosenfield [5]에 의해 계산되었다. 확률 분석을 위해, 채굴자와 공격자가 일정시간 동안 생성한 블록의 개수를 독립적인 Poisson 확률 분포[8]를 갖는 랜덤 변수들로 모델링 하였다. Poisson 확률 모델을 바탕으로, 이중지불공격의 성공을 위한 두 조건의 달성 확률 P_1과 P_2를 각각 계산 한 후 곱하였다.

먼저, 두 번째 조건인 ii) 비공개블록의 개수가 정상블록의 개수보다 많을 확률은 Gambler's ruin theorem [9]를 적용하여 계산하였다. 채굴자와 공격자가 보유한 컴퓨터 자원의 비를 각각 p와 q라 칭하겠다 ($p+q=1$). 이중지불공격이 시작된 이후 어느 시점에서 채굴자 갈래의 정상블록 개수가 h개이고 공격자 갈래의 비공개블록 개수가 a개 ($h \geq a$)라 가정하겠다. 이후 무한정한 시간이 지났을 때, 공격자가 언젠가는 두 번째 조건을 달성할 확률은

$$P_2(h-a)=\begin{cases}\left(\frac{q}{p}\right)^{h-a+1}, & if\ p>q\ and\ h\geq a,\\ 1, & otherwise\end{cases} \quad (1)$$

이다.

Nakamoto와 Rosenfield의 분석 결과는 첫 번째 조건인 i) 정상블록의 개수가 이체확인 수 보다 클 확률의 계산 방법에서 차이가 있다. 이 확률을 계산하기 위해서는 채굴자가 생성한 정상블록의 개수가 이체확인 수 (N_{BC})와 같아지기까지 소요되는 시간에 관한 확률모델이 필요하다. Nakamoto는 이 소요시간을 상수로 가정한 반면, Rosenfield는 이 소요시간을 랜덤 변수로 정의하여 보다 일반적인 방법으로 접근하였다.

구체적으로, 채굴자가 하나의 정상블록을 생성하는데 평균 D_H의 시간이 소요될 때, 공격자의 비공개블록 생성 평균 소요시간 D_A를 다음과 같이 계산 할 수 있다.

$$D_A = D_H \frac{p}{q}. \quad (2)$$

이는 블록생성 평균 소요시간이 공격자 혹은 채굴자가 보유한 컴퓨터 자원에 반비례한다는 가정을 바탕으로 계산되었다. Nakamoto는 공개블록의 개수가 N_{BC}와 같아지기까지 소요된 시간을 $D_H N_{BC}$로 가정하였다. 따라서 $D_H N_{BC}$의 시간 동안 공격자가 생성한 비공개 블록의 평균 개수는 $D_H N_{BC}/D_A$ 이며, 식 (2)에 의해 이 값은 qN_{BC}/p와 같다. Poisson 확률 분포에 의해, Nakamoto가 계산한 정상블록이 N_{BC}개 생성되기까지 소요된 시간 동안 공격자가 생성한 비공개블록의 개수가 k 개일 확률은

$$G_1(k)=\left(\frac{qN_{BC}}{p}\right)^k \frac{e}{k!}^{\frac{qN_{BC}}{p}} \quad (3)$$

이다. 반면 Rosenfield는 정상블록의 개수가 N_{BC}와 같아지기까지 소요된 시간이 랜덤 변수 일 때, 그 시간 동안 공격자가 생성한 비공개블록의 개수가 k 인 확률이 negative binomial 확률 분포를 따른다는 사실을 적용하였다. 다시 말해, Rosenfield가 계산한 공개 블록이 N_{BC}개 생성되기까지 소요된 시간 동안 공격자가 생성한 비공개 블록의 개수가 k 개일 확률은

$$P_1(k)=\binom{N_{BC}+k-1}{N_{BC}-1}p^{N_{BC}}q^k \quad (4)$$

이다. Rosenfield의 계산 결과를 바탕으로, 공격자가 언젠가는 이중지불공격에 성공할 확률 P_{AS}는

$$\begin{aligned}P_{AS}&=\sum_{k=0}^{\infty}P_1(k)P_2(N_{BC}-k)\\&=\begin{cases}\sum_{k=0}^{N_{BC}}\binom{N_{BC}+k-1}{N_{BC}-1}p^{N_{BC}}q^k\left(\frac{q}{p}\right)^{N_{BC}-k+1}+\sum_{k=N_{BC}+1}^{\infty}\binom{N_{BC}+k-1}{N_{BC}-1}p^{N_{BC}}q^k, & if\ p<q,\\ 1, & if\ p\geq q\end{cases}\\&=\begin{cases}1-\sum_{k=0}^{N_{BC}}\binom{N_{BC}+k-1}{N_{BC}-1}p^{N_{BC}}q^k\left(1-\left(\frac{q}{p}\right)^{N_{BC}-k+1}\right), & if\ p<q,\\ 1, & if\ p\geq q\end{cases}\end{aligned} \quad (5)$$

이다.

식 (5)에 의해, $P_{AS}=1$, 즉 이중지불 공격의 성공을 보장하기 위한 필요-충분 조건이 $p \leq q$ 이라는 것을 알 수 있다. 다시 말해, 공격자가 채굴자보다 더 많은 컴퓨터 자원을 보유하는 것이 공격 성공의 조건이다. 이러한 결론은 Nakamoto의 계산식에서도 마찬가지로 유도될 수 있다. Gambler's ruin theorem을 적용하여 얻은 이 결론은 공격자에게 무한정의 시간이 주어진다는 가정이 내포되어 있다. 그러나, 공격을 시도하는 시간 동안 컴퓨터 자원을 운용하는 비용이 지속적으로 발생되기 때문에 이러한 가정은 비현실적이다. 뿐만 아니라, 공격 성공확률 100%가 아니어서 실패의 위험이 존재한다고 하더라도, 공격 성공 시 얻을 수 있는 이윤이 소요된 비용보다 훨씬 크다면 공격자의 입장에서는 공격을 시도해 볼 수 있다. 따라서 이중지불 공격의 성공률뿐만 아니라 이윤도 분석 할 필요가 있다.

V. 이중지불 공격의 이윤 분석

앞서 이중지불 공격의 성공률 분석을 통해 공격자의 컴퓨터 자원이 채굴자의 컴퓨터 자원보다 더 적을 때, 즉 $p > q$ 일 때는 이중지불 공격이 실패 할 수 있음을 확인하였다. 본 장에서는 $p > q$ 이더라도, 50% 미만 이중지불 공격이 수익성이 있으며 따라서 거래자에게는 위협적임을 Monte-Carlo 시뮬레이션을 통해 확인한다. 본 장의 내용은 [6]에서 수학적으로 증명되었다.

공격자의 컴퓨터 자원의 비율이 q 일 때, 이중지불 공격의 이윤 $F(q)$ 를 다음과 같이 정의 하였다.

$$F(q) = V(q) - C(q), \tag{6}$$

여기서 $V(q)$ 는 이중지불 공격으로부터 얻는 수익이며, $C(q)$ 는 q 만큼의 컴퓨터 자원을 운용하는데 소요된 지출이다.

지출 $C(q)$ 는 컴퓨터 자원을 운용한 시간과 컴퓨터 자원의 크기에 비례한다고 가정한다. $C(q)$ 를 계산하기에 앞서, $p > q$ 이기 때문에 이중지불 공격이 실패할 가능성이 존재함을 주의해야 한다. 만약 이중지불 공격이 실패하면, 컴퓨터 자원을 운용하는 시간이 무한정 늘어나며, 따라서 지출 $C(q)$ 도 무한대로 발산한다. $p > q$ 인 경우에서 이러한 무한대의 지출을 방지하기 위해, 중단 시간 (cut time) t_{cut} 을 정의한다 [참조문헌 6의 Theorem 7]. 공격자는 t_{cut} 의 시간 내에 이중지불 공격에 성공하지 못할 경우, 지출의 발산을 방지하기 위해 공격을 중단한다. 만약 t_{cut} 내에 공격이 성공할 경우, 지출 $C(q)$ 는 공격 성공 시간 동안 소요된 컴퓨터 자원 운용 비용이다. 공격 성공 시간은 불확정적이기 때문에 랜덤 변수 T_{AS} 로 모델링 될 수 있다. 컴퓨터 자원의 크기는 공격자의 시간당 평균 블록 생성량, 즉 D_A^{-1} 에 비례한다고 가정한다. 종합하면, 공격자의 컴퓨터 자원 비율이 q 이고 중단 시간이 t_{cut} 일 때의 지출 $C(q)$ 은

$$C(q) = \begin{cases} \gamma D_A^{-1} T_{AS}, & if\ attack\ succeeds, \\ \gamma D_A^{-1} t_{cut}, & otherwise \end{cases} \tag{7}$$

이며, 여기서 γ 는 하나의 블록을 생성하는데 소요되는 평균비용이다.

식 (7)의 지출을 계산하기 위해서는 파라미터 D_A 와 γ 가 필요하다. D_A 는 채굴자의평균 블록생성 주기인 D_H 로부터 (2)번 식을 통해 계산이 가능하다. 파라미터 D_H 와 γ 는 공격 대상 블록체인 네트워크에 따라 다르며, 그 값은 인터넷에 공개된 정보로부터 얻을 수 있다. 본 논문에서는 BitcoinCash 네트워크를 예로 들겠다. BitcoinCash의 평균 블록생성 주기는 $D_H = 600$ 초로 네트워크 개발자에 의해 고정되어있다. 채굴자가 보유한 컴퓨터 자원의 크기가 변동하면, 채굴 알고리즘에 D_H 가 유지되도록 채굴 난이도가 변경된다. 또 다른 파라미터인 γ 의 값은 컴퓨터 자원 대여 서비스를 제공하는 업체인 nicehash.com에 의해 결정 될 수 있다. nicehash.com에 따르면, 2018년 12월을 기준으로 BitcoinCash에서 하나의 블록을 채굴하는데 소요되는 비용은 $\gamma = 0.33$ 비트코인(BTC) 이다.

수익 $V(q)$ 는 이중지불 공격이 성공 할 경우 이중지불 공격의 대상이 되는 거래의 가치 v 와 같으며, 공격이 실패할 경우 0이다. 공격이 성공 할 확률은 공격자의 컴퓨터 자원 q 에 영향을 받는다. 수식으로는,

$$V(q) = \begin{cases} v, & if\ attack\ succeeds, \\ 0, & otherwise \end{cases} \tag{8}$$

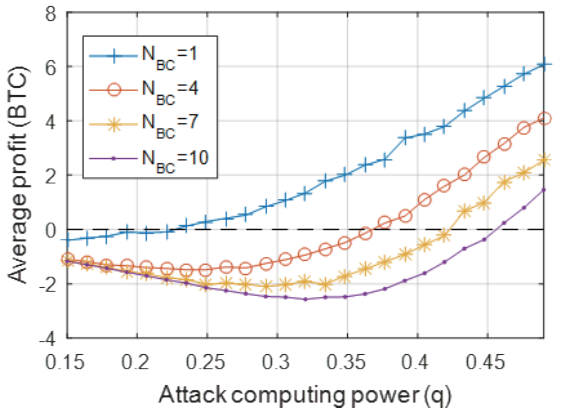
으로 표현 될 수 있다. 공격 대상 거래의 가치는 공격자가 상대 거래자 (피해자)와의 합의를 통해 함께 결정한다.

식 (6)의 이윤을 계산하기 위해 남은 변수는 랜덤 변수인 공격성공 소요시간 T_{AS} 이다. 랜덤 변수 T_{AS} 의 정확한 확률 분포는 [참조문헌 6의 Proposition 4]에서 계산되었으며, 본 논문에서는 T_{AS} 를 Monte-Carlo 실험으로 측정하였다. 실험을 위해, MATLAB상에서 두 개의 독립적인 Poisson counting process (PCP)를 구현하였다. 두 개의 PCP는 각각 공격자와 채굴자가 생성한 블록들의 생성 시간을 나타내며, 평균 블록생성 시간에 영향을 받는다. 공격자 PCP의 평균 블록생성 주기는 D_A 이며 채굴자 PCP의 평균 블록생성 주기는 D_H 이다. 중단 시간 t_{cut} 까지의 두 PCP의 블록생성 시간들을 실현 (realization) 한 후, 두 PCP를 비교하여 이중지불 공격의 두 가지 성공 조건이 달성유무를 판단하였다. 식 (7)의 지출을 계산하기 위해, 만약 이중지불 공격이 성공하였다면, PCP로부터 성공 시간 T_{AS} 를 추출하여 대입하였으며, 만약 공격이 실패하였다면, t_{cut} 을 대입하였다. 마찬가지로, 식 (8)의 수익을 계산하기 위해 만약 이중지불 공격이 성공하였다면, $V(q) = v$ 로 계산하였고, 그렇지 않을 경우 $V(q) = 0$ 으로 계산하였다. 이러한 일련의 과정을 5000번씩 반복한 후 계산 결과들에 평균을 취하였다.

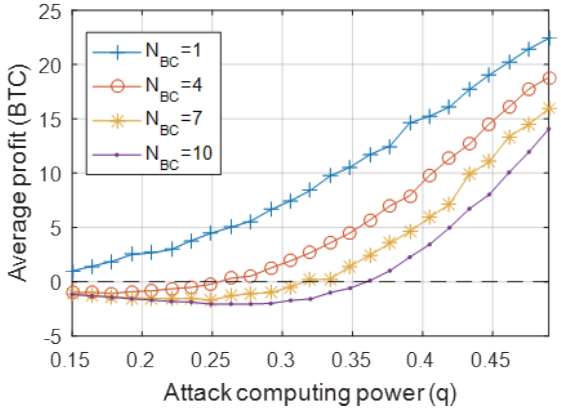
그림 5는 이중지불공격 실험 결과를 보여준다. 실험에 사용된 블록체인 네트워크 파라미터는 블록생성 평균비용 $\gamma = 0.33$ BTC와 블록생성 평균주기 $D_H = 600$ 초이며, 이는 2018년 12월 기준의 BitcoinCash 네트워크의 파라미터와

같다. 중단 시간 $t_{cut} = 12000$초로 설정하였다. 그래프는 다양한 이체확인 수 (N_{BC})와 다양한 공격대상 거래가치 (v)에 대해 이중지불 공격의 표본평균 이윤을 공격자의 컴퓨터 자원 (q)의 함수로 나타내었다.

그림 5로부터 공격자의 컴퓨터 자원이 네트워크 채굴자의 컴퓨터 자원보다 적은 경우, 즉 $q < p$ 인 경우에도 이중지불 공격에서 이윤을 기대할 수 있음을 알 수 있다. 다시 말해, 50% 이상의 컴퓨터 자원을 사용하는 이중지불공격뿐만 아니라 50% 미만의 컴퓨터 자원을 사용하는 이중지불공격도 위협적이다. 그래프는 이중지불 공격에 이윤을 가져다 주기 위한 공격대상의 거래가치 (v)의 요구조건이 이체확인 수 (N_{BC})가 커질수록 증가함을 보여준다. 즉, 가치가 큰 거래가 50% 미만 이중지불공격으로부터 안전하기 위해서는 충분히 큰 N_{BC}가 필요함을 보여준다. 수익성이 있는 50%미만 이중지불공격을 위한 공격대상 거래가치에 대한 정확한 조건은 [참조문헌6의 Theorem 8]에서 계산되었다.



(a) 거래가치 BTC



(b) 거래가치 BTC

〈그림 5 다양한 거래가치와 이체확인 수에 대한 50% 미만 이중지불 공격의 평균 이윤〉

VI. 결론

이중지불공격에 관한 기존 문헌들은 공격자의 컴퓨터 자원이 네트워크 채굴자의 컴퓨터자원보다 더 클 때, 즉 공격자가 전체 컴퓨터 자원의 50% 이상을 보유해야만 이중지불 공격이 성공 할 수 있다는 것을 보였다. 이러한 이유로 이중지불 공격은 51% 공격으로 알려져 왔다. 반면 본 논문에서는 50% 미만의 컴퓨터 자원을 사용하는 이중지불공격, 즉 50%미만 공격의 위험성을 분석하였다. 대규모 시뮬레이션을 통해 50% 미만의 컴퓨터 자원을 사용하는 이중지불공격도 공격자에게 큰 이윤을 가져다 줄 수 있음을 보였다. 구체적으로는, 거래자가 설정하는 이체확인 수가 작을수록 이중지불공격의 이윤이 커짐을 보였다. 다시 말해, 이체확인 수가 작을수록 거래의 처리속도는 빠르지만 50%미만 공격에는 매우 취약하다. 본 논문의 실험 결과는 블록체인의 거래자가 거래 가치와 이체확인 수를 결정하는 것에 관한 가이드라인을 제공 할 수 있다.

Acknowledgement

이 논문은 2019년도 광주과학기술원의 재원으로 GRI(GIST연구원) 사업의 지원을 받아 수행된 연구임. 이 논문은 2019년도 광주과학기술원의 재원으로 "과학기술응용연구단의 실용화 연구개발사업"의 지원을 받아 수행된 연구임.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] C. Osborne, "Bitcoin Gold suffers double spend attacks, $17.5 million lost," ZDNet, 25-May-2018. [Online]. Available: https://www.zdnet.com/article/bitcoin-gold-hit-with-double-spend-attacks-18-million-lost.

[3] "ZenCash Statement on Double Spend Attack," Horizen, 03-Jun-2018. [Online]. Available: https://blog.zencash.com/zencash-statement-on-double-spend-attack/.

[4] A. Hertig, "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular," CoinDesk, 08-Jun-2018. [Online]. Available: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/.

[5] M. Rosenfeld, "Analysis of Hashrate-Based Double Spending," arXiv:1402.2009 [cs], Feb. 2014.

[6] J. Jang and H.-N. Lee, "Profitable Double-Spending Attacks," submitted to IEEE Transactions on Information Forensics and Security, Mar. 2019. Available: arXiv:1903.01711 [cs]
[7] G.-T. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," Journal of Information Processing Systems, vol. 14, no. 1, pp. 101 - 128, 2018.
[8] A. Papoulis and S. U. Pillai, "Random walks and other applications," in Probability, Random Variables and Stochastic Processes, 4th edition., Boston, Mass.: McGraw-Hill Europe, 2002.
[9] W. Feller, "Random walk and ruin problems," in An introduction to probability theory and its applications, New York: Wiley, 1968.

Biographies



장재혁

2014년: 금오공과대학교 전자공학 학사
2016년: 광주과학기술원 정보통신공학 석사
2016년~현재: 광주과학기술원 전기전자컴퓨터공학 박사과정
관심분야: 블록체인, 신호 및 시스템, 압축센싱, 레이더
E-mail: jjh2014@gist.ac.kr



Heung-No Lee

Heung-No Lee (SM'13) received the B.S., M.S., and Ph.D. degrees from the University of California, Los Angeles, CA, USA, in 1993, 1994, and 1999, respectively, all in electrical engineering. He then worked at HRL Laboratories, LLC, Malibu, CA, USA, as a Research Staff Member from 1999 to 2002. From 2002 to 2008, he worked as an Assistant Professor at the University of Pittsburgh, PA, USA. In 2009, he then moved to the School of Electrical Engineering and Computer Science, GIST, Korea, where he is currently affiliated. His areas of research include information theory, signal processing theory, communications/networking theory, and their application to wireless communications and networking, compressive sensing, future internet, and brain-computer interface. He has received several prestigious national awards, including the Top 100 National Research and Development Award in 2012, the Top 50 Achievements of Fundamental Researches Award in 2013, and the Science/Engineer of the Month (January 2014).
E-mail: heungno@gist.ac.kr

Inter-Chain 기술 동향

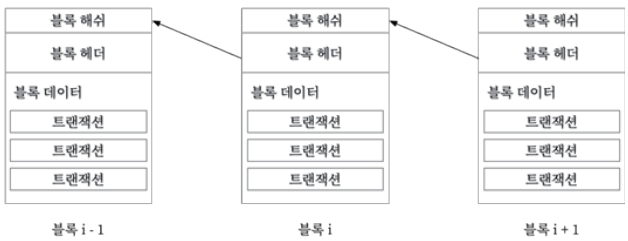
김준희, 김중헌
중앙대학교

Abstract

본 논문은 이기종 간의 블록체인 네트워크를 통합하여 관리할 수 있는 Inter-Chain 기술에 대해서 소개한다. 다양한 블록체인 네트워크들이 각자의 관심 서비스를 바탕으로 하여 제안됨에 따라 여러 서비스들의 통합된 메타 서비스가 필요할 경우에 이를 다룰 수 있는 기술이 필연적으로 필요하며 따라서 Inter-Chain기술이 필수불가결하게 필요하게 된다. 따라서 해당 기술에 대해서 깊게 알아보고 현재 존재하는 주된 기술에 대해서 논하며 주된 연구 주제에 대해서 알아보도록 한다.

I. 서론

사토시 나카모토(Satoshi Nakamoto)의 비트코인(Bitcoin)의 등장으로 탈중앙화를 특징으로 하는 블록체인(Blockchain) 기술에 관심이 높아졌다 [1]. 이에 따라 블록체인에 대한 다양한 연구가 진행되고 있다. 블록체인은 분산 원장 기술로, 어떤 주체의 도움없이 거래 정보 등의 데이터를 공개하여 다수가 함께 관리하는 분산 컴퓨팅 기술의 한 종류다 [2]. 그림 1과 같은 체인 형태로 데이터가 저장되어 임의로 수정할 수 없으며, 모든 거래 정보를 네트워크의 노드들이 함께 관리한다. 따라서 투명성이 보장되고 결과적으로 탈중앙화를 이룰 수 있다는 점에서 큰 인기를 얻었다.



〈그림 1. 블록의 체인 구조〉

블록체인 기술은 크게 퍼블릭 블록체인과 프라이빗 블록체인의 두 가지 종류로 나뉜다. 퍼블릭 블록체인(Public Blockchain)은 누구나 자유롭게 참여할 수 있는 블록체인이다. 트랜잭션(Transaction) 내역과 네트워크의 동작이 모두 공개되고 누구나 거래 기록의 묶음인 블록(Block)을 생성할 수 있다. 현재 비트코인(Bitcoin), 이더리움(Ethereum), 이오스(EOS) 등과 같은 예가 대표적이다. 프라이빗 블록체인(Private Blockchain)은 네트워크 주체 등으로부터 허가된 노드만 참여할 수 있는 블록체인 네트워크이다 [3]. 이렇게 인증된 노드 만이 거래 내역을 확인하거나 블록을 생성할 수 있다. 대표적인 예로 하이퍼레저 패브릭(Hyperledger Fabric), 리플(Ripple) 등이 있다.

그러나 블록체인은 아직 해결해야할 여러 문제점이 존재한다. 블록체인에서 어떤 거래 내역이 처리되려면 해당 트랜잭션이 포함된 블록이 생성될 때까지 기다려야 한다. 이와 같은 문제로 여러 서비스들이 상대적으로 속도가 빠른 프라이빗 블록체인을 사용하여 개발/출시됐지만 근본적인 문제를 해결하지 못했다. 더불어 확장성(Scalability)에서도 주요한 문제가 존재한다. 블록의 크기가 고정되어 있어 네트워크 노드 수가 증가하고 사용자 수가 많아지면 데이터 크기가 방대해져 트랜잭션이 한 블록에 기록되기 힘들어지는 것을 의미한다.

블록체인 기술이 인기를 얻고 다양한 블록체인 네트워크가 구성되면서 다른 블록체인 네트워크와의 데이터 교환에 대한 필요성이 대두되었다. 각 도메인(Domain)에 특화된 블록체인 네트워크를 서로 엮어 새로운 블록체인 네트워크를 만들고 블록체인 간 데이터 교환을 가능하게 하는 인터체인(Interchain) 기술이 등장하였다 [4]. 따라서 본 논문에서는 이러한 인터체인 기술에 대해서 논하고자 한다.

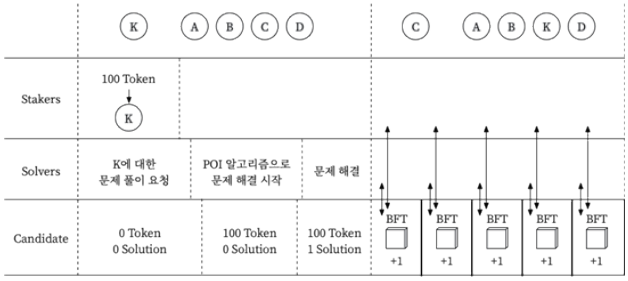
본 논문은 다음과 같이 구성되어 있다. 2장에서는 인터체인과 현재 동향에 대해 설명한다. 3장에서는 인터체인의 기술들에 대해 설명한다. 그리고 4장에서 결론을 내리며 본 논문을 마친다.

II. 인터체인(Interchain)

인터체인은 여러 블록체인 간의 데이터 교환을 위해 서로 다른 블록체인을 연결한 체인이다. 일반적인 블록체인 시스템에서 A 블록체인의 토큰을 이용하는 서비스는 오직 A 블록체인의 토큰으로만 이용이 가능하다. 그러나 인터체인을 활용하면 A 블록체인의 토큰만으로 이용할 수 있는 서비스를 B 블록

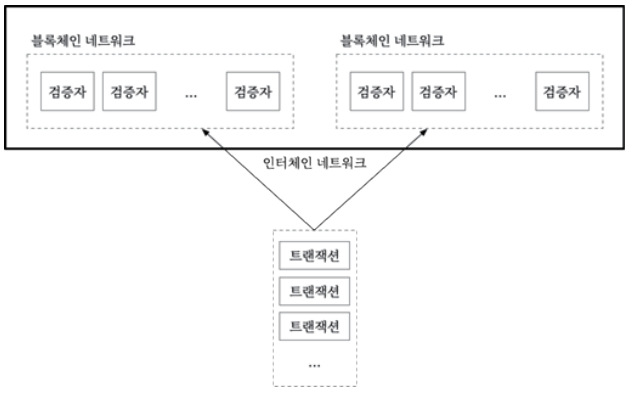
체인의 토큰으로도 사용할 수 있게 된다. 이렇게 인터체인은 각자 다른 목적과 특징을 가지고 분산화된 블록체인을 연결하여 확장성 문제를 해결하고 상호운용성(Interoperability)을 높이고자 등장하였다.

인터체인의 중요한 요소는 인터체인 네트워크에 포함될 수 있는 블록체인네트워크를 선별하는 것과 각 네트워크가 동일한 내용의 블록을 생성할 수 있도록 합의 알고리즘을 구성하는 것이다. 블록체인 간 연결을 통해 서로 데이터를 주고 받기 위해서 별도의 프로토콜을 정의해야 한다. 그리고 인터체인에 포함될 블록체인 네트워크는 이 프로토콜로 통신할 수 있어야 한다. 또, 각 블록체인이 같은 트랜잭션에 대해 동일하게 처리할 수 있도록 합의 알고리즘이 설계되어야 한다. Proof of Work (PoW) 등과 같은 알고리즘은 각 블록체인의 블록 생성자나 블록 데이터가 서로 다를 수 있기 때문에 인터체인의 합의 알고리즘으로는 적합하지 않다. 이와 같은 이유로 대부분 Byzantine Fault Tolerant (BFT) 계열의 블록체인이 인터체인 대상으로 연구되고 있다.



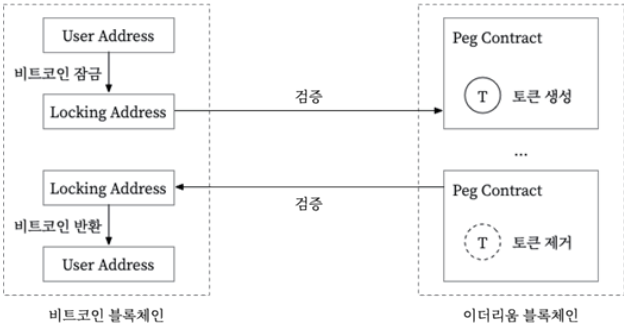
〈그림 2. AION의 검증자 선발 및 운영 방식〉

인터체인은 각 블록체인 네트워크 사이에서 서로 주고받고자 하는 트랜잭션에 대한 검증을 필요로 한다. 이를 위해 각 블록체인의 검증자가 필요하게 된다. 검증자의 선발 기준과 검증에 대한 인센티브는 각 블록체인이 고려해야 할 중요한 요소다. 이와 같은 이유로 그림 2의 AION과 같이 인터체인의 검증자는 복잡한 검증자 선발 방식을 거친다 [5].



〈그림 3. 인터체인을 통한 TPS 향상〉

인터체인 네트워크를 사용하면 서로 다른 블록체인끼리 트랜잭션을 교환할 수 있을 뿐만 아니라 기존의 블록체인이 가지고 있던 속도 문제를 어느 정도 해결할 수 있다. 블록을 생성할 때, 단순히 네트워크 안의 검증자 수를 늘리는 것 만으로는 속도 향상의 한계가 있다. 그러나 그림 3과 같이 동일한 블록체인 네트워크를 추가하고 인터체인으로 묶으면 트랜잭션에 대한 Transaction Per Second (TPS)를 높일 수 있어 속도를 향상시킬 수 있다. 뿐만 아니라 이미 사용중인 블록체인으로 인터체인 내의 다른 블록체인을 사용할 수 있고, 독립된 블록체인끼리 데이터를 주고 받을 수 있다. 더불어 다른 블록체인의 데이터를 조회하는 것도 가능해진다.

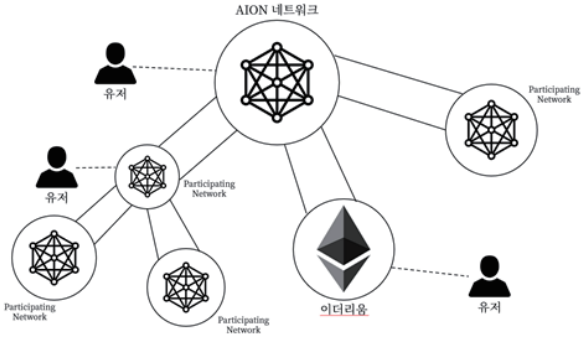


〈그림 4. 비트코인과 이더리움을 이용한 투 웨이 페깅〉

인터체인은 보통 브릿지(Bridge) 혹은 릴레이(Relay) 등이라 불리는 연결 다리를 통해 블록체인을 연결한다. 만약 A에서 B로 트랜잭션을 보낼 때 중간의 허브가 이를 검증하도록 한다. 다른 블록체인끼리 코인을 교환할 때는 그림 4와 같은 투 웨이 페깅(Two Way Pegging) 방식을 사용한다. 이는 사용되는 블록체인의 코인에 해당하는 가치만큼 사용하려는 블록체인의 코인 가치로 환산된다. 트랜잭션을 통해 코인이 사용되면 기존 블록체인의 코인이 사용되도록 하여 다른 블록체인에서도 원하는 블록체인의 암호화폐로 서비스를 이용할 수 있다 [6].

III. 인터체인 기술 현황

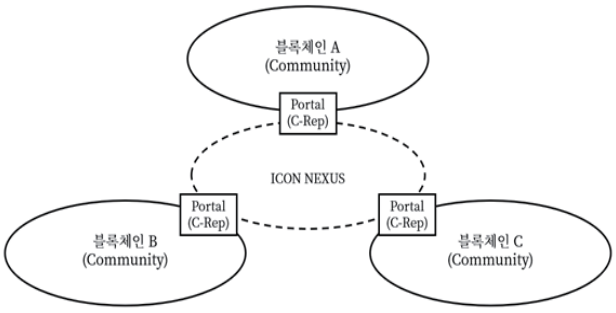
3.1 AION



〈그림 5. AION Network 구성도〉

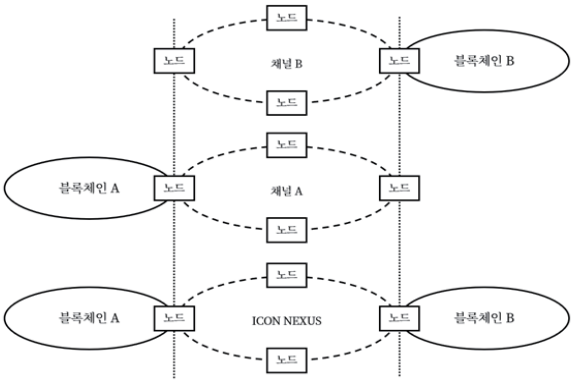
인터체인에 대해 크게 3가지 프로젝트가 활발하게 연구되고 있다. AION은 3세대 블록체인으로 이더리움과 AION 내 블록체인 간의 데이터 교환을 목표로 하는 인터체인이다. 빠르고 큰 데이터를 사용할 수 있는 탈중앙화된 프로토콜을 제시한다. AION 블록체인 네트워크는 그림 5와 같이 Connecting Network, Participating Network, Interchain Transaction, Bridge로 구성된다 [5]. AION의 Connecting Network은 이더리움 혹은 다른 블록체인 네트워크 간의 커뮤니케이션을 위해 존재한다. 블록체인 간의 데이터 교환을 위한 인터페이스를 제공하고 메시지가 잘 전달될 수 있는지 검증하는 역할을 한다. Participating Network는 AION에 참여하는 블록체인 네트워크로서 Connecting Network가 제공하는 인터페이스를 맞출 수 있는 블록체인이어야 한다. 요구하는 인터페이스를 만족시키지 못하는 블록체인 네트워크는 AION 인터체인에 참여할 수 없다. Interchain Transaction은 AION의 트랜잭션을 위한 일종의 메시지로 상호작용하고자 하는 블록체인에 트랜잭션을 전송하는 데에 사용된다. Bridge는 Connecting Network 혹은 Participating Network 간의 트랜잭션을 전송하는 프로토콜이다. Bridge는 트랜잭션의 서명을 확인하고 수수료가 올바른지 검증한다. 여러 검증자로 구성된 Bridge는 Lightweight BFT 기반의 합의 알고리즘을 사용하며 검증을 완료한다. AION은 트랜잭션에 대한 수수료로 AION 토큰을 이용하도록 하여 블록체인 간 트랜잭션 교환의 인센티브로 활용한다.

3.2 ICON



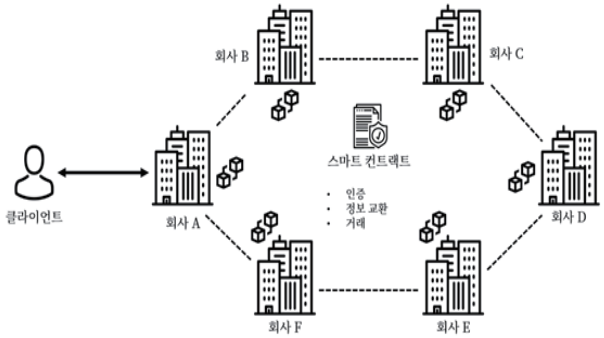
〈그림 6. ICON 블록체인 구조〉

또 다른 인터체인으로 한국에서 진행중이며, 중간 연결 다리 없이 블록체인을 연결하는 것을 목표로 하는 ICON이 있다. 이는 이미 구축된 프라이빗 블록체인 시스템을 인터체인에 활용할 수 있고 거래가 빠르다는 장점을 가지고 있다. ICON은 그림 6과 같이 C-Node, Community, C-Rep, Nexus, Portal, Blockchain Transmission Protocol (BTP) 등으로 구성된다 [7]. C-Node는 ICON 내 블록체인 네트워크의 노드로 해당 블록체인의 합의 과정과 거버넌스에 참여한다. Community는 ICON 인터체인에 참여하는 블록체인 네트워크를 의미하며 C-Node들로 구성된다. C-Rep은 Community에 속하면서 ICON 블록체인 네트워크에 참여한다. ICON에서 발생하는 거래에 대한 검증을 진행하며 이에 따른 인센티브를 받는다. Nexus는 각 블록체인 네트워크, 즉 Community를 연결하는 블록체인으로 C-Rep이 Nexus의 노드가 된다. C-Rep은 BFT 기반의 Loop Fault Tolerance (LFT) 합의 알고리즘을 사용하여 블록을 생성한다. Nexus는 ICON Exchange (ICX) 토큰을 사용하여 트랜잭션에 대한 수수료를 지불할 수 있도록 한다.



〈그림 7. Nexus의 멀티 채널 기능〉

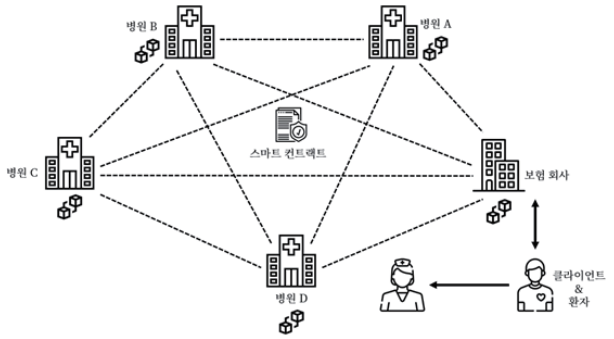
Nexus는 그림 7과 같은 다중 채널(Multi-Channel)을 지원하여 각 블록체인 별로 Channel을 사용할 수 있다. Nexus는 Community의 노드가 되어 해당 블록체인의 거래 내역을 확인할 수 있다. Portal은 Community와 Nexus를 연결하며 BTP 통신을 사용한다. 각 Community의 정책에 따라 Portal은 자체적인 합의 네트워크를 구성할 수 있다. BTP는 Community와 Nexus의 트랜잭션 교환을 위한 프로토콜이다.



〈그림 8. SCORE를 이용한 ICON 블록체인 환경〉

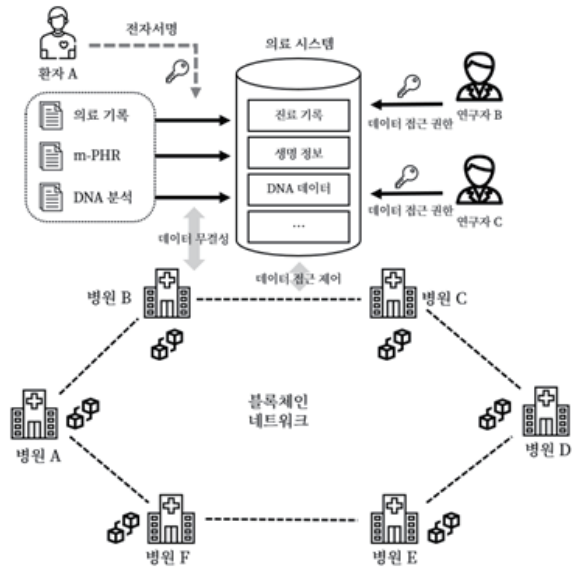
ICON은 SCORE라는 스마트 컨트랙트(Smart Contract) 환경을 제공하여 인증, 거래 등의 업무에 대한 블록체인 네트워크를 구축할 수 있다. 그림 8과 같이 안전하다고 인증 받은

회사들의 블록체인을 연결하고 스마트 컨트랙트를 이용하여 탈중앙화되고 자동화된 비즈니스 프로세스를 가능케 한다.

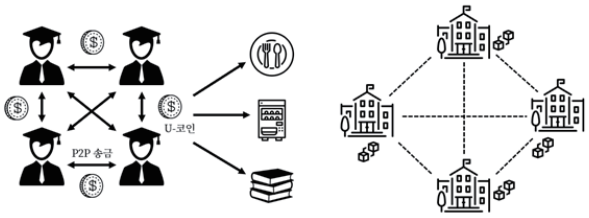


〈그림 9. ICON을 이용한 병원-보험 블록체인 환경〉

이 외에 ICON은 그림 9와 같은 병원-보험 블록체인 네트워크에도 사용될 수 있다. 병원에서 개인정보를 이용한 업무는 병원 블록체인에서 진행하고 이에 대한 보험 업무는 보험 블록체인에서 수행하여 보험금 청구에 대한 자동화를 지원한다.



〈그림 10. ICON을 활용한 의료 블록체인 시스템〉

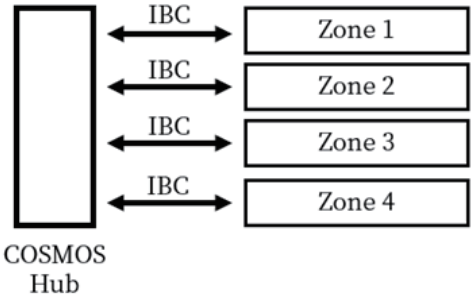


〈그림 11. ICON을 이용한 대학 블록체인 시스템〉

또, 그림 10, 그림 11과 같이 의료, 교육 등 넓은 분야에 사용하여 블록체인의 상호운용성을 높일 수 있다.

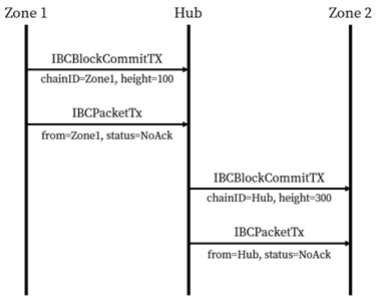
3.3 COSMOS

COSMOS는 Inter-Blockchain Communication (IBC) 프로토콜을 통해 블록체인 간 상호 통신이 가능하게 하는 블록체인 네트워크다. 기본적으로 PBFT 알고리즘의 합의 알고리즘을 기반으로 하지만 이더민트와 같은 이더리움을 위한 빠른 성능의 합의 알고리즘을 지원하여 범용성이 높은 이더리움과의 데이터 교환을 지원한다.



〈그림 12. COSMOS 블록체인 구조〉

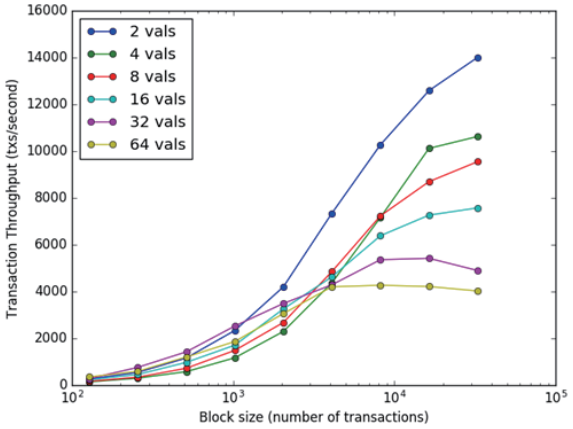
COSMOS는 크게 Zone과 Hub로 구성된다. Zone은 각각의 독립된 블록체인 네트워크를 의미하며 IBC 메시지를 통해 데이터를 교환한다. Hub는 다중 자산(Multi-Asset) 분산 원장을 관리하는 블록체인 네트워크로 COSMOS 블록체인 전체를 관리한다 [8].



〈그림 13. IBC 프로토콜〉

Zone 간의 트랜잭션 교환을 위해선 지분(Stake) 기반의 토큰을 사용해야 한다. IBC 프로토콜은 그림 13과 같이 2가지의 트랜잭션을 교환하는 방식으로 전파된다. 송신자는 먼저 최신 블록 해시를 전송하여 자신을 증명할 수 있도록 한다. 그 다음, 전송하려는 데이터 패킷에 대해 머클 증명(Proof of Merkle)을 사용하여 패킷 전송을 증명할 수 있도록 한다.

COSMOS는 텐더민트(Tendermint) 프로토콜을 사용하여 합의 알고리즘을 진행한다. 이는 PBFT 기반의 합의 알고리즘으로 단순하고 빠른 성능을 보인다 [9]. 텐더민트는 지분 기반으로 검증자들을 선발한다. 이렇게 선발된 검증자들만이 합의에 참여한다. 이들은 Propose, Prevote, Precommit과 같은 3단계의 프로세스를 거쳐 검증자의 2/3를 초과하는 인원이 동의할 경우 합의가 이루어지고 블록이 생성된다.



〈그림 14. 검증자 수에 따른 성능 그래프 [8]〉

그림 14와 같이 텐더민트는 검증자 수가 증가할수록 성능이 저하되는 단점을 가지고 있지만, 충분한 검증자 수를 유지하면 안정적으로 동작할 수 있다. 또, 검증자를 선발하는 알고리즘에 따라 퍼블릭 블록체인과 프라이빗 블록체인 모두를 구현할 수 있다는 장점을 가지고 있다.

IV. 결론

인터체인 기술은 블록체인 생태계가 소수의 플랫폼 위주로 돌아가는 것보다 다양한 블록체인이 공존할 수 있는 것을 목표로 발전하고 있다. 네트워크가 Internet과 TCP/UDP 프로토콜로 발전했듯이 인터체인과 BTP, IBC 등의 기술이 블록체인을 한 걸음 더 발전시킬 수 있을 것이다. 인터체인을 통해 중개자 없이 안전하게 블록체인 간 데이터 교환을 이루기 위해선 여러 기술의 발전과 표준화가 필수적이다. 실제로 ISO, ITU 등의 기구에서 블록체인 기술 표준화에 대해 논의 중에 있다. 복잡한 기술로 접근성이 낮은 블록체인이 표준화되고 인터체인을 통해 사용 편의성을 높이면 블록체인을 여러 분야에 활용하기 더 용이할 것이다.

Acknowledgement

본 연구는 한국연구재단 신진연구자지원사업(2016R1C1B1015406)의 지원으로 수행되었음(교신저자: 김중헌)

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, www.cryptovest.co.uk, October 2008.
[2] X. Xu et al., “The Blockchain as a Software Connector,” 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA) pp. 182-191, 2016.
[3] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. Weed Cocco, and J. Yellick, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”, ArXiv e-prints, January 2018.
[4] L. Kan, Y. Wei, A. H. Muhammad, W. Siyuan, G. Linchao, and H. Kai., “A multiple blockchains architecture on inter-blockchain communication”, IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pages 139 - 145, July 2018.
[5] Matthew Spoke, Nuco Engineering Team, “AION: Enabling the decentralized Internet”, AION White Paper, July 2017.
[6] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille, “Enabling Blockchain Innovations with Pegged Sidechains”, m http://www.blockstream.com/sidechains.pdf, October 2014.
[7] ICON Foundation, “ICON: Hyperconnect the World”, ICON White Paper, August 2017.
[8] Jae Kwon, Ethan Buchman, “COSMOS: A Network of Distributed Ledgers”, COSMOS White Paper, January 2019.
[9] Ethan Buchman, “Tendermint: Byzantine Fault Tolerance in the Age of Blockchains”, Master’s thesis, University of Guelph, June 2016.

Biographies



김준희
2019년: 중앙대학교 컴퓨터공학부 학사
2019년~현재: 중앙대학교 컴퓨터공학과 석사과정
관심분야: Distributed System, Security, Blockchain
E-mail: jhkim.cau@gmail.com



김중헌
1999년~2006년: 고려대학교 컴퓨터학과 학사/석사
2009년~2014년: USC 박사
2006년~2009년: LG전자 우면R&D캠퍼스, 주임연구원
2013년~2016년: Intel Corporation USA, Systems Engineer
2016년~현재: 중앙대학교 소프트웨어학부 조교수
E-mail: joongheon@gmail.com

블록체인 기반의 ID 관리 기술 동향

김석현, 조영섭, 김수형
ETRI

Abstract

기존의 ID 관리 기술은 사용자의 개인정보가 중앙집권형으로 관리되어 사용자의 자기 정보 통제 기능이 미흡하고 개인정보 유출 및 오남용 문제를 가지고 있다. 이러한 문제를 해결하기 위해 최근 연구되고 있는 분산원장 기술을 이용한 ID 관리 기술은 사용자 스스로 자신의 ID 정보 및 디지털 자산을 완벽하게 제어하는 자기주권 ID 관리 기술을 제공하여 자신이 누구인지 증명할 수 있고 자신의 ID를 직접 제어할 수 있다. 본 고에서는 이러한 블록체인 기반의 ID 관리 기술에 대한 동향과 관련 기술에 대해서 기술한다.

I. 서론

사용자의 신원(Identity, ID)은 온라인뿐만 아니라 오프라인에서 발생하는 거의 모든 상호작용에서 매우 중요하다. 이는 본인을 증명할 수 있는 ID가 없다면 공공 서비스는 물론 금융이나 의료 등의 서비스를 제공받기 어렵기 때문이다.

현재 전 세계의 국가 및 지역에서 공적인 ID를 가지지 못한 사람의 수는 11억 명이다. 이런 사회적인 문제를 해결하고자 2017년 6월 UN 본부에서 'ID2020 Summit'이 개최되었고 민관 공동으로 디지털 ID의 발행에 노력하기로 발표하였다[1]. ID2020은 디지털 ID 인증으로 사람들의 삶을 개선하고자 하는 글로벌 연합으로 블록체인을 통해 사용자 스스로 자신의 정보를 소유하고 통제할 수 있는 데이터베이스와 새로운 형태로 만들어질 인증에 대한 시스템을 구축하는 것을 목표로 가지고 있다. 디지털 ID를 발행하기 위한 방법으로 블록체인 기술을 채택하고 있는 것은 블록체인이 거래정보를 공동으로 관리하는 분산원장(Distributed Ledger Technology, DLT) 공유 기술을 적용하여 중재자 없는 신뢰 프로세스를 구축할 수 있기 때문이다.

본 고에서는 이러한 블록체인 기반으로 연구되고 있는 ID 관리 기술에 대한 동향을 살펴볼 것이다. 본 고는 다음과 같이 구성되어 있다. 2장에서는 블록체인 기술에 대한 개념 및 종류, 세대별 특징을 알아본다. 3장에서는 블록체인 기반에 ID 관리 연구의 필요성 및 현재 연구 개발되고 있는 기술을 소개한다. 4장에서는 본인이 정보를 소유하고 통제하는 자기주권 신원 (Self-sovereign identity) 관리 기술에 대한 개념과 관련 기술을 설명하고, 5장에서 결론을 내린다.

II. 블록체인 기술 개요

2.1 블록체인

블록체인은 P2P(Peer-to-Peer) 네트워크에서 디지털 거래정보를 공동으로 관리하는 분산원장 공유 기술로 네트워크의 모든 참여자가 공동으로 거래 정보를 검증, 기록, 보관할 수 있는 기술이다. 블록체인의 대표적인 특징은 중재자가 없이 디지털 정보에 대한 보안 관리가 가능한 신뢰 프로세스를 구축할 수 있다는 것이다[2]. 블록체인은 기술적으로 중앙 서버 없이 'P2P로 구현된 비가역적(Irreversible)인 공유 데이터베이스'로 볼 수 있다. 즉, P2P 방식으로 이루어진 네트워크에서 참여자(Node, Client)들은 데이터를 담은 블록을 생성하고 서로 검증한다[3]. 각 참여자들은 어느 한 거래 정보가 변경되면 전체 블록체인의 해시(Hash) 값이 변경 되는 특징으로 특정 노드가 임의로 정보를 조작하는 것을 불가능하게 함으로써 정보의 무결성을 유지한다. 또한 P2P 네트워크를 통한 완전한 정보 공유로 인해서 전체 시스템이 중단되는 '단일 장애점(Single Point of Failure)' 위험에도 대비할 수 있다[4]. 또한 '스마트 계약(Smart Contract)'을 이용하여 암호화폐를 뛰어넘어 모든 종류의 거래가 가능한 온라인 플랫폼으로 활용 가능하다.

2.2 블록체인의 종류

블록체인은 참여자의 범위에 따라 퍼블릭(Public), 프라이빗(Private), 하이브리드(Hybrid) 블록체인으로 분류할 수 있다.

퍼블릭 블록체인은 누구나 허가없이 참여할 수 있는 개방형 블록체인으로 인터넷에 연결된 PC, 노트북, 스마트폰 등 다양한 장치를 통해 참여할 수 있다. 블록체인을 운영하는 주체가 없기 때문에 블록체인 네트워크의 신뢰성을 유지해 주는 사용

자들에게 인센티브를 제공한다.

프라이빗 블록체인은 네트워크 운영자에게 허가를 받아 참여할 수 있는 허가형 블록체인으로 허가된 장비를 통해서만 참여할 수 있다. 프라이빗 블록체인에서는 네트워크 운영자가 명확히 존재하기 때문에 인센티브 지원이 반드시 필요하지는 않다. 프라이빗 블록체인은 기밀성과 속도가 강화된 모델이지만, 적은 사람들에 의해 합의가 진행되기 때문에 일부 중앙화가 발생하여 보안성이 낮아질 수 있다는 단점이 있다.

하이브리드 블록체인은 퍼블릭 블록체인과 프라이빗 블록체인을 동시에지원하는 형태의 블록체인이다. 예를 들어, 기밀성이 중요한 IoT 기기에는 프라이빗 블록체인을 이용하고, 자동화된 결제를 위해서는 퍼블릭 블록체인을 이용하는 방식이다.

2.3 블록체인 기술의 세대별 특징

블록체인 기술은 분산원장 공유 기술을 처음 도입하고 적용한 비트코인(Bitcoin)이 발표된 2009년부터 이더리움(Ethereum)이 발표되기 전 2015년까지를 1세대로 보고, 스마트 계약 기술을 활용한 이더리움이 다양한 분야에서 응용되는 현재까지의 시기를 2세대로 구분할 수 있다[5]. 그림 1은 블록체인 기술을 세대별로 구분하고 세대별 주요 특징 및 적용사례를 요약한 내용이다[6].

구분	1세대(2009~2014)	2세대(2015~현재)	3세대(향후)
주요 특징	○ 가상통화 ○ 자산 거래	○ 스마트계약(비즈니스 자동화) ○ 분산 앱(Decentralized Application)	○ 확장성(Scalability) ○ 블록체인 간 상호운용성(Interoperability) ○ IoT 지원
대표 사례	○ 비트코인	○ 이더리움 ○ 하이퍼레저	○ 다양한 블록체인 플랫폼 개발 중
개발 현황	도입기	확산기	성숙기

〈그림 1. 블록체인 기술에 대한 세대별 특징〉

1세대의 블록체인 기술은 주로 디지털 통화로 활용되어 개념적인 혁신성에도 불구하고 그 기술적 파급이 제한적이었으며 느린 거래 속도로 인해 기술의 응용이 한정적인 영역에 그쳤다. 2세대의 블록체인 기술은 사전에 설계한 조건에 따라 계약이 자동으로 수행되도록 구조화된 스마트 계약을 시스템에 채택한 이더리움이 등장하고 이를 기반으로 응용 사례인 디앱(DApp)들이 활발하게 상용화되고 있다. 현재는 기업의 업무 목적에 맞는 비즈니스 환경에 따라 기밀 유지와 확장성을 지원할 수 있는 프라이빗 블록체인 기반의 하이퍼러저 패브릭 (Hyperledger Fabric) 프레임워크가 다양한 분야에서 활용되고 있다. 3세대의 블록체인 기술은 기존 1, 2세대 블록체인의 기술적 한계점을 극복하는 블록체인 기술로서, 합의 알고리즘 개선과 시스템에 자체 의사결정 기능을 탑재하여 거버넌스 기능 강화 트랜잭션 처리 성능을 개선하여 확장성을 향상시키기 위한 연구가 진행될 것으로 예상된다.

표 2는 1세대와 2세대의 블록체인 기술로 대표되는 비트코인과 이더리움, 하이퍼레저 패브릭의 기술적인 특징을 요약한 내용이다[7].

표 1 비트코인, 이더리움, 하이퍼레저 패브릭에 대한 기술적 특징 비교

특징	비트코인	이더리움	하이퍼레저 패브릭
인센티브	비트코인	이더, 사용자가 생성한 암호화폐	없음
네트워크	공개	공개형 또는 허가형	허가형
거래	익명	익명 또는 비공개	공개 또는 비밀
합의	작업증명	작업증명(POW)	SOLO, Kafka, SBFT(지원예정)
스마트 계약	없음	있음(Solidity, Serpent, LLL)	있음(chaincode)
언어	C++	Golang, C++, Python	Golang, Java, Node.js

* POW(Proof of Work), SBFT(Simple Byzantine Fault Tolerance)
* SOLO: 단일 노드로 동작하는 것으로 주로 개발용으로 사용되는 방식
* kafka: 분산된 스트리밍 플랫폼이며 publish-subscribe(발생/구독) 모델을 사용

III. 블록체인 기반 ID 관리 기술

본 장에서는 블록체인 기반 ID 관리의 필요성과 현재 진행되고 있는 연구 내용에 대해서 기술한다.

3.1 블록체인 기반 ID 관리의 필요성

ID 관리(Identity Management) 기술은 적법한 개인이 적절한 시점에 올바른 자원(Resource)에 접근할 수 있게 하는 보안 분야 기술이다[8]. 기존의 ID 관리 기술은 일반적으로 ID 관리 서비스 제공자가 사용자의 개인정보를 수집하고 이용할 권한 등을 모두 허용할 것을 사용자에게 요구하고 수집된 사용자의 개인정보를 중앙 서버에 저장하고 관리한다. 반면 사용자는 자신의 개인정보의 유통 및 관리에 대해 통제할 수 있는 수단이 미흡하거나 존재하지 않는 경우가 대부분이다. 이와 같은 ID 관리 구조는 최근 카드사, 쇼핑몰, 게임회사 등 대기업이 보유한 사용자의 개인정보가 유출 또는 불법 유통되는 문제가 발생하는데 주요한 원인이 되었다. 즉, 기존 ID 관리 기술은 사용자의 개인정보가 중앙집중형으로 관리되고 사용자가 자신의 개인정보에 대한 통제 능력이 없으며 개인정보 유출 및 오남용에 대한 문제에 항상 노출되는 문제를 가지고 있다 [9].

이와 같은 문제를 해결하기 위해 최근 블록체인의 분산원

장 기술을 이용한 새로운 ID 관리 기술이 연구되고 있다. 이 기술은 사용자가 자신의 ID 정보 및 디지털 자산을 완벽하게 제어하는 자기주권 신원 관리 기술을 제공하여 사용자 스스로 자신이 누구인지 증명할 수 있고 데이터를 직접 제어할 수 있도록 한다. 즉, 블록체인 기반의 ID 관리를 지원하는 DApp(Decentralized App)을 이용하면, 기존의 ID 관리 시스템이 가지고 있던 문제를 해결할 수 있다. 사용자는 자신의 ID 정보를 통제할 수 있는 권한을 가지게 되므로 서비스 제공자로부터 개인정보가 오남용되거나 거래되는 것을 방지할 수 있고, 자신의 ID 정보를 서비스 제공자에게 위탁하지 않고도 ID 정보를 제공하고 증명받을 수 있기 때문에 서비스 제공자들로부터 발생되는 정보유출 문제에서도 자유롭다[10].

3.2 블록체인 기반 ID 관리 기술 동향

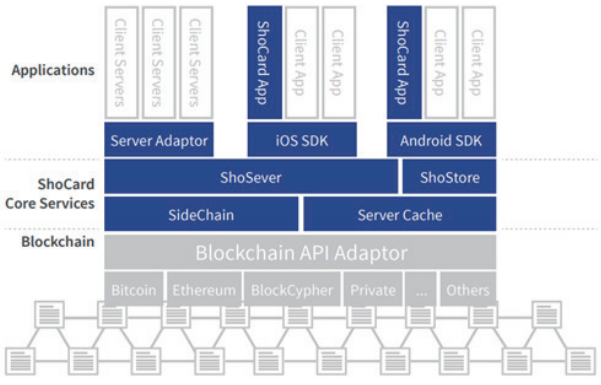
본 장에서는 현재 연구되고 있는 블록체인 기반의 ID 관리 기술에 대하여 기술한다.

Dunphy와 Petitcolas[11]는 블록체인 기반 ID 관리 기술을 크게 자기주권 ID(Self-Sovereign Identity) 기술과 분산형 신뢰 ID(Decentralized Trusted Identity) 기술로 분류하였다. 자기주권 ID은 외부의 행정 기관에 의존할 필요가 없고 ID 정보가 유출될 가능성이 없는 소유자에 의해서 관리되고 제어되는 ID을 의미하고, 대표적으로 Sovrin이 여기에 속한다. 분산형 신뢰 ID는 기존의 신뢰할 수 있는 ID(예: 여권)을 기반으로 사용자의 신원을 증명하는 것은 중앙집중형 서비스가 처리하고, 추후 제 3의 기관에 의한 유효성 검증을 위해서 신원 입증(Identity Attestation)을 분산원장에 기록하는 방식이다. 대표적으로 ShoCard가 여기에 속한다. 표 2는 자기주권 신원과 분산형 신뢰 신원으로 구분 가능한 기술들을 정리한 내용이다.

표 2 블록체인 기반의 ID 관리 기술 분류

분류	기술명	설명
분산형 신뢰 신원	ShoCrad	블록체인 기반의 다중 요소 인증을 통한 ID 관리 서비스를 제공하는 플랫폼
	ID2020	2020년까지 지구상 모든 사람들에게 디지털 ID을 제공하고자 하는 UN의 컨소시엄 프로젝트
	Trust Stamp	소셜 미디어 및 기타 공개적으로 사용 가능한 데이터를 사용하여 ID 정보를 확인하고 고유한 신뢰 점수를 제공하는 기술
	Bitnation	온라인 상의 가상 국가이고, 분산되고 국경이 없는 자발적인 국가를 목표로 하는 플랫폼
	e-residency	에스토니아 공화국이 만든 세계 시민을 위한 디지털 국가이고, 정부는 회사 설립, 은행, 결제 처리 및 세금과 같은 에스토니아 서비스에 접근할 수 있는 디지털 ID를 발행하는 플랫폼
자기주권 신원	Sovrin	정보를 개인 또는 조직이 소유하고 제어하는 새로운 ID 관리 기술
	Blockstack	사용자가 자신의 ID 정보를 소유할 수 있도록 디지털 키 정보를 제공하는 오픈 소스 기반에 블록체인 응용 프로그램
	Uport	사용자가 자신의 ID정보과 개인정보를 제어할 수 있는 자기주권 신원이 가능한 최초의 ID 관리 시스템

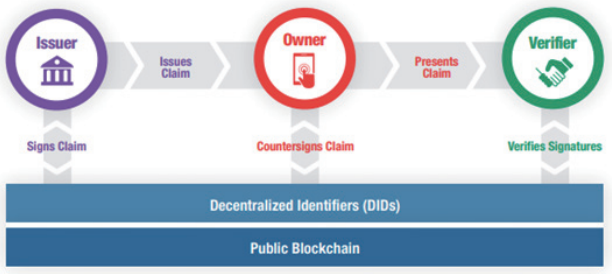
- ShoCard는 사람들이 디지털 ID을 소유하고 보호할 수 있는 블록체인 기반의 ID 관리 시스템이다. ID 정보를 공유할 사람과 시기를 결정할 수 있고, 다른 신뢰 기관이 ID 정보를 보증하지 않아도 블록체인을 사용하여 ID 정보의 신뢰성을 확인할 수 있다. ShoCard ID 관리 플랫폼은 조직 및 개인에게 3가지 기능을 제공한다. 개인 또는 기관에 대한 인증 기능, 감사가 가능한 권한 부여, 개인 크리덴셜(Credential) 교환 기능을 제공한다. 이 플랫폼은 iOS와 Android를 모두 지원하는 소프트웨어 개발 키트(SDK)를 통해 모바일 Apps 및 서버에 통합되도록 설계되어 있다. 그림 2는 ShoCard에 대한 아키텍처를 나타낸다. ShoCard 아키텍처는 퍼블릭 블록체인의 성능에 얽매이지 않고 높은 처리량의 트랜잭션을 제공하도록 설계되어 있어서 30분 이내에 작업 증명(proof of work)으로 5백만 명 이상의 신규 사용자를 만들고 인증할 수 있다. 또한 동시에 여러 개의 블록체인을 사용할 수 있으며 앞으로 프라이빗 블록체인을 포함하여 새로운 블록체인을 적용할 수 있다. 그리고 개인 식별 정보의 해킹을 방지하기 위해 ShoCard 시스템은 데이터를 검증하기 위해서만 블록체인을 이용하고 개인 식별 정보는 블록체인에 저장하지 않는다[12].



〈그림 2. ShoCard 아키텍처〉

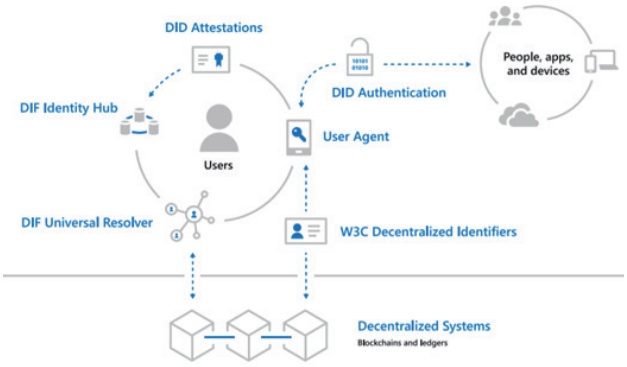
- Sovrin은 디지털 크리덴셜(Digital Credential)에 대한 새로운 표준으로, 운전면허증과 신분증 같은 기존 ID에 대한 신뢰와 개인 제어 및 사용의 편의성을 인터넷에서 제공될 수 있도록 설계한 것이다. 전체적으로 공개 표준과 오픈 소스

인 Hyperledger Indy 프로젝트를 기반으로 개발되고 있다. Sovrin의 새로운 디지털 크리덴셜을 제공하기 위해서는 두 가지 문제에 대한 해결이 필요하다. 첫 번째 문제는 디지털 ID 증명에 대한 표준화된 형식이 없다는 것이다. 여권은 전 세계 어디에서도 사용자의 신원을 확인할 수 있다. 이것은 여권의 형식이 표준화되어 있기 때문에 가능한 것으로 디지털 크리덴셜도 이와 같은 표준이 필요하다. 현재 W3C의 Verifiable Claims Working Group에서 표준화가 진행되고 있는 Verifiable Credential Data Model 1.0 표준을 이용하면 디지털 크리덴셜을 위한 표준화된 형식을 제공할 수 있다. 이 표준의 목적은 주장(claims)을 온라인에서 더 쉽고 안전하게 표현(expressing)하고 교환(exchanging) 및 검증(verifying)하는 방법을 제공하고 있다. 두 번째 문제는 디지털 크리덴셜에 대한 출처 및 무결성을 확인할 수 있는 표준화된 방법이 없다는 것이다. Sovrin의 디지털 크리덴셜이 보편적으로 채택되려면, 누구나 검증을 위한 올바른 공개키를 신속하게 확인할 수 있는 방법이 필요하다. 현재 W3C의 Credentials Community Group에서 다루고 있는 Decentralized Identifiers(DIDs) 표준 기술과 분산원장 기술을 결합하여 사용하면 누구나 디지털 서명된 크리덴셜을 발급할 수 있고, 누구나 서명된 크리덴셜을 검증할 수 있다. 이를 통해서 수세기 동안 오프라인에서 사용해 온 것과 같은 동일한 과정으로 온라인에서도 사용자의 크리덴셜을 검증할 수 있게 된다. 그림 3은 Sovrin의 디지털 크리덴셜을 검증하기 위한 생태계를 표현한 개념도이다[13].



〈그림 3. Sovrin의 디지털 크리덴셜을 위한 생태계〉

- IBM은 리눅스 재단과 IBM의 주도로 2015년 12월부터 블록체인 오픈소스 프로젝트인 'Hyperledger' 프로젝트를 시작하였다. 그 중에서 Hyperledger Indy 프로젝트가 Sovrin foundation 주도로 개발되고 있는 인증에 특화된 블록체인 플랫폼이다. Hyperledger Indy의 목적은 블록체인에 기반한 독립된 디지털 ID 생성 및 사용을 위한 툴, 라이브러리, 재사용 컴포넌트들을 제공하여 인터넷 환경에서 중재자 없이 ID를 제공하는 것이다[14].
- Microsoft는 개인이 자신의 ID 정보를 직접 관리하고 통제할 수 있는 새로운 디지털 ID 관리 모델을 개발하고 있다. 최근 블록체인 기술을 활용한 분산 ID 시스템을 구축하는 백서를 공개했다. 백서를 통해서 그림 4와 같은 새로운 분산 ID 개념도를 소개하고 분산 ID 시스템의 필요성을 다음과 같이 설명하고 있다. ID 정보를 직접 소유하고 관리해야 하고, 철저한 프라이버시 중심의 정책 지원 가능이 가능해야 하며, 사용자 중심의 앱과 서비스 구조로 설계되어야 하고, 세계적인 규모를 지원하고 개방성과 상호운용성을 통하여 모든 사람들이 이용할 수 있는 접근성 확보가 필요하다고 기술한다[15].



〈그림 4. 마크로소프트의 분산 ID 시스템 개념도〉

IV. 자기주권 ID 관리 기술

본 장에서는 자기주권 ID(Self-Sovereign Identity, SSI)의 의미와 특성을 살펴보고, 자기주권 ID 관리 시스템에서 활용되는 분산 식별자(Decentralized Identifiers, DIDs)와 검증 가능한 크리덴셜(Verifiable Credential)에 대해서 기술한다.

4.1 자기주권 ID 관리

자기주권 ID를 구성하는 단어의 의미로 살펴보면 Self는 '스스로', Sovereign은 '독립적인, 권한을 가진', Identity는 '신원, 신분'을 나타낸다. 즉, 자기주권 ID는 '스스로 권한을 부여한 신원'으로 정의될 수 있으며 사용자 개인이 자신의 ID을 만들고 관리하는 것은 자기 자신이라는 개념을 가지게 된다. 이것은 ID 증명의 패러다임이 중앙집중형 ID 증명 방식에서 개인이 주권을 가지고 자신의 ID을 관리 및 활용할 수 있는 체제로 변화한다는 것을 의미한다.

자기주권 ID는 블록체인, 즉 분산 원장을 사용하므로 중앙 디렉토리가 없어도 분산 식별자를 조회할 수 있다. 블록체인 자체는 신원 문제를 해결하는 것이 아니라 그동안 없었던 연결 고리를 제공한다. 그래서 사용자들이 온라인 상에서도 오프라인에서와 같이 분산된 검증 가능한 크리덴셜을 사용하여 스스로를 입증할 수 있게 된다[16].

자기주권 ID 검증은 주류 매장에서 운전면허증을 제시하는 상황을 예로 설명될 수 있다. 도로교통공단은 검증 가능한 크리덴셜을 발행하는 기관이며 크리덴셜을 요청한 사용자에게 운전면허증에 대한 검증 가능한 크리덴셜을 제공한다. 도로교통공단은 블록체인에서 자신이 제어하는 분산 식별자와 연결된 개인키를 사용하여 사용자가 요청한 크리덴셜에 서명한다. 따라서 이 크리덴셜을 받은 사람은 누구나 그 발행자가 도로교통공단임을 알 수 있다. 사용자는 지갑에 검증 가능한 크리덴셜을 넣고, 블록체인에서 자신이 제어하는 분산 식별자에 연결된 개인키를 사용해 디지털 운전면허증에 부서(countersign)한다. 매장에서 손님이 법적 성인임을 확인해야 하는 경우, 손님이 부서한 디지털 운전면허증을 제시하면 매장은 이것이 유효하고 변경되지 않았는지, 매장이 신뢰하는 도로교통공단이 발행한 것이 맞는지, 이를 제시하는 사람의 디지털 운전면허증인지를 확인할 수 있다.

누구나 블록체인을 사용하여 분산 식별자를 조회하고 연결된 공개키를 확인할 수 있다. 또한 모든 조직 또는 개인은 원하는 검증 가능한 크리덴셜을 발급할 수 있다. 어떠한 크리덴셜도 자유롭게 지갑에 보관할 수 있다. 또한 크리덴셜 검증자는 어떤 크리덴셜을 신뢰할지를 직접 선택할 수 있기 때문에 많은 분야에서 자기주권 ID 관리 시스템을 사용할 수 있다.

4.2 분산 식별자

분산원장 기술의 출연으로 완전히 새로운 ID 관리 시스템이 개발되고 있다. 분산된 ID 관리 시스템에 존재하는 엔티티(Entity)는 공유된 신뢰 루트를 자유롭게 사용할 수 있다. 전 세계적으로 분산된 원장(또는 유사한 기능을 제공하는 분산된 P2P 네트워크)는 중앙집중형 권한을 사용하지 않고 ID을 관리할 수 있는 수단을 제공한다. 분산원장 기술과 분산 식별자를 함께 사용하면 모든 엔티티가 분산되어 독립적이고 신뢰성 있는 루트에서 고유한 식별자를 만들고 관리할 수 있다. 또한 분산 ID 관리 시스템의 엔티티는 분산 식별자로 식별되어 증명을 통해 인증할 수 있다.

분산 식별자는 검증 가능한 자기주권 ID를 위한 새로운 유형의 식별자이고, 전 세계적으로 고유하고 암호학적으로 입증 가능한 영구적인 식별자를 만들 수 있는 표준 방식을 제공한다[17]. 분산 식별자는 중앙집중형 기반의 ID 제공 업체부터 독립되어 DID 주체(subject)의 통제하에 관리된다. 그리고 분산 식별자는 자신에 대한 사용 방법을 간단하게 기술한 DID Documents를 가리키며, 각각의 DID Document는 최소한 증명 목적(proof purposes), 검증 방식(verification methods), 서비스 엔드포인드(service endpoints) 정보를 포함한다. 표 3은 분산 식별자를 표현한 샘플 정보와 분산 식별자를 설명하는 DID Document에 대한 예제 코드이다.

표 3 DID 및 DID Document 샘플

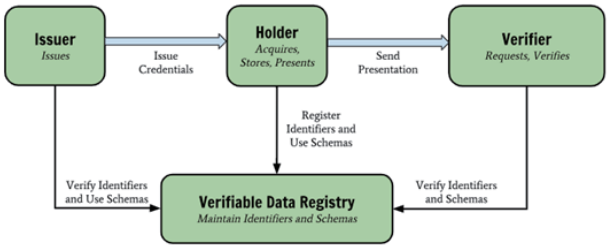
DID	did:example:123456789abcdefghi
DID Document	{ "@context": "https://w3id.org/did/v1", "id": "did:example:123456789abcdefghi", "authentication": [{ // this key can be used to authenticate as did:...fghi "id": "did:example:123456789abcdefghi#keys-1", "type": "RsaVerificationKey2018", "controller": "did:example:123456789abcdefghi", "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----₩r₩n" }], "service": [{ "type": "ExampleService", "serviceEndpoint": "https://example.com/endpoint/8377464" }] }

증명 목적은 검증 방법과 결합하여 사물(things)들을 증명하기 메커니즘을 제공한다. 예를 들어, DID Document는 공개키 또는 익명의 생체 인식 프로토콜과 같은 특정 검증 방식을 사용하여 인증 목적으로 생성된 증명(proof)를 검증할 수 있음을 구체적으로 명시할 수 있다. 서비스 엔드포인트는 DID 컨트롤러와 신뢰할 수 있는 상호 작용을 가능하게 한다.

4.3검증 가능한 크리덴셜

운전면허증은 자동차를 운전할 수 있다는 자격을 가지고 있다는 사실을 주장하는데 사용하고, 대학 학위는 교육 수준을 주장하는데 사용하고, 정부가 발생한 여권은 해외 여행을 가능하도록 해준다. 이러한 크리덴셜들은 물리적 세계에서 사용될 때 다양한 혜택을 제공하지만, 웹에서의 사용은 불가능하다. 왜냐하면 현재 물리적인 크리덴셜을 웹에서 이용할 수 있는 형태로 표현하는 것이 어렵기 때문이다.

W3C의 Verifiable Claims Working Group에서는 Verifiable Credentials Data Model 1.0 표준을 작업하고 있으며, 이 표준은 암호학적으로 안전하고 프라이버시를 보존하며 기계가 검증할 수 있는 방식으로 웹 상에 다양한 종류의 크리덴셜을 표현할 수 있는 방법을 제공한다. 이를 통해 검증 가능한 크리덴셜은 물리적인 크리덴셜과 동일한 모든 정보를 표현할 수 있고, 디지털 서명과 같은 기술을 추가하면 정보에 대한 변조 여부도 확인 가능해 물리적인 크리덴셜보다 더 신뢰할 수 있다. 그림 5는 검증 가능한 크리덴셜을 위한 생태계와 핵심 액터(Actor)의 역할 및 그들 간에 관계에 대해서 설명한다[18].

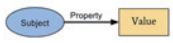
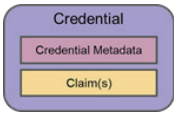
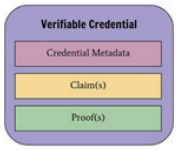
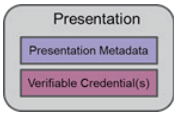
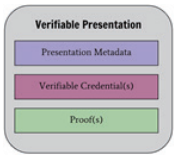


〈그림 5. 검증 가능한 크리덴셜을 위한 생태계〉

- 발급자(Issuer): 특정 객체에 대한 검증 가능한 크리덴셜을 생성하고, 그것을 Holder에게 전달하는 역할 (예, 정부, 기관, 단체 등)
- 소유자(Holder): 하나 또는 그 이상의 검증 가능한 크리덴셜을 소유하고 있고, 그것을 Verifier에게 제출할 때에는 Presentation 형태로 생성해서 전달하는 역할 (예, 학생, 직원, 고객 등)
- 검증자(Verifier): Holder가 적절한 검증 가능한 크리덴셜을 보유하고 있는지 검증하는 역할 (예, 고용주, 보안 담당자, 서비스 제공자 등)
- 검증 가능한 데이터 저장소(Verifiable Data Registry): 식별자, 키 및 기타 관련 데이터의 생성 및 검증을 중재하는 역할 (예, 분산 DB, 정부 ID DB, 분산 원장 등)

표 4는 검증 가능한 크리덴셜을 표현하는 핵심 데이터 구조를 설명한다.

표 4 검증 가능한 크리덴셜을 표현하는 핵심 데이터 구조

데이터	정의	표현
Claim	주체(Subject)의 특성(Property)에 대한 정보(Value)를 설명하는 것	
Credential	동일한 Entity에 대한 하나 또는 그 이상의 Claim의 집합	
Verifiable Credential	암호학적으로 Credential 발급자와 위변조 사실을 확인할 수 있는 Credential	
Presentation	하나 또는 둘 이상의 발급자로부터 받은 다수의 Credential의 집합	
Verifiable Presentation	암호학적으로 Presentation 제출자와 위변조 사실을 확인할 수 있는 Presentation	

IV. 결론

본고에서는 블록체인 기술을 이용한 ID 관리 기술과 자기주권 ID 관리를 위한 분산 식별자와 검증 가능한 크리덴셜에 대해 기술하였다. 블록체인 기반의 ID 관리 기술은 자신의 정보를 스스로 관리하고 통제할 수 있는 자기주권을 강조하고 있다. 자기주권 ID 시스템을 구성하는데 꼭 필요한 분산 식별자와 검증 가능한 크리덴셜은 현재 W3C를 통해 표준화가 활발하게 진행되고 있지만, 아직까지는 그룹 보고서 또는 초안 문서 형태로 발표되고 있는 단계이다.

현재 블록체인 기반 ID 관리 기술의 연구는 정보에 대한 공유 및 활용에 대한 측면에 집중되어 있다. 향후 다양한 분야에 적용되는 것을 고려할 때, 이종 도메인 간에 정보 공유를 위한 제약 사항 분석 및 공유 정보에 대한 갱신 및 삭제 처리에 대한 연구도 함께 진행되어야 한다. 또한 향후 개인에 대한 ID 관리 기술을 넘어 법인이나 단체와 같은 그룹의 ID, 스마트 기기의 ID 등 매우 다양한 엔티티들에 대한 ID 관리와 새로운 형태의 인증 기술에 대한 연구에도 관심을 가질 필요가 있다.

Acknowledgement

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0—01369, 020 서비스를 위한 무자각 증강인증 및 프라이버시가 보장되는 블록체인 ID 관리 기술 개발)

References

[1] 한국정보화진흥원, “블록체인을 활용한 디지털 ID 인증 서비스 공개,” D.gov, 2017.11.
[2] 김태형, “블록체인 개념 및 분야별 활용사례 분석,” 전기저널 487, 2017. 7.
[3] 송민정, “디지털 시대의 신원 확인과 블록체인 기술 연계,” 2017.12 from http://www.hellot.net/new_hellot/magazine/magazine_read.html?code=202&idx=38221&public_date=2017-12
[4] 이제영, 우청원, “블록체인 기술의 전망과 한계 그리고 시사점,” Future Horizon 2018 제 38호, 2018.12
[5] 박정숙, 박준영, 최선미, 오진태, 김기영, “블록체인 세대별 기술 동향,” 전자통신동향분석, 2018. 12
[6] “블록체인 기술 발전 전략,” 과학기술정보통신부, 2018. 6
[7] IBM Homepage, [online] Available: https://www.ibm.com/kr-ko/blockchain/ hyperledger
[8] Manohar, Arthi, Jo Briggs, “Identity Management in the Age of Blockchain 3.0,” HCI for Blockchain - CHI

2018 workshop, 22nd, April 2018.
[9] Rohan Pinto, "How Blockchain Can Solve Identity Management Problems", Forbes, July 2018. [online] Available: https://www.forbes.com/sites/forbestechcouncil/2018/07/27/how-blockchain-can-solve-identity-management-problems /#38fab2ad13f5
[10] Microsoft Blog, "Decentralized digital identities and blockchain: The future as we see it," February 2018. [online] Available: https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/
[11] Paul Dunphy, and Fabian A. P. Petitcolas. "A First Look at Identity Management Schemes on the Blockchain," IEEE Security and Privacy Magazine special issue on "Blockchain Security and Privacy", August 2018.
[12] ShoCard Whitepaper, "Identity Management Verified Using the Blockchain," January 2018. [online] Available: http://shocard.com/wp-content/uploads/2018 /01/ShoCard-Whitepaper-Dec13-2.pdf
[13] Sovrin Whitepaper, "A Protocol and Token for Self-Sovereign Identity and Decentralized Trust", January 2018. [online] Available: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf
[14] IBM Blog, "Hyperledger Fabric 개요", 2018. 11. [online] Available: https://deve loper.ibm.com/kr/cloud/blockchain/blockchain-special-series/2018/11/12/hype rledger-fabric-%ED%95%98%EC%9D%B4%ED%8D%BC%EB%A0%88%EC%A0% 80-%ED%94%84%EB%A1%9C%EC%A0%9D%ED%8A%B8-%EA%B0%9C%EC%9A%94/
[15] Microsoft Whitepaper, "Decentralized Identity – Own and control your identity," [online] Available: https://azure.microsoft.com/en-us/overview/decentralized-identity/
[16] Phillip Windley, "블록체인은 어떻게 자주적 신원을 실현하는가", IT World, 2018. 1. [online] Available: http://www.itworld.co.kr/news/107849
[17] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, Markus Sabadello, "Decentralized Identifiers (DIDs) v0.11," W3C Community Group Report, March 2019.
[18] Manu Sporny, Dave Longley, "Verifiable Credential Data Model 1.0," W3C Working Group, February 2019.

Biographies



김석현(Seok-hyun Kim)

2008년: 충주대학교 전자통신학과 학사
2010년: 전남대학교 정보보호협동과정 석사
2010년~현재: 한국전자통신연구원 정보보호연구본부 선임연구원
관심분야: 인증, ID 관리, 블록체인, 정보보호
E-mail: ksh4uu@etri.re.kr



조영섭(Young-Seob Cho)

1993년: 인하대학교 전자계산공학과 학사
1995년: 인하대학교 전자계산공학과 석사
1999년: 인하대학교 전자계산공학과 박사
1998년~현재: 한국전자통신연구원 정보보호연구본부 책임연구원
관심분야: 인증, ID 관리, 프라이버시 보호, 정보보호
E-mail: yscho@etri.re.kr



김수형(Soo-hyung Kim)

1996년: 연세대학교 컴퓨터과학과 학사
1998년: 연세대학교 컴퓨터과학과 석사
2016년: KAIST 전산학 박사
2000년: 한국정보통신연구원
2000년~현재: 한국전자통신연구원 정보보호연구본부 기술총괄
관심분야: ID 관리, 바이오 인증, 핀테크 보안, 개인정보보호
E-mail: lifewsky@etri.re.kr

IoT 환경에 적합한 블록체인 및 스마트 컨트랙트 기술 연구

김베드로, 이대화, 지우중, 김형식
성균관대학교

Abstract

본 논문은 IoT환경에 적합한 블록체인 기술 및 스마트 컨트랙트 기능 개선연구에 대해 소개한다. 이를 위해 IoT 환경에서의 요구 조건에 대해 정의하고, 기존의 블록체인 합의 알고리즘 및 스마트 컨트랙트의 언어에 대한 분석을 진행하였다. 결론적으로 IoT환경에 최적화된 합의 알고리즘과 스마트 컨트랙트 개선방향에 대해 제시한다.

I. 서론

사물인터넷(IoT, Internet of Things)을 이용한 기술이 발전함에 따라 IoT 환경에서 개인정보를 수집 및 활용하는 사례가 급증하고 있다. 이에 따라 IoT환경에서 보안성을 높일 수 있는 한 가지 방안으로 블록체인을 적용한 연구가 활발히 진행되고 있다. 기존의 연구에서는 IoT 환경에서 블록체인을 활용하면 디바이스들 간의 서비스와 리소스 공유를 촉진할 수 있으며, 암호화 방식으로 검증 가능하도록 자동화함으로써 보안 취약점을 보완할 수 있다는 장점을 가지고 있다고 기술하였다[1][2]. 하지만 IoT 기기에서는 작은 규모의 데이터가 빈번히 생성되며 이에 대한 처리가 빠르게 진행되어야 문제없이 다음 작업을 이어나갈 수 있는 연속성을 요구할 때가 많다. 그러므로 높은 확장성을 바탕으로 하여 빠른 속도로 블록을 생성하고 트랜잭션을 처리할 수 있는 환경이 중요하다. 또한 대부분의 IoT 장치가 사용할 수 있는 자원은 한정적이나, 채굴은 상당히 많은 연산 비용이 들기 때문에 작업 증명과 같은 합의 알고리즘보다는 에너지를 적게 소모하고, 요구 성능이 낮은 환경이 중요하다.

본 논문에서는 IoT 환경에 최적화된 블록체인 기술에 대한 연구를 진행하기 위해 기존의 블록체인 기술을 분석하여 IoT 환경에 적합한 기술을 선별하고자 한다. 또한 검증 자동화를 위해 사용하게 되는 스마트 컨트랙트를 최적화하기 위해 스마트 컨트랙트에서 활용되는 언어를 분석하고 개선할 수 있는 방향에 대해 기술하였다.

본 논문은 다음과 같이 구성되어 있다. 먼저 2장에서는 기존 블록체인 기술에 대한 구성 및 특징에 대한 분석을 진행한다. 3장에서는 IoT환경에 적합한 블록체인 개선 방향에 대해 소개한다. 4장에서는 스마트 컨트랙트 언어에 대한 분석을 수행한다. 5장에서는 IoT환경에 적합한 스마트 컨트랙트 개선 방향에 대해 기술한다. 마지막으로 6장에서 결론을 내리며 본 논문을 마친다.

II. 블록체인 기술 개요

2.1 블록체인

블록체인[3]은 관리 데이터를 블록 단위로 묶어 다음 블록에서 이전 블록의 해시를 저장하는 연결리스트와 같은 체인 형태를 지니며 P2P 네트워크를 통해 모든 노드에게 공유하는 기술이다. 블록체인에 데이터가 한번 기록되면, 영원히 변하지 않고 저장되는 비가역성과 무결성의 특징을 지닌다. 또한 모든 이용자가 블록에 저장된 기록에 접근이 가능한 투명성을 가진다.

2.2 블록체인의 종류

블록체인은 참여자의 범위에 따라 퍼블릭 블록체인, 프라이빗 블록체인, 하이브리드 블록체인으로 나눌 수 있다[4].



〈그림 1. Public blockchain VS Private blockchain〉

퍼블릭 블록체인은 누구든지 허가없이 참여할 수 있는 개방형 블록체인으로 인터넷에 연결된 PC, 노트북, 스마트폰 등 다양한 컴퓨터 장비를 통해 참여할 수 있다. 투명성과 보안성이 강화된 모델이지만, 많은 사람들에 의해 합의가 진행되고

전체 네트워크에 전파하여 동기화해야 하기 때문에 속도가 느리다는 단점이 있다. 퍼블릭 블록체인으로는 PoW 합의 알고리즘, PoS 합의 알고리즘, DPoS 합의 알고리즘이 적합하다.

프라이빗 블록체인은 네트워크 운영자에게 허가를 받아 참여할 수 있는 허가형 블록체인으로 허가된 컴퓨터 장비를 통해서만 참여할 수 있다. 기밀성과 속도가 강화된 모델이지만, 적은 사람들에 의해 합의가 진행되기 때문에 일부 중앙화가 되어 보안성이 낮아질 수 있다는 단점이 있다. 프라이빗 블록체인에서는 PBFT 합의 알고리즘이 적합하며, IBM이 개발하는 hyper ledger가 이에 속한다.

하이브리드 블록체인은 퍼블릭 블록체인과 프라이빗 블록체인을 서로 연결하거나 섞은 혼합형 블록체인으로 기밀성이 중요한 IoT 기기에는 프라이빗 블록체인을 이용하고, 자동화된 결제를 위해서는 퍼블릭 블록체인을 이용하는 방식이다. 더블 체인은 Hdac에서 IoT 블록체인 플랫폼을 지향하여 사용한다.

2.3 블록체인 구성요소

블록체인의 가장 기본 요소는 블록(block)으로, 이를 구성하기 위해서는 먼저 거래의 최소 단위인 트랜잭션에 대한 정보를 수집해야 한다[5]. 트랜잭션은 더 이상 쪼갤 수 없는 데이터의 최소 단위로 블록을 구성하는데 사용된다. 트랜잭션은 해시함수를 통해 암호화되어 고정된 비트의 크기로 표현되며, 사용자의 개인키로 서명한 뒤, 마이너들에 의해 블록에 저장되게 된다. 블록은 트랜잭션 정보 이외에 블록 헤더라는 값을 가지며, 아래와 같이 7가지 요소로 구성된다.

표 1 블록 헤더의 구성

이름	설명
Version	소프트웨어 및 프로토콜 정보
Merkle root hash	개별 트랜잭션 해시로 구성한 2진 트리의 루트 트리
Time	블록 생성 시간
Previous block hash	이전 블록의 해시값
nBits	작업의 난이도를 조절
Nonce	0부터 시작하여 1씩 증가하는 숫자
Txn_count	트랜잭션의 수를 카운트

이러한 정보들은 하나의 해시값으로 변환되어 다음 블록의 previoushash 공간에 저장되며, P2P 네트워크를 기반으로 블록들을 정보를 공유하게 된다. 이때 발생할 수 있는 정보 불일치 문제는 추후 언급될 합의 알고리즘을 통해 해결하였다. 이처럼 블록체인에서는 다음 블록에서 이전 블록의 모든 정보를 해시의 형태로 가지고 있기 때문에 특정 블록에서 변조가 발생할 경우, 그 후의 모든 블록이 영향을 받아 값이 변하게 됨으로 문제가 발생한 블록을 쉽게 찾아낼 수 있다.

2.4 합의 알고리즘 분석

합의 알고리즘은 다수의 노드들이 하나의 통일된 의사 결정을 위한 알고리즘이다. 블록체인에서 모든 노드가 데이터를 공유하기 때문에 원본과 사본의 구별이 없으며, 여러 블록 중 어떠한 것을 우선으로 인정할 것인가를 해결한 방법이다. 대표적으로 작업 증명과 지분 증명이 존재한다[6].

작업 증명(PoW, Proof of Work)은 블록을 생성하기 위해 일정한 작업량을 수행했음을 증명하는 방법이다. 새로 증명할 블록 헤더를 SHA256 알고리즘을 통해 해시값을 구하여 nBits에서 정한 숫자보다 작은 숫자가 나올 때까지 Nonce를 1씩 증가시킨다. 이 때, nBits에서 정한 숫자보다 작은 숫자가 나올 때까지 Nonce를 1씩 증가시키는 작업을 Mining, 작업자를 Miner라고 부른다. 더 큰 네트워크를 구성할수록 안정성과 안전성이 증가하며, 간단한 구조로 누구나 구성하기 쉽다는 장점이 있다. 하지만 해싱 파워를 이용하기 때문에 51%의 해싱 파워를 보유하면 네트워크 전체 합의를 좌우할 수 있는 51% 공격이 가능하며, 불필요하게 많은 양의 컴퓨터 자원을 사용한다는 단점이 있다.

이와 달리 지분 증명(PoS, Proof of Stake)은 해당 암호화폐를 보유하고 있는 사람들에게 지분율에 비례하여 의사 결정 권한을 주게 된다. 이는 다음과 같은 두가지 방식으로 나눌 수 있다. 첫째는 지분을 이용하여 투표하는 방식으로, 여러 블록 후보 중 합당하고 생각하는 블록에 대해 자신이 보유한 지분만큼 투표를 하고 그 블록이 최종적으로 많은 투표를 받아 정식 블록으로 등록된다면 자신이 투표한 만큼 새 블록의 보상을 받게 된다. 두번째 방식은 지분에 따라 다른 난이도의 블록 난이도를 받는 방식으로 기본 PoW 합의 알고리즘과 같게 진행되지만 nBits에서 정한 난이도가 지분율에 비례하여 정해진다. 또한 해시값을 구하지 않고 투표를 하거나, 비교적 난이도가 쉬운 문제를 풀게 함으로써, 불필요하게 많은 양의 컴퓨터 자원을 낭비하는 문제를 해결하였다. 해싱 파워가 아닌 지분을 사용하기 때문에 51% 공격을 훨씬 힘들게 했다는 장점이 있다. 하지만 지분이 많을수록 더 많은 증명을 할 수 있기 때문에 여러 곳에 동시에 투표하여 투표의 공정성을 해치는 Nothing at Stake 문제가 발생한다는 단점이 있다

III. IoT 환경에서 블록체인

3.1 IoT 환경에서 블록체인 요구사항

IoT 기기에서는 생성된 데이터 및 트랜잭션에 대한 빠른 처리를 요구하기 때문에 연속성과 최종성을 보장해야 한다[7]. 하지만 기존의 퍼블릭 블록체인의 경우, 속도가 느리고 트랜잭션이 블록에 업로드 된 후에 누락되지 않음을 확인하는 최종성이 보장되지 않기 때문에 IoT 환경에 사용하기 어렵다. 반대로 프라이빗 블록체인은 투명성이 보장되지는 않지만 속도가 빠르고 최종성이 보장된다는 장점을 가지고 있다. 하지만 활용방법에 대한 use case 정보가 부족하기 때문에 IoT환경에 적합하지 않다. 그러므로 높은 확장성을 기반으로 빠르게 블록을 생성하고 트랜잭션을 처리할 수 있는 환경이 필요하다. 또한 대부분의 IoT 장치가 사용할 수 있는 자원은 한정적이기 때문에 채굴에 따른 고연산 비용 문제를 해결할 수 있어야한다.

3.2 IoT 환경에 적합한 블록체인 개선 방향

IoT환경에 블록체인을 적용하기 위해서는 앞서 언급된 것처럼 트랜잭션 및 데이터 처리 속도 개선, 확장성 보장 등이 이루어져야 한다. 블록체인의 속도를 개선하기 위한 대표적인 방법으로 샤딩[8]이 존재한다. 이는 블록체인 네트워크를 수평으로 공정하게 나누어 네트워크 별로 트랜잭션을 병렬 처리하게 된다. 이를 적용하면 초당 처리 가능한 결제의 수를 높일 수 있게 된다는 장점이 있다. 하지만 10개로 나누었을 때, 부정직한 공격자가 블록체인의 해싱 파워를 전체 6퍼센트만 가지고 있다고 하더라도 한 네트워크에 몰아서 공격을 하게 되면 총 60퍼센트의 효과가 나기 때문에 중앙화 되어 쉽게 공격받을 수 있다는 위험이 있다. 샤딩의 개념을 도입한 합의 알고리즘으로 Hierarchical PoS (HPoS)가 있다. HPoS의 장점은 지분 증명을 사용하기 때문에 해시값을 구하지 않고 투표를 하거나, 비교적 난이도가 쉬운 문제를 풀게 함으로써 불필요하게 컴퓨터 자원을 낭비하는 문제를 해결하였다는 것이다. 또한 해싱 파워가 아닌 지분을 사용하기 때문에 51% 공격을 힘들게 하면서 빠른 합의 속도를 이룰 수 있다는 장점을 가지고 있다. 매 순간 합의하지 않고, 한 번의 합의를 통해 검증 노드와 대표 노드를 정해 일정 시간동안 소모적인 합의 과정없이 빠르게 합의를 도출할 수 있다는 장점이 있다. 다른 방법으로는 IoT기기에서 전송되는 데이터의 사이즈를 작게 만들어 효율성을 높이는 방식이 존재한다. 데이터를 줄이는 방법으로 슈노 시그니처[9]를 도입할 수 있다. 이는 비트코인 거래들이 전자 서명되고 처리되는 것을 효과적으로 도와주는 방법이다. 이는 여러 주소를 통해 하나의 주소에게 트랜잭션을 보낼 경우, 거래 처리 과정에서 다수의 전자 서명이 필요했던 것을 단 하나의 전자 서명을 이용하여 보낼 수 있도록 개선하여 블록 사이즈를 줄이는 방법이다. 이를 적용하면 최대 25%의 저장 공간을 효율적으로 사용할 수 있다.



〈그림 2. 슈노 시그니처 방식〉

블록체인의 확장성 문제를 해결하기 위한 방안으로는 off-chain 방식의 Lightning Network[10]가 존재한다. Lightning Network의 핵심은 지불 채널을 활용해 잦은 트랜잭션을 메인 블록체인의 밖에서 처리하는 것이다. 즉, 일정 시간에 따라 발생하는 트랜잭션을 메인 블록체인에 브로드캐스트하지 않고 지불 채널 내부에서 처리한다. Lightning Network에서는 여러 개의 채널이 결합되어 경로를 구성할 수 있으며, 이러한 경로를 통해 네트워크의 모든 참여자와 직접적인 채널을 열지 않고도 거래할 수 있다. 하지만, 이와 같은 지불 채널의 결합은 Lightning Network 노드의 차수(degree)가 멱함수 분포(power-law distribution)를 따르는 scale-free 특성을 갖게 하며, scale-free 특성을 갖는 네트워크는 노드의 차수가 갖는 분포에 의해 소수의 차수가 높은 허브(hub) 노드를 통해 전체 네트워크의 연결성(connectivity)을 유지하기 때문에 이러한 노드를 목표로 하는 공격에 취약할 수 있다.

IV. 스마트 컨트랙트 분석

4.1 스마트 컨트랙트 언어 분석

스마트 컨트랙트는 블록체인 위에 작성된 코드에 대해 특정 조건이 충족되면 자동으로 실행되는 프로토콜이다. 한번 기록된 사항은 거부하거나 부인할 수 없으며 지시된 사항대로 계약된 내용이 이행되어야 한다. 스마트 컨트랙트를 작성하는 프로그램으로는 Solidity, Viper, Serpent 등이 존재하며, 각 언어별 특징은 다음과 같다.

Solidity[11]는 자바스크립트와 유사한 이더리움 전용의 프로그래밍 언어로, 이더리움에서 스마트 컨트랙트 작성 및 실행에 사용된다. Solidity의 특징으로는 다중상속을 포함한 상속 및 라이브러리 기능을 지원하며 복잡할 수 있는 사용자 정

의 유형을 지원하는 특징이 있다. Solidity로 만들어진 스마트 컨트랙트를 EVM위에서 실행이 되며, Solidity 전용 컴파일러(solc)를 사용하여 Bytecode로 변환이 되어야한다. 이렇게 변환된 바이트코드(스마트 컨트랙트)는 Ethereum Virtual Machine (EVM)에서 실행이 된다. Solidity로 작성된 스마트 컨트랙트가 가장 많이 이용되는 이더리움의 큰 특징 중 하나는 turing complete한 언어를 사용한다는 것이다. 단순한 거래의 실행에 대한 조건을 나타내는 비트코인 스크립트 언어와는 달리 이더리움의 스마트 컨트랙트 언어는 turing complete하기 때문에 대부분의 일반적인 계약의 내용들을 구현할 수 있다. 하지만 turing complete 언어는 다양하고 복잡한 계약조건을 구현할 수 있는 반면 복잡성으로 인해 버그가 발생할 확률 또한 높다. 이러한 버그의 가능성을 줄이고자 개발된 스마트 컨트랙트 언어가 Viper[12]이다.

Viper는 Solidity와 마찬가지로 EVM 바이트 코드로 컴파일되어 실행된다. 그러나 Viper는 Solidity보다 사용자 친화적인 환경을 목표로 높은 투명성과 더 나은 보안을 스마트 계약을 단순화하는 것을 목표로 하였다. Viper를 이용해 스마트 컨트랙트가 완벽하고 효과적으로 실행되기 위해서는 코드가 매우 효율적이어야 한다. 만약 코드의 요구 사항을 충족시키지 못하면 스마트 계약 시, 스마트 컨트랙트의 가스량(수수료)가 증가한다.

Serpent[13]은 초기 이더리움에서 스마트 컨트랙트를 작성하는 프로그래밍 언어 중 하나였다. 이는 파이썬과 매우 유사하도록 설계되었으며 Solidity와 마찬가지로 EVM 환경 위에서 작동한다. Serpent는 Solidity와는 달리 EVM 환경에서 작동하기 위해 컴파일러에 의해 어셈블리 코드로 변환된다. 하지만 보안성의 문제로 현재 스마트 컨트랙트에서 더 이상 사용되지 않는 언어로 자리 잡았다.

V. IoT 환경에서 블록체인

5.1 IoT 환경에 적합한 스마트 컨트랙트 개선 방향

IoT 환경에서 스마트 컨트랙트를 적용하기 위해서는 IoT 환경이 가지는 저전력, 저성능, 속도 등 IoT 환경만이 가지는 장점을 이용하여야 한다. 하지만 기존의 IoT 환경에서는 IoT 장치들 사이에서 매초마다 발생하는 다양한 크기를 가진 데이터 등의 문제점이 존재하기 때문에 스마트 컨트랙트를 적용하기는 어렵다. 이러한 문제점을 해결하고자 IoT 환경에 프록시 노드를 설치한다. 이 프록시 노드의 가장 큰 역할은 IoT 장치에서는 작거나 큰 규모의 데이터가 아주 자주 발생하며 그 처리가 빠르게 진행되어야 문제없이 다음 작업을 이어나갈 수 있는 연속성을 필요로 한다. 하지만 IoT 장치에서 어떠한 비즈니스 로직을 수행하는 스마트 컨트랙트가 실행되면 해당 스마트 컨트랙트의 코드량이나 스마트 컨트랙트에 존재하는 코드 중 컴파일이나 EVM에서 실행할 때 높은 성능이나 상당한 시간을 요구하는 instruction이 존재하게 된다. 이러한 환경에서는 IoT 장치들이 연속성을 유지할 수 없으며, 이는 성능치가 낮은 IoT 장치에 큰 부하를 주게 된다. 이를 해결하기 위해 컴퓨팅 파워가 강한 프록시 노드를 별도로 설치하여 모든 IoT 장치들이 프록시 노드에게 데이터를 전송하게 한다. 프록시 노드에서는 IoT 장치들에게서 받은 정보와 데이터로 비즈니스 로직을 수행할 수 있는 스마트 컨트랙트를 EVM 환경에서 동작 시키기 위해 바이트 코드로 변환하여 실행한다. 이 후, 스마트 컨트랙트의 실행 결과를 해당 IoT 장치들에게 알려주어 IoT 장치들의 연속성을 유지할 수 있다. 또한 스마트 컨트랙트를 작성할 때, 최소한의 instruction만으로 구성하여야 하여야 스마트 컨트랙트를 실행시키기 위한 컴파일 및 EVM 환경에서의 실행 시간, 요구되는 가스량 등을 최소한으로 유지할 수 있다. 이를 통해 나온 실행 결과를 스마트 컨트랙트로 전송하여 IoT 환경에서 스마트 컨트랙트를 적합하게 사용할 수 있을 것으로 보인다.

VI. 결론

본 논문에서는 IoT 환경에 최적화된 블록체인 기술 및 스마트 컨트랙트 개선 방향에 대한 연구를 진행하였다. 이를 위해 먼저 블록체인에 대한 정의와 특징에 대해 알아보았다. 이를 기반으로 기존의 IoT 환경에 블록체인 기술을 적용하기 위해 개선해야 할 문제점에 대해 분석하였다. 이를 통해 기존의 블록체인을 IoT환경에 적용하기 위해서는 트랜잭션 및 데이터 처리 속도 개선, 확장성 보장 등이 이루어져야 한다는 것을 알 수 있었다. 또한 기존의 합의 알고리즘은 에너지를 많이 소모하고 속도가 느리기 때문에 새로운 합의 알고리즘이 필요하다는 결론을 내렸다. 이를 바탕으로 IoT 요구사항을 추출하고, IoT 환경에 적합한 블록체인 개선 방향에 대해 알아보았다. 샤딩, 슈노 시그니처, Hierarchical PoS(PoS), 라이트닝 네트워크를 통해 이를 해결하고자 하였다. 특히 HPoS는 기존 지분 증명 방식을 사용하기 때문에 해시값을 구하지 않고 투표를 하거나, 비교적 난이도가 쉬운 문제를 풀게 함으로써 불필요하게 많은 양의 컴퓨터 자원을 낭비하는 문제를 해결하였다. 또한 해싱 파워가 아닌 지분을 사용하기 때문에 51% 공격에 대한 문제를 개선할 수 있다는 사실을 알 수 있었다. 또한 매 순간 합의하는 것이 아닌, 한 번 합의하여 검증 노드와 대표 노드를 정한 뒤 일정 시간동안 소모적인 합의 과정 없이 정

해진 검증 노드와 대표 노드만으로 빠르게 합의할 수 있다는 장점이 있는 것을 발견할 수 있었다. 마지막으로 스마트 컨트랙트 언어인 Solidity, Viper, Serpent를 분석하여 IoT 환경에 적합한 스마트 컨트랙트 개선 방향을 제시하였다. 개선 방향으로 프록시 노드를 추가로 도입하여 스마트 컨트랙트를 실행하는 방법을 제시하였다.

Acknowledgement

본 논문은 2019년도 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT연구센터지원사업의 연구결과로 수행되었음(IITP-2019-2015-0-00742).

References

[1] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[2] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains," arXiv preprint arXiv:1804.03903, 2018.

[3] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation, vol. 2, no. 71, pp. 6-10, 2016.

[4] M. Pilkington, "11 Blockchain technology: principles and applications," Research handbook on digital transformations, vol. 225, 2016.

[5] C. Decker, R. Wattenhofer, "Information propagation in the Bitcoin network," IEEE International Conference on Peer-to-Peer Computing, 2013.

[6] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," Work Pap, 2016.

[7] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," IEEE Internet of Things Journal, vol. 5, no.2, pp. 1184-1195, 2018.

[8] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," ACM SIGSAC Conference on Computer and Communications Security, pp. 17-30, 2016.

[9] C. P. Schnorr, "Efficient signature generation by smart cards," Journal of cryptology, vol. 4, no. 3, pp. 161-174, 1991.

[10] I. C. Lin and T. C. Liao, "A Survey of Blockchain Security Issues and Challenges," IJ Network Security, vol. 19, no. 5, pp. 653-659, 2017.

[11] I. Grishchenko, M. Maffei, and C. Schneidewind, "A semantic framework for the security analysis of ethereum smart contracts," International Conference on Principles of Security and Trust, pp. 243-269, 2018.

[12] M. Y. Afanasev, Y. V. Fedosov, A. A. Krylova, and S. A. Shorokhov, "An application of blockchain and smart contracts for machine-to-machine communications in cyber-physical production systems," IEEE Industrial Cyber-Physical Systems (ICPS), pp. 13-19, 2018.

[13] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "A programmer's guide to ethereum and serpent," URL: https://mc2- umd.github.io/ethereumlab /docs/serpent_tutorial.pdf, 2016.

Biographies



김베드로

2015년: 한국산업기술대학교 메카트로닉스공학과 학사
2017년: 성균관대학교 전자전기컴퓨터공학과 석사
2019년~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
관심분야: 보안공학, 블록체인



이대화

2017년: 용인대학교 컴퓨터과학과 학사
2018년~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야: 보안공학, 블록체인



지우중

2018년: 중부대학교 정보보호학과 학사
2018년~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야: 보안공학, 네트워크 보안, IoT 보안



김형식

1999년: 성균관대학교 정보공학부 학사
2001년: KAIST 컴퓨터과학과 석사
2012년: University of Cambridge 컴퓨터공학과 박사
2013년~현재: 성균관대학교 전자전기컴퓨터공학과 부교수
관심분야: 보안공학, 소셜 컴퓨팅

ETRI
한국전자통신연구원
Electronics and Telecommunications Research Institute



제4차 산업혁명을 선도하는

ICT Innovator

ICT Innovator leading the 4th Industrial Revolution

ETRI의 최첨단 기술은
새로운 영역과 새로운 가치를 만들어내고 있습니다.
꿈꾸는 모든 것을 현실로 구현하는 기술,

ETRI의 첨단 ICT기술은
세상을 더욱 풍요롭게 만들어갑니다.