J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

프라이버시 보호 관점에서의 블록체인 플랫폼 분석☆

Analysis of Blockchain Platforms from the Viewpoint of Privacy Protection

박 지 선[1] 신 상 욱[2*]
Ji-Sun Park Sang Uk Shin

요 약

암호화폐로 분류될 수 있는 비트코인은 혁신적인 디지털 통화이자 블록체인 시스템의 시초이기에 다양한 업계의 주목을 받고 있다. 하지만 비트코인에 대한 연구가 진행되면서 여러가지 보안 취약점과 가능한 공격들이 분석되었다. 그 중 블록체인 데이터베이스의 투명성 때문에 발생하는 보안 문제는 블록체인 시스템이 다양한 분야에 적용되는 것을 방해한다. 이 취약점은 또 다시 참여 노드의 약한 익명성 문제와 거래 내역 공개로 인한 프라이버시 노출 문제로 분류될 수 있다. 최근 몇 년 동안 이러한 취약점들에 대한 여러 보완책이 개발되었다. 본 논문에서는 먼저 공개 블록체인, 사설 블록체인의 주요한 특징에 대하여 기술하고 프라이버시와 비연결성, 익명성 등 용어에 대해서도 설명한다. 또한 비트코인으로부터 파생되었으나 거래 데이터의 프라이버시 및 송수신자의 익명성 보호를 중점적으로 제공하는 3가지 공개 블록체인 플랫폼인 대시, Zcash, 모네로, 그리고 사설 블록체인 플랫폼인 하이퍼레저 패브릭에서 적용하고 있는 프로토콜의 동작 원리를 분석한다. 추가적으로 적용된 기술들을 프라이버시 보호 기법과 익명성 보호 기법으로 상세히 분류하고 장단점을 분석하고, 또한 적용된 암호학적 기법들의 연산 속도를 바탕으로 플랫폼의 상대적 성능을 비교·분석한다.

☞ 주제어 : 암호화폐, 프라이버시, 익명성, 블록체인, 비트코인

ABSTRACT

Bitcoin, which can be classified as a cryptocurrency, has attracted attention from various industries because it is an innovative digital currency and the beginning of a Blockchain system. However, as the research on Bitcoin progressed, several security vulnerabilities and possible attacks were analyzed. Among them, the security problem caused by the transparency of the Blockchain database prevents the Blockchain system from being applied to various fields. This vulnerability is further classified as the weak anonymity of participating nodes and privacy problem due to disclosure of transaction details. In recent years, several countermeasures have been developed against these vulnerabilities. In this paper, we first describe the main features of the public and private Blockchain, and explain privacy, unlinkability and anonymity. And, three public Blockchain platforms, Dash, Zcash and Monero which are derived from Bitcoin, and Hyperledger Fabric which is a private Blockchain platform, are examined. And we analyze the operating principles of the protocols applied on each platform. In addition, we classify the applied technologies into anonymity and privacy protection in detail, analyze the advantages and disadvantages, and compare the features and relative performance of the platforms based on the computational speed of the applied cryptographic mechanisms.

☞ keyword : Cryptocurrency, Privacy, Anonymity, Blockchain, Bitcoin

1. 서 론

첫 암호화폐(cryptocurrency)는 데이비드 차움(David Chaum)에 의해서 구상된 Ecash라고 하는 익명의 암호학적 전자화폐로 볼 수 있다[1]. 그 이후 차움은 전자 지불 시스템인 디지캐시(Digicash)를 1995년에 직접 구현하였다. 이후에도 디지털 통화에 대한 연구는 꾸준히 진행되었지만 본격적으로 탈중앙화된 암호화폐가 사람들의 많은 관심을 받게 된 것은 2008년 비트코인(Bitcoin)[2]의 등장 이후부터이다. 암호 프로토콜이 적용되기 때문에 단순히 가상화폐라기보다는 암호화폐라고 불리는 이 시스템은 블록체인(Blockchain)과 P2P(Peer-to-Peer) 네트워크를

1 Interdisciplinary Program of Information Security, Graduate School, Pukyong National University, Busan, 48513, Korea.
2 Dept. of IT Convergence and Application Eng., Pukyong National University, Busan, 48513, Korea.
* Corresponding author (shinsu@pknu.ac.kr)
[Received 29 August 2019, Reviewed 23 September 2019(R2 15 October 2019), Accepted 21 October 2019]
☆ This research was a part of the project titled 'Future fisheries food research center', funded by the Ministry of Oceans and Fisheries, Korea, and was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (No. 2019R1I1A3A01060652).

기반으로 한 디지털 통화를 말한다. 비트코인은 오픈소스로 구현되었기 때문에 누구든 시스템 코드를 수정하여 개발이 가능하고 이로 인해 비트코인 소스코드에서 파생된 다양한 암호화폐들이 상장되었다. 2018년 8월 총 1855개의 암호화폐가 거래소에서 현재 거래되고 있다[3]. 또한 여러 분야에서 비트코인에 대한 연구가 활발히 진행되고 있으며 특히 보안적인 측면에서 비트코인을 분석한 논문들도 많이 발표되었다. 논문들은 비트코인의 여러 취약점과 가능한 공격들에 대해 언급하는데 그 중 심각하게 여겨지는 문제점은 프라이버시(privacy) 노출 문제이다.

비트코인은 블록체인이라는 특별한 데이터베이스를 바탕으로 운영된다. 블록체인은 블록들을 체인처럼 연결된 형태로써 각 블록 안에는 노드(node)들이 생성한 거래(transaction)가 포함되어 있다. 블록체인 데이터베이스(Database)는 일반적인 서버 데이터베이스와 달리 네트워크상의 모든 노드들이 데이터베이스 내용을 볼 수 있는 투명성의 특징을 지닌다. 또 다른 특징으로는 비트코인의 노드들은 거래 송수신시에 자신의 신원정보 대신 각자의 공개키 주소를 사용한다. 따라서 많은 사용자들은 비트코인 시스템이 익명성(anonymity)을 가진 것으로 착각할 수 있으나, 엄밀히 말하자면 비트코인은 가명성(pseudonymity)을 갖고 있다. 이는 프라이버시 측면에서 완벽하게 안전하다고 할 수 없는데 이 가명성과 투명성을 바탕으로 누구나 블록체인 데이터베이스에 접근하여 특정 주소 계좌의 거래 내역을 파악 하는 행위를 할 수 있기 때문이다. 다시 말해, 모든 블록과 거래가 공개되기 때문에 만약 한 사람의 비트코인 계좌 주소가 노출되면 누구나 그 사람의 비트코인 활동을 추적하고 관련 거래들을 연결하여 코인의 흐름을 관찰할 수 있다[4]. 이와 같이 의도하지 않은 개인의 프라이버시 노출 위험은 범죄에 악용되거나 피해자에게 경제적으로 영향을 끼칠 수 있다. 또 다른 문제점으로는 노드가 불법적인 거래에 사용되었던 코인을 파악하여 그 코인의 수신을 거부할 수도 있다. 해당 코인의 흐름은 단절되게 된다.

위와 같은 심각한 문제를 야기하는 프라이버시 노출 위험을 해결하기 위하여 암호 프리미티브 기법들이 적용된 여러 암호화폐 플랫폼이 등장하게 되었다. 본 논문에서는 대표적인 암호화폐 플랫폼들을 분석하여 프라이버시를 보호하기 위해 채택하고 있는 기법들에 대해 분석한다. 이를 위해 대시(Dash), Zcash, 모네로(Monero), 하이퍼레저 패브릭(Hyperledger Fabric) 블록체인 플랫폼을 분석한 후, 프라이버시와 익명성 관점에서 사용된 암호 기법들을 비교 분석한다. 먼저 2장에서는 관련 연구로 블록체인의 두 유형과 여러 용어들의 차이를 살펴본다. 3장은 프라이버시 보호 기법에 초점을 둔 4개의 블록체인 플랫폼과 적용된 암호 기법들에 대해 자세히 다룬다. 4장에서는 살펴본 블록체인 플랫폼들에 대해 보안측면에서 분석하고 마지막으로 5장에서 결론으로 본 논문을 마무리한다.

2. 관련 연구

2.1 공개(Public) 블록체인과 사설(Private) 블록체인

블록체인은 노드들의 P2P 네트워크 참여형태에 따라서 공개 무허가형 블록체인과 사설 허가형 블록체인으로 크게 나눌 수 있다[5]. 먼저 비트코인, 이더리움(Ethereum)과 같이 누구나 네트워크에 참여하여 거래 생성, 내역 확인 또는 블록 생성을 할 수 있는 블록체인을 공개 무허가형 블록체인(public permissionless Blockchain)이라 한다. 공개 블록체인의 대부분 노드들은 신뢰관계가 없는 상황에서 상호작용을 해야 하기 때문에 다수의 노드가 네트워크에서 활동해야 시스템이 안전하게 운영된다. 여러 노드들의 정직한 활동을 위한 합의 알고리즘으로는 작업증명(PoW, Proof of Work)이 가장 대표적이다. 작업증명 기반 플랫폼에서는 채굴자 노드들 중 가장 먼저 해시 퍼즐을 푸는 채굴자에게 블록 생성 권한이 주어진다. 기존의 공개 블록체인 형식의 암호화폐들은 블록체인의 투명성과 불변성을 바탕으로 안전성을 강조한다. 모두에게 거래가 투명하게 공개되기 때문에 악의적인 행동을 함부로 할 수 없다는 장점이 있는 반면에 이런 특징 때문에 노드들의 프라이버시가 전혀 보장되지 않는다고도 볼 수 있다.

블록체인 등장 초반의 암호화폐들은 대부분 공개 블록체인으로 공공장부를 관리하였다. 신뢰가 없는 P2P 네트워크의 노드들에게 모든 거래 내용이 무분별하게 공개되는 공개 블록체인의 특징은 블록체인 시스템 응용분야에 있어서 제약을 가지게 하였다. 특히 기업 내에 데이터 공유 등의 목적으로는 이 블록체인 형식은 적당하지 않았다. 결과적으로 권한을 가진 노드들만 네트워크에 참여하는 사설 허가형 블록체인(private permissioned Blockchain) 시스템이 등장하게 되었다. 사설 블록체인은 멤버십 서비스(membership service)를 두고 신원이 보장된 또는 조건에 맞는 노드들만 블록체인 네트워크에 접근을 허용한다. 채굴자 노드 역시 허가를 받은 노드들만이 될 수 있고 합의 알고리즘 또한 공개 블록체인 플랫폼과는 다른

알고리즘을 채택한다. 이미 신뢰관계가 보장된 네트워크이기 때문에 노드 수는 공개 블록체인에 비해 상당히 적고 생성되는 거래는 네트워크의 외부에 공개되지 않는다. 따라서 공개 블록체인 보다 프라이버시 보호가 된다고 할 수 있다. 또한 일반적으로 채굴 보상에 대하여 인센티브가 필요하지는 않는 것도 특징이다. 가장 잘 알려진 사설 블록체인 플랫폼으로는 하이퍼레저 패브릭(Hyperledger Fabric)이 있고 이 시스템은 PBFT(Practical Byzantine Fault Tolerance) 합의 알고리즘을 사용한다.

2.2 익명성과 프라이버시 (Anonymity and Privacy)

많은 사용자들이 익명성과 프라이버시 두 용어를 혼용해서 사용한다. 하지만 브래드버리(Bradbury)[6]는 익명성과 프라이버시의 의미를 다음과 같이 정의한다. 프라이버시는 어떠한 비밀사항을 숨기는 것이고 익명성은 그 비밀의 소유주를 숨기는 것이다. 즉, 블록체인 시스템에서의 익명성은 거래의 송신자 또는 수신자 정보(주소 값 등)를 모든 노드에게 노출되는 것을 방지하는 특성을 말한다. 3절에서 살펴볼 여러 플랫폼에서 익명성에 대한 기법으로 믹싱 기법, 스텔스 주소 스킴 등이 사용되었다. 반면에 프라이버시는 거래의 내용(금액 등)을 숨기는 것이다. 프라이버시 보호 기법으로는 믹싱 기법, 링 CT 등이 제안되어 사용되고 있다.

비연결성(unlinkability)과 비추적성(untraceability)의 의미도 비슷하다고 생각할 수 있으나 쿠마르(Kumar) 등[7]은 두 개의 거래가 있을 때 같은 노드가 생성한 거래임을 알 수 없는 성질을 비연결성으로 정의한다. 이와 조금 다른 의미인 비추적성은 거래 입력 값이 주어졌을 때 그에 따른 출력 값이 여러 출력 값들 중 정확하게 어떤 값인지 밝혀지지 않는 성질이다. 프라이버시를 보호하기 위해서는 비연결성과 비추적성이 보장되어야 한다. 3.3절의 모네로에서는 링 서명 기법으로 비추적성을, 스텔스 주소 스킴으로는 거래의 비연결성을 향상시킨다.

3. 블록체인 플랫폼과 프라이버시 보호 기법들

3.1 대시(Dash)

다크코인(DarkCoin)으로 이미 알려진 대시는 2014년 1월 18일에 상장되었으며 오픈소스로 구현된 P2P 네트워크 기반의 암호화폐이다[8]. 대시는 비트코인의 소프트웨어 포크를 한 형태로, 알트코인(altcoin)의 한 종류이다. 2019년 7월 현재 대시는 전체 암호화폐 시장에서 15위의 시가총액과 18위의 거래량을 보유하고 있다[9]. 비트코인과 대시의 가장 큰 차이점으로는 대시는 비트코인에 비해 강력한 프라이버시 보호 기능을 갖추고 있고 마스터 노드로 인한 분산화된 통치 시스템 (decentralized governance system)이라는 점이다. 이러한 시스템적 특징으로 대시는 최초의 성공적인 다오(DAO, Decentralized Autonomous Organizations) 플랫폼이라 할 수 있다. 대시는 합의 알고리즘으로 작업 증명(PoW, Proof of Work)과 서비스 증명(PoSe, Proof of Service)을 통합하여 사용한다.

작업증명 합의 알고리즘의 경우 비트코인과 동일하다. 채굴자들은 해시 함수 조건에 맞는 어떠한 난수 값을 찾기 위해 시도하고 적절한 난수 값을 찾으면 자신이 생성한 블록을 체인에 등록할 수 있는 권한을 가진다. 네트워크의 다른 노드들이 그 블록을 유효하다고 판단하면 채굴자는 보상을 받는다. 이 때 사용하는 해시 함수는 비트코인에 적용된 해시 함수와는 다른 X11 해시 알고리즘[10]을 사용한다. 대시는 일반 노드, 채굴자 노드 외 마스터 노드를 두고 있는데 이 마스터 노드가 네트워크에 중요한 서비스를 제공하기 때문에 서비스증명 합의 알고리즘이란 특징을 갖는다.

마스터 노드란 비트코인에서의 풀 노드(full node) 역할을 하면서 동시에 프라이빗샌드(PrivateSend), 인스턴트샌드(InstantSend) 등의 특수한 기능을 하는 거래를 생성할 수 있는 노드를 말한다. 채굴자 노드가 한 블록을 생성하면 블록 보상은 채굴자 노드:마스터 노드:예산 시스템 = 45:45:10으로 분배된다. 또한 마스터 노드는 전체 네트워크를 관찰하면서 채굴자 노드에 의해 생성된 블록을 거부할 수 있는 권한도 가진다. 이와 같이 마스터 노드는 강력한 권한을 부여받기 때문에 채굴자 노드와 달리 아무나 될 수 없고 항상 1000DASH의 자산을 지닌 노드만 그 자격을 얻는다.

노드의 익명성, 거래의 프라이버시 보호를 위해 대시에서는 프라이빗샌드(PrivateSend)라는 특수한 거래를 사용한다. 마스터 노드만 생성할 수 있는 대시의 프라이빗샌드 거래는 코인조인(CoinJoin) 기법에서 확장된 기법으로 다크코인의 다크샌드(DarkSend)에서 2016년 프라이빗샌드로 명칭이 변경되었다[11]. 거래의 한 종류이며 마스터 노드에 의해서만 생성된다. 마스터 노드는 여러 개의 거래를 모아서 하나의 익명 거래인 프라이빗샌드로 병합하는 믹싱 기능을 수행할 수 있다. 이 익명 거래를 통해서 각 노드는 자신의 거래에 참여하지 않는 외부 노드로

부터 프라이버시와 익명성을 보호받는다. 자세한 거래 생성 과정은 다음과 같다[11].

먼저 노드는 대시 코어 지갑(dash core wallet) 프로그램에서 생성할 프라이빗샌드 거래에 대해 설정할 수 있다. 얼마만큼의 코인을 이 거래 입력 값으로 할 것인가, 믹싱 라운드는 얼마로 할 것인가에 대하여 설정하는데, 이 믹싱 라운드는 2~8 사이의 값으로 설정가능하다. 프라이빗샌드는 거래 입력 코인을 0.01대시, 0.1대시, 1대시, 10대시 코인의 작은 단위로 분할한다. 믹싱 시작 버튼을 누르면 노드의 지갑은 한 마스터 노드에게 프라이빗샌드 요청을 보낸다. 이때 선택된 마스터 노드는 요청을 보낸 노드에 대하여 아무런 정보를 받지 못하기 때문에 거래 송신자의 프라이버시는 보호된다. 마스터 노드가 요청을 수락하는 메시지를 보내면 송신자는 원하는 입력 값과 출력 값을 마스터 노드에게 전송한다. 믹싱 작업은 프라이빗샌드를 원하는 다른 노드들을 더 모아서 이루어진다. 모든 노드들의 요청 값은 메모리 큐에 저장된다. 설정한 만큼의 믹싱 라운드를 거친 후에 마스터 노드는 생성한 병합 거래를 메시지로 보여준다. 거래 송신자는 분할된 각 입력 값에 대하여 서명을 한다. 그리고 각 입력 값들은 거래 수신자의 주소로 전송된다. 만약 거래 송신자와 수신자가 동일 노드인 경우 해당 노드 지갑에 속해있는 다른 주소로 전송하기 때문에 코인의 흐름은 연결되지 않는다.

3.2 Zcash

Zcash는 비트코인에 비해 상대적으로 높은 프라이버시 제공을 목적으로 한 암호화폐로써 제로코인(Zerocoin) 프로토콜이 제로캐시(Zerocash) 시스템으로 개선되었고 2016년에 Zcash 암호화폐로 구현되었다. 역시 비트코인에서 소프트웨어 포크를 한 형태이며 Zcash는 암호화폐 시장에서 22위(2019년 7월 현재[12])에 해당한다. 간단하게 설명하자면, Zcash는 기존의 공개 코인을 비공개 코인 리스트에 추가함으로써 암호화하여 해당 코인의 흐름을 차단하는 방식이다. 합의 알고리즘으로 Equihash 작업증명을 채택하고 있다. Zcash의 가장 큰 특징으로는 무엇보다도 영지식증명(Zero-Knowledge Proof)의 한 기법인 zk-SNARKs[13]를 사용한다는 점이다. 거래의 송수신자와 거래내역은 모두 암호화되고 오직 거래 생성 시간만 다른 노드에게 공개된다. 암호화된 상황에서 한 노드가 자신의 거래 유효성을 입증하기 위해 zk-SNARKs를 사용한다. 따라서 Zcash는 분권화된 익명의 지급결제 체계(DAP schemes, Decentralized Anonymous Payment schemes)로 분석된다. 또한 악의적인 공격자의 이중 지불 공격 방어가 가능하다. 추가적으로 Zcash에서는 스텔스 주소(stealth address) 스킴을 사용하여 거래 수신자 주소를 보호하는데 이 스킴은 3.3.2절에서 자세히 설명한다.

Zcash의 거래는 기존의 코인 송금 외에 공개 코인을 노트(note)라고 부르는 보호된 값으로 변환하는 작업(commitment)을 수행하기도 한다[14]. 노트를 다시 공개 코인으로 변환하거나 다른 노드에게 전송할 수도 있다. zk-SNARKs 증명을 생성하는 프로토콜을 JoinSplit이라 하며, 이 프로토콜은 생성된 노트들을 관리하기 위한 목적으로 머클트리(Merkle tree) 자료구조를 이용한다. Zcash 프로토콜 명세서(Zcash Protocol Specification)[15]는 이 트리를 노트 위임 트리(note commitment tree)라고 명칭한다. 노트가 트리에 존재한다는 것은 노트가 유효하고, 이전에 다른 거래에서 사용되지 않았으며, 이 거래 출력 값의 합은 입력 값의 합과 일치한다는 사실이 이미 증명되었음을 의미한다. 즉 비트코인에서의 UTXO 풀(Unspent Transaction Output pool)과 같은 역할을 한다. 노트가 생성될 때마다 리프노드가 하나씩 사용되고 두 번 사용되지 않는다. 비트코인의 UTXO 풀과 다른 점은 이중 지불 공격을 방어하기 위한 목적은 갖고 있지 않다는 점이다. Zcash 네트워크의 모든 노드는 이 트리를 저장하고 있다.

Zcash는 보안, 프라이버시, ASIC 채굴 저항 등의 이유로 Equihash 작업증명[16]을 선택하였다. Equihash 작업증명은 3개의 파라매터 값과 1개의 시드 값으로 퍼즐을 풀어야 한다. Equihash 퍼즐은 일반화 생일 문제(GBP, Generalized Birthday Problem)에 대한 워그너(Wagner)의 알고리즘에서 찾을 수 있다. CryptoLUX 과학자들[17]에 따르면 이 합의 알고리즘은 특수한 채굴 하드웨어를 사용하는 최상위 채굴자 몇 명이 채굴 과정을 독점하는 상황을 방어함으로써 디지털 통화의 “민주화”에 기여한다.

Zcash에서 zk-SNARKs라 불리는 영지식증명(Zero-Knowledge Proof) 기법을 사용한다. 영지식증명(Zero-Knowledge Proof)이란 직접적으로 데이터를 공개하지 않고 연산사실 만으로 데이터 지식을 증명하는 기법이다. 영지식증명은 동형암호(homomorphic encryption)의 한 종류이며 1985년에 샤피(Shafi) 등[18]에 의해 발표되었다. zk-SNARKs는 이 영지식증명 기법 종류 중 하나로 zero-knowledge Succinct Non-Interactive Arguments of Knowledges의 약어이며 증명 과정이 쉽고 간결한 것이 장점이다. 투명한 주소(transparent addr.)를 사용한 거래는

비트코인과 같이 주소 값과 거래 내용이 공공장부에 모두 공개되지만 JoinSplit 거래를 이용하면 소유하고 있는 공개 코인 금액과 주소 등의 거래 내용이 모두 암호화되게 된다. 이때 개인키가 없이 암호화된 내용을 볼 수는 없다. 채굴을 하거나 보호 주소(shielded addr.)끼리 거래를 생성할 때 암호화된 거래에 대해 복호화 하지 않고 그 유효성을 입증하기 위해서 zk-SNARKs 기법을 사용한다.

노트 값에는 공개 코인에서 변환된 금액과 이 노트를 생성한 노드의 보호된 주소의 일부인 지불 키(paying key)가 있다. 그리고 노트를 생성하고 유효함을 증명하기 위해서는 지출 키(spending key)가 사용된다. 변환 거래가 블록에 채굴되기 위해서는 머클트리의 고정된 입력 노트 위치(note position)와 입력 노트의 고유 값인 nullifier가 사용된다. 이 nullifier을 계산할 때 지출 키가 사용되므로 이것은 지출 키에 대한 지식 없이는 계산하는 것이 불가능하다. 즉, 입력 노트를 생성한 노드가 적절한 지출 키를 알고 있고 실제 노트에 대한 소유자임을 뜻한다. 각 거래는 입출력 값 등을 포함하면서 동시에 0개 이상의 JoinSplit 설명 값(JoinSplit description)도 포함한다. 이 JoinSplit 설명은 최대 2개의 입출력 노트를 가질 수 있다. 입력 노트의 nullifier은 이중 지불 방지를 위해 공개되고 출력 노트의 위임(commitment) 값도 공개된다. 제 3자는 입력 노트의 nullifier 값의 공개로 이 노트가 소비되었음을 확인할 수 있다. 이때 역시 직접적인 nullifier 값의 공개가 아닌 해시 값 등으로 값에 대한 지식을 증명한다. 네트워크의 증명자(또는 채굴자)는 각자 nullifier 집합(set)을 저장하고 있으며 JoinSplit 거래가 유효하면 그 입력 노트의 nullifier 값을 집합에 저장한다. 어떤 거래의 입력 노트에 대한 nullifier 값이 이미 집합에 있다면 그 거래는 이중 지불 노트로 판단되어 거부당한다.

3.3 모네로(Monero)

크립토노트(CryptoNote) 프로토콜을 구현한 여러 플랫폼 중 가장 유명한 모네로는 2014년 4월에 첫 기원 블록(genesis block)이 발행되었다. 공식 홈페이지에서는 모네로를 '안전하고, 개인적이고, 추적이 불가능한 화폐'로 소개하고 있다[19]. 모네로는 스텔스 주소, 링 서명, 링 CT, 코브리(Kovri) 프로토콜을 이용하여 거래의 송수신자와 거래 내용, 거래의 네트워크 기록까지 무분별하게 공개되지 않도록 보호한다. 모네로는 현재 전체 암호화폐 시장에서 14위를 기록하고 있고[20], 합의 알고리즘으로는 크립토나이트(CryptoNight) 작업증명을 채택하였다.

크립토노트 프로토콜은 블록체인 거래의 출처를 숨기기 위하여 처음으로 링 서명 사용을 제안한 디지털 화폐로 2012년 12월에 발표되었다[21]. 크립토노트를 사용하면 거래 송신자가 자신의 개인키와 그룹 다른 멤버들의 공개키를 사용하여 링 서명을 구성한다. 관찰자는 그룹 멤버 중 한명인 노드가 거래에서 전송되는 입력 코인의 계좌 주소에 해당하는 비밀 키를 소유하고 있고 그것을 소비하려 한다는 것을 확신할 수 있다. 하지만 거래를 생성한 정확한 노드는 누구인지 알 수 없다. 수신자 주소도 일회용 주소를 사용하기 때문에 거래 수신자에 대한 코인의 흐름도 파악하기 어렵다. 더 효과적인 프라이버시 보호를 위해 모네로는 크립토노트 프로토콜에 거래에서 취급하는 코인의 금액까리 숨기는 링 CT 기법을 추가로 적용하였다. 또한 I2P(The Invisible Internet Project) 네트워크의 구현된 형태인 코브리 프로토콜[22]로 여러 네트워크 공격들로부터 안전한 거래를 보장한다.

크립토나이트 작업증명[23]은 바이트코인(Bytecoin) 개발팀과 모네로 개발팀의 합작으로, 합의 과정의 모든 참가자가 동등한 투표권을 갖게 하는 평등주의를 지향하는 합의 알고리즘이다. 내장된 CPU 명령을 일반적인 PC에 적합한 작업증명 가격 책정 함수와 함께 사용한다. 이 작업증명 가격 책정 함수는 새로운 메모리 기반 알고리즘을 기반으로 구현되었으므로 CPU와 GPU 채굴에 대해 대략 동등하게 효율적이며 ASIC 채굴은 제한하도록 설계되었다.

모네로의 익명성, 프라이버시 보호 스킴들을 차례로 살펴본다. 3.3.1 절에서는 링 서명을, 3.3.2 절에서는 스텔스 주소, 마지막 3.3.3절에서는 링 CT에 대해 언급한다.

3.3.1 링 서명(Ring signature)

일반적인 디지털 서명 (예를 들어, ECDSA 등) 검증 프로세스에는 서명자의 공개키가 포함된다. 공개키를 이용하여 실제로 서명자는 서명을 생성한 비밀키를 소유하고 있다는 것을 증명할 수 있다. 따라서 서명 검증자는 서명에 생성된 공개키가 어느 것인지 반드시 알아야 한다. 하지만 비트코인과 같은 공공장부에서는 이러한 기능이 관찰자에게 코인의 흐름을 파악할 수 있게 하여 프라이버시 유출 문제를 낳는다.

모네로는 비트코인에서의 추적가능성을 보완하기 위해 2001년 발표된 링 서명[24]을 사용한다. 서명자는 각각의 비밀키, 공개키 쌍을 가진 그룹에 속해있고, 서명자 자신의 비밀키와 서명자가 선택한 그룹의 다른 공개키들

을 사용하여 링 서명을 생성한다. 이때 다른 공개키 소유자의 동의 또는 참여는 필요하지 않지만 이 공개키에 연결된 계좌에는 서명자가 송금하는 코인과 같은 금액의 코인이 보유되어 있어야 한다. 간단한 프로세스는 다음과 같다[24][25].

먼저 송신자는 링 서명의 크기를 결정하게 되는데 이 크기는 블록체인으로부터 정해진다. 링 크기가 클수록 거래 크기도 커지고 수수료도 높아진다. 송신자는 거래에 대해서 개인키로 서명하고 네트워크로 전송한다. n명의 그룹 멤버 공개키($P_1, P_2, ..., P_n$)와 거래 생성자의 개인키 S_i, 서명 생성 메시지 m으로 생성된 서명 값은 $\sigma = Enc(m, S_i, P_1, ..., P_n)$로 표현 가능하다.

일반적인 디지털 서명 방식과 주된 차이점은 서명자의 비밀키로 서명을 생성하지만 검증자가 서명자의 정확한 신원을 확인할 수 없다는 점이다. 이 접근법은 트랜잭션 작성자가 트랜잭션에서 지정된 금액을 사용할 수 있음을 증명하지만 그의 신원 정보는 링 서명에 사용한 공개키를 가진 사용자와 구분할 수 없게 한다. 또한, 두 명의 노드가 같은 공개키 세트를 사용하여 링 서명을 작성해도 동일한 개인키를 사용하지 않는 한 서명이 달라진다.

3.3.2 스텔스 주소(Stealth Address)

블록체인 네트워크에서는 모든 노드들의 거래가 네트워크에 투명하게 공개되기 때문에 제 3의 관찰자가 거래 수신자의 공개키 주소를 검색하여 그가 다시 다른 거래에서 코인을 소비하는 것을 확인함으로써 프라이버시 문제가 발생한다. 비트코인에서는 한 노드의 주소가 관찰자에 의해 추적이 되는 것을 막기 위한 방어책으로 매 거래 시 한번만 사용하는 일회용 주소 사용을 권장하고 있다. 하지만 이러한 방법은 하나의 공개키 주소를 사용하는 것보다 계좌 관리가 불편하다. 크립토노트는 단일 공개키로부터 파생된 여러 개의 고유한 일회용 키들을 통해 각각의 거래에 대하여 이러한 딜레마를 해결한다. 이 방법은 DHKE (Diffie- Hellman Key Exchange) 프로토콜을 이용하는 스텔스 주소 기법이다. 정확히는 ECDH 키 동의 (Elliptic Curve Diffie- Hellman Key Agreement) 기법을 사용한다.

[24]에서 자세한 스텔스 주소 생성 과정에 대해 설명한다. 모네로 계정을 만들면 비밀 뷰키(private view key, VK_{priv}), 비밀 지출키(private spend key, SK_{priv}), 공개 주소가 같이 생성된다. SK_{priv} 키는 거래를 전송하는데 사용되고, VK_{priv} 키는 사용자의 계정으로 전송된 거래들을 보고자 할 때 사용한다. 공개 주소는 코인을 받을 때 사용한다. VK_{priv} 키만 사용하면 회계 또는 감사 목적의 거래 확인용 지갑으로 사용가능하다. 사용자는 자신의 VK_{priv} 키를 원하는 사람과 공유하여 잔액 확인 권한을 부여할 수도 있다. 모네로 거래는 기본적으로 비공개이며 선택적으로 반투명하다.

거래의 두 참여자가 수신자의 공개키에서 공통의 키를 공유하여 동일한 스텔스 주소를 생성할 수 있다. 먼저 송신자가 주소를 생성하는 과정은 다음과 같다. 타원 곡선 기준점(base point)은 G라 할 때 송신자는 이번 거래의 일회용 랜덤 스칼라 값 r을 선택하여 $R = r \cdot G$값을 연산한다. 수신자의 개인키 쌍은 $VK_{priv} = a$, $SK_{priv} = b$라고 하면 공개키 쌍은 $VK_{pub} = a \cdot G = A$, $SK_{pub} = b \cdot G = B$이 된다. 생성된 일회용 스텔스 주소 P는 다음과 같다. $P = H(rA)G + B$. 이때 H는 해시 함수를 뜻한다.

수신자가 자신의 키로 스텔스 주소 P'을 생성하는 과정은 다음과 같다. 먼저 송신자로부터 R을 수신한다. 그리고 $VK_{priv} \cdot R = aR$을 계산한다. 송신자와 마찬가지로 해시 연산 후 SP_{priv}값인 b를 더한다. 이 값은 일회용 개인키 x가 된다. $x = H(aR) + b$. x에 기준점 G를 곱하면 최종적으로 계산한 스텔스 주소 값은 $P' = xG = H(aR)G + bG$이고 수신한 거래에 명시된 주소 값과 일치하는지 확인한다.

3.3.3 링 CT(Ring Confidential Transaction)

링 CT[27]는 Ring Confidential Transactions의 약어로 모네로의 거래에서 송신자 정보, 다뤄지는 금액을 모두 숨기는 기법이다. 링 CT는 2017년 1월 블록 #1220516에서 처음 구현되었고, 2017년 9월 이후 이 기능은 네트워크의 모든 거래에서 필수 항목이 되었다.

링 CT의 기본적인 원리는 페더슨 위임(Pedersen commitment)[26][27]을 사용하며 Zcash와 유사하다. 링 CT 적용 이전에 거래를 생성할 때 노드는 링 서명 설정 단계에서 공개키-금액 쌍을 전송한다. 링 CT를 사용하게 되면 거래의 입력, 출력 값의 공개키-금액 쌍을 위임 기법을 사용하여 암호화한다. 외부 네트워크에서 보았을 때 암호화된 전체 거래에서 입출력 주소와 거래 금액은 볼 수 없다. 대신, 입력 위임 값의 합과 출력 위임 값이 동일하면 유효한 거래라고 판단한다.

뇌터(Noether) 등[28]이 제안한 MRL-0005 문서에 따르면 그레그(Greg)[29]가 제안했던 기존의 링 CT을 수정하

여 모네로에 맞는 링 CT를 적용할 필요성이 있다. 따라서 이 문서에서는 향상된 링 서명을 사용하여 MLSAG (Multilayered Linkable Spontaneous Anonymous Group signature) 링 CT에 대하여 언급을 하고 있다.

3.4 하이퍼레저 패브릭(Hyperledger Fabric)

사설 블록체인을 채택한 대표적인 플랫폼으로 하이퍼레저 패브릭이 있다. 패브릭은 리눅스 재단의 후원하에 운영되는 오픈소스 블록체인 기술인 하이퍼레저의 프로젝트 중 하나이다. 패브릭은 탄력성(resiliency), 유연성(flexibility), 확장성(scalability) 및 기밀성(confidentiality)을 목표로 하는 새로운 블록체인 구조를 도입했다[30]. 패브릭은 모듈화 되어 있으며 표준 프로그래밍 언어로 작성된 분산 응용 프로그램의 실행을 지원한다. 따라서 패브릭은 허가형 블록체인을 위한 최초의 분산 운영체제라고 할 수 있다.

패브릭은 신뢰할 수 없는 환경에서 신뢰할 수 없는 코드를 분산 실행하기 위하여 기존 블록체인 플랫폼들과는 다른 실행(execute)-신청(order)-검증(validate) 패러다임을 따른다. 패브릭 어플리케이션은 스마트 계약에 해당하는 체인코드(chaincode)와 보증 정책(endorsement policy), 크게 두 부분으로 나뉜다. 먼저 체인코드는 어플리케이션 로직을 구현하고 실행단계에서 실행되는 프로그램 코드이다. 패브릭의 핵심부분이며 신뢰도에 상관없이 어느 개발자든 구현이 가능하다. 전반적인 블록체인 시스템과 매개변수를 유지 관리하기 위한 시스템 체인코드도 존재한다. 그리고 보증 정책은 검증단계에서 이뤄지며 신뢰된 어플리케이션 개발자에 의해서만 수정이 가능하다. 이 정책에 의해 선택된 개발자 피어가 일반 클라이언트의 거래를 실행 후 보증 결과를 기록한다.

공개 블록체인 모델들과 가장 큰 차이점 중 하나는 패브릭만의 구성요소인 멤버쉽 서비스 공급자, MSP (Membership Service Provider)이다. 이 구성요소는 시스템(클라이언트, 피어 및 주문자)의 모든 노드의 ID를 유지·관리하며 인증 및 권한 부여에 사용되는 노드 자격 증명을 발급한다. 패브릭은 허가형 블록체인 네트워크이기 때문에 일반적으로 디지털 서명을 사용한 인증 메시지를 통해 노드끼리 상호작용을 한다. 멤버쉽 서비스는 각 노드의 거래 인증, 거래 무결성 확인, 보증을 서명·확인 등의 작업을 하는 구성요소이다. 기본 MSP 구현은 디지털 서명 기반의 표준 PKI 방법을 채택하였으며 상업용 인증기관(CA)을 이용하기도 한다.

다른 플랫폼에 비해 허가형 블록체인 모델이기 때문에 멤버쉽 서비스로 인한 무분별한 프라이버시 노출 위험은 적은 편이나 더 세부적인 익명성과 프라이버시 보호를 위하여 패브릭에서는 채널, 비밀 데이터 모음 등의 기법을 채택하고 있다.

3.4.1 채널(Channel)

하이퍼레저 패브릭 채널은 비공개 및 기밀 거래를 실행하기 위해 특정 네트워크 구성원 간의 통신에 대한 개인 서브넷 또는 서브 블록체인으로 말할 수 있다[31]. 네트워크상의 각 거래는 채널에서 실행되며 채널의 각 피어들은 인증되어야 하고 권한이 있어야한다. 채널에 참여하는 각 피어는 MSP가 제공하는 자체 ID를 가지며 채널의 기존 피어들에게 신원을 인증해야 한다. 프라이버시 관점에서 볼 때, 채널은 블록체인 네트워크 참여자의 하위 그룹이 여러 개의 공통된 거래들을 공유하는 경우에 유용하다.

채널은 특수한 구성 블록(configuration blocks)에 의하여 유지 관리된다. 각 구성 블록에는 전체 채널 설정 사항이 포함되며 다른 거래는 포함되지 않는다. 채널 구성에는 MSP 정의, 운영 규칙, 채널 리소스에 대한 접근 정책 등이 포함된다. 채널에 속한 피어들에서만 거래를 공유하기 때문에 거래에 대한 기밀성 및 프라이버시가 보호된다. 채널은 대용량의 데이터를 효율적으로 공유 할 수 있는 확장성도 제공한다.

3.4.2 비밀 데이터 모음(Private Data Collection)

채널에 있는 그룹 피어들 중 일부 선택된 피어들 외에는 데이터를 비공개로 유지해야하는 경우 데이터에 접근 가능한 피어들만으로 구성된 새 서브 채널을 만들 수 있다[32]. 그러나 별도의 채널을 많이 만들면 추가 관리 오버헤드 비용이 발생하며 모든 채널 참가자에게 거래 내용 데이터의 일부분만을 비공개로 하는 경우는 불가능하다. 그래서 패브릭 v1.2부터는 개별 채널을 만들지 않고도 채널의 서브 그룹 멤버들에게만 개인 데이터를 보증, 수용 기능을 허용하는 비밀 데이터 모음을 생성할 수 있다. 비밀 데이터 모음은 실제 비밀 데이터(the actual private data)와 그 데이터의 해시 값(the hash of that data)으로 이루어져 있다. 실제 비밀 데이터는 SideDB와 같은 개인 데이터베이스에 저장되어 있는 데이터이며, 해시 값은 데이터에 대한 거래 발생의 증거로 사용되며 채널

(표 1) 익명성과 프라이버시 보존을 위한 블록체인 플랫폼과 핵심 기술들
(Table 1) Blockchain platforms and core techniques for anonymity and privacy protection

Type of Blockchain	Platform name	Consensus Alg.	for Privacy	for Anonymity		Relative Performance
				Sender	Receiver	
Public permission-less Blockchain	Dash	PoW, PoSe	PrivateSend			high
	Zcash	Equihash PoW	zk-SNARKs		Stealth Addr. scheme	low
	Monero	CryptoNight PoW	Ring CT	Ring sign.	Stealth Addr. scheme	moderate
Private permissioned Blockchain	Hyper-ledger Fabric	PBFT	Membership Service Provider, Channel			high
			Private Data Collection (SideDB etc.)			

의 모든 피어들끼리 공유하는 공공 장부에 기록된다. SideDB는 개인 데이터에 대한 참조를 포함하는 거래가 생성될 때 공공 장부와 함께 업데이트된다.

비공개 거래를 익명 클라이언트 인증 기법들과 결합하여 거래 생성자의 신원과 공공 장부의 해시 데이터 간의 연결이 누출되지 않도록 할 수 있다. 비공개 데이터의 업데이트 패턴 또한 민감한 정보가 될 수 있다. 하이퍼레저 패브릭 시스템은 실제 개인 데이터에 대한 무단 접근을 방어하지만 네트워크 참가자는 공공 장부에 기록되는 개인 데이터의 해시 값을 통해 수정되는 시기가 관찰이 가능하다.

4. 보안적 측면에서 적용 기법들 비교·분석

3절에서는 익명성·프라이버시 보호에 초점을 둔 블록체인 기반 플랫폼 4가지(대시, Zcash, 모네로, 하이퍼레저 패브릭)와 각 플랫폼의 적용 기법에 대하여 살펴보았다. 각 적용 기법들마다 다 다른 특징과 암호학적 연산을 사용하기 때문에 보안적인 측면에서 분석하는 연구가 필요하다. 본 절에서는 3절의 내용에 더불어 [4], [14]의 논문을 바탕으로 각 시스템과 기법들의 장단점 및 성능 등을 분석하였다.

표 1을 살펴보면 먼저 각 플랫폼을 공개 블록체인과 사설 블록체인으로 분류하였다. 공개 블록체인 플랫폼에는 대시, Zcash, 모네로가 있고 하이퍼레저 패브릭이 사설 블록체인 플랫폼에 해당한다. 3절에서 논의하였던 각 플랫폼의 합의 알고리즘도 표 1에 나타내었다. 공개 블록체인 플랫폼들은 조금씩 다르지만 대체로 기존 비트코인의 작업증명 알고리즘을 수정한 형태를 채택하고 있음을 알 수 있다.

플랫폼들의 프라이버시와 익명성 보호 기법들도 정리를 표 1에 나타나는데 그 중 익명성 보호 기법들은 보호 대상에 따라 세부적으로 분류하였다. Zcash의 zk-SNARKs 기법 같은 경우 거래 내용 프라이버시와 익명성은 송신자의 정보만 보호한다. 패브릭은 공개 블록체인 플랫폼들과 다른 유형의 블록체인 플랫폼이라서 표 1의 내용에서도 많은 차이를 보인다. 일단 MSP를 통해서 내부 네트워크의 모든 내용(송수신자 정보, 거래 정보)이 모두 보호되기 때문에 3가지 보호 기법의 범주에 포함하였다. 마지막으로 [4]에서 주요 프라이버시 보호 암호 기법들의 상대적인 속도에 대하여 분석하였다. 이 분석을 기반으로 표 1에 각 플랫폼의 성능에 대하여 평가한다.

4.1 대시의 프라이빗샌드

대시의 프라이빗샌드 거래는 네트워크의 코인 기록을 삭제하는 새로운 분산형 믹서이다. 프라이빗샌드와 같은 보호 기법이 없으면 프라이버시 측면에서는 이전에 연관된 거래가 없고 기록이 적은 코인만 점점 더 가치 있게 될 것이다[33]. 하지만 프라이빗샌드라는 특수한 거래를 통해 강한 프라이버시 보호를 원하는 노드들은 자신의 거래내역 흐름을 끊고 새로운 코인의 기록을 생성한다.

프라이빗샌드의 믹싱 기능은 특정한 기준을 통과한 신뢰할 수 있는 마스터 노드에 의해 처리되기 때문에 기존의 코인조인 기법의 단점을 보완한 형태이다. 추가적으로 강력한 보안을 위해 대시는 거래 서명 시 타원곡선기반 블라인드 서명 스킴(ECC-based blind signature scheme)을 사용한다.

다른 믹싱 소프트웨어에서는 공격자가 거래 수수료를 이용하여 네트워크에서 노드를 식별 할 수 있다. 이러한 공격을 방어하기 위해 모든 입출력에 대한 서명이 완성되어 해당 거래가 유효해지면 DSTX라는 특수 메시지를 마스터 노드가 공표한다. 네트워크는 이러한 메시지를 추적하여 마스터 노드가 수수료를 지불하지 않고 N시간마다 하나의 프라이빗샌드 거래를 전송할 수 있도록 한다. 이 기술을 사용하여 거래에서 수수료를 분리하여 타이밍 공격을 방어할 수 있다.

프라이빗샌드 거래 생성 시 거래에 참가하는 노드들에 대한 정보가 직접적으로 마스터 노드에게 전달되지 않으며 병합된 거래는 외부에서 내용 확인이 불가능하다. 또한 각 노드의 지갑에는 1000개의 주소가 저장되어 있다. 거래 송신자가 송금 후 잔액을 받는 등의 이유로 코인을 받는 거래 생성 시 출력 주소는 입력 주소와 다른 저장된 주소가 사용된다. 그리고 모든 주소가 다 사용되면 지갑은 새로 주소를 더 생성한다. 프라이빗샌드 기법은 거래 송수신자의 익명성과 거래 내용 프라이버시까지 보호하는 기법이다.

프라이빗샌드의 성능은 다른 기법들에 비해 실행 속도가 빠른 편이므로 좋다고 할 수 있다. 많은 연산을 요구하는 암호 프로토콜이 적용된 것이 아닌 여러 개의 거래를 병합한 믹싱 거래(mixing transaction)를 생성하는 것이기 때문에 시간은 비교적 적게 소요된다.

4.2 Zcash의 zk-SNARKs

Zcash는 노드의 프라이버시와 익명성 보장을 위해 의무적인 투명성이 아닌 선택적 투명성을 기반으로 하고 있다. zk-SNARKs를 통해 모든 데이터를 암호화하고 권한이 있는 노드에게만 복호화 키를 부여함으로써 특정 노드만 데이터를 열람하도록 한다. 이는 기존의 공개 블록체인 플랫폼에서는 불가능 했던 방식이다. Zcash 노드는 JoinSplit 프로토콜로 공개 코인을 새 노트로 변환하는 위임(commitment)를 생성하여 암호화한다. 암호화된 위임에서 노트의 금액과 같은 정보들은 비공개된다. 거래에서 프라이버시가 보호되는 것이다. 어떤 위임을 소비하는 거래에서도 직접적으로 노트에 대한 정보를 공개하는 것이 아니라 노트 소유주만이 할 수 있는 연산을 채굴자와 같은 인증자에게 증명함으로써 영지식증명으로 노트 소비의 유효성을 인증한다.

노드의 익명성을 위해 Zcash 거래에 사용되는 주소로는 두 가지 유형이 있다[34]. 네트워크 모든 노드들에게 공개되는 투명한 주소(transparent address)인 t-addr은 항상 “t”로 시작한다. TVP (Transparent Value Pool)과 상호작용하여 거래 내용을 공개한다. 또 다른 방식의 주소는 항상 ″z″로 시작하며 ″z-addrs″라고도 한다. 이 주소는 보호된 주소(shielded address)이며 비공개 값이다. 입출력 주소의 유형에 따라 기본 거래의 유형이 4가지로 나뉜다. 공개형(public), 비밀형(private), 보호형(shielding), 비보호형(deshielding). 공개형은 t->t, 비밀형은 z->z, 보호형은 t->z, 비보호형은 z->t 이다. 노드는 다양한 거래 옵션을 선택하여 원하는 레벨의 익명성을 보호받을 수 있다. 그리고 스텔스 주소 스킴으로 투명한 거래에서도 수신자의 익명성을 보장한다.

zk-SNARKs의 대표적인 단점은 파라매터 값 설정 단계 및 복잡한 암호 스킴 때문에 발생하는 느린 연산 속도이다. 영지식증명을 사용하는 플랫폼 중 하나인 제로코인[35]의 저자는 지식에 대한 이중 이산대수 증명이 사용되기 때문에 상당한 계산 노력이 필요하다고 언급하였다. 영지식증명의 효율성에 대한 연구는 계속되고 있지만, zk-SNARKs의 실제 소프트웨어 구현은 여전히 느린 것으로 보여진다. Zcash의 기술 설명 블로그에서는 Jubjub[36]이란 타원 곡선으로 zk-SNARKs의 낮은 성능에 대한 개선 방안을 논의하기도 했다.

4.3 모네로의 링 서명 기법 등

모네로는 비트코인에서 익명성 보장을 위해 링 서명 사용을 처음으로 제안한 디지털화폐 크립토노트의 구현 시스템 중 하나이다. 크립토노트 프로토콜에 언급된대로 링 서명으로 거래 송신자의 정보를 숨기고 스텔스 주소로 거래 수신자의 정보를 숨긴다. 더 완벽한 익명성과 프라이버시를 위해 모네로 개발팀은 2017년에 링 서명 기반의 비밀 거래인 링 CT를 적용하였다. 게다가 노드간의 통신 중 네트워크 정보가 노출되는 것을 막기 위해서 코브리 프로토콜도 적용하였다.

보편적인 링 서명의 가장 큰 단점은 이중 지불 공격을 방어할 수 없다는 것이다. 일반적으로 비트코인의 경우 채굴자들이 채굴과정 중에 거래의 이중 지불 여부가 간

단하게 확인이 가능하다. 하지만 링 서명을 사용하는 경우 거래 생성자가 불분명하기 때문에 이중 지불 공격의 가능성이 높다. 이를 위해 크립토노트는 키 이미지(key image)라는 값을 사용한다. 거래가 생성될 때마다 스텔스 주소 기법으로 일회용 주소를 생성하는데 키 이미지 I 값은 송신자의 SP_{priv}키 b를 스텔스 주소 P의 해시 값과 곱한다. $I=b \cdot H(P)$. 거래마다 스텔스 주소는 달라지고 송신자는 키 b를 공개하지 않을 것이기 때문에 키 이미지는 각 거래에 대해 유일무이한 값이 된다. 노드는 이전에 사용된 모든 키 이미지의 목록을 유지·관리하고 이전에 사용된 키 이미지에 대한 거래는 거부하는 방식으로 거래의 이중 지불을 확인할 수 있다. 그 외에 일회용 링 서명(one-time ring signature)라는 기법도 적용하여 이중 지불을 막는다.

스텔스 주소 스킴으로 송신자와 수신자는 랜덤한 스칼라 값 r과 수신자의 VK_{priv}값인 a를 직접적으로 교환하지 않고 동일한 주소 값을 생성한다. 주소 생성 프로세스에는 수신자의 개인키가 포함되므로 제 3자는 송신자가 생성한 일회용 값과 수신자의 고유한 공개 주소 사이의 어떠한 연결을 발견할 수 없다. 송신자가 수신자에게 거래에 대하여 직접적으로 증명을 하고 싶다면 랜덤한 스칼라 값 r을 공개하거나 그에 대한 영지식증명 기법을 사용하면 된다.

모네로의 단점이라고 하면 거래의 크기라고 할 수 있다. 링 CT의 사용으로 이전보다 좀 더 복잡한 연산이 사용되게 되므로 거래의 크기는 커질 수밖에 없다. 차후 모네로가 암호화폐뿐만 아니라 다른 응용 분야에 적용되기 위해서는 거래의 크기가 개선되어야 할 것이다. 하지만 성능은 나쁘지 않다고 할 수 있다. 모네로의 메인 기술은 링 서명인데 링 서명의 연산 자체는 영지식증명 만큼 많은 연산량을 필요로 하지는 않기 때문에 중간 정도의 성능을 갖고 있다고 평가할 수 있다.

4.4 패브릭의 채널 등

마지막으로 하이퍼레저 패브릭은 대표적인 사설 블록체인 기반 플랫폼이다. MSP를 두고 권한이 있는 노드들만 네트워크에 참가를 허용한다. 거래 생성 및 확인 등의 기능도 네트워크 참가자들끼리만 가능하다. 따라서 패브릭은 멤버십 서비스에 의하여 기본적으로 무분별하게 정보가 공개 되지 않기 때문에 익명성과 프라이버시 보호가 적용된다고 표 1에 분류하였다.

기본적인 멤버십 서비스 외에 추가된 프라이버시 보호 기법으로는 채널과 비밀 데이터 모음 등이 있다. 두 기법의 공통점은 기존의 사설 네트워크에서 더 작은 범위의 서브 네트워크를 생성해서 거래 내용 공유를 원하는 피어들끼리만 하고자하는 목적을 갖고 있다. 하지만 비밀 데이터 모음 기법이 채널과 다른 점은 생성되는 모든 거래가 전체 채널 멤버들 내에서 비밀로 유지되어야 하는 경우에 사용하고, 거래는 공유되어야 하지만 채널의 일부 멤버들만 데이터에 접근해야 하는 경우에는 데이터 모음을 사용하는 것이 프라이버시 보호에는 더 효율적이다.

표 1에 패브릭의 채널 스킴은 MSP와 유사하게 비밀 네트워크를 생성하는 것이기 때문에 익명성과 프라이버시 모두 보호하는 기법으로 분류하였다. 하지만 비밀 데이터 모음은 SideDB를 두고 직접적으로 데이터가 공유되지 않고 접근 권한이 없는 제 3자는 데이터가 공유되었다는 사실만을 해시 값을 통해 추론할 수 있다. 때문에 비밀 데이터 모음은 프라이버시 보호기법으로 분류하였다.

비록 패브릭은 사설 블록체인 기반이라서 다른 암호화폐들과 성능을 평가할 때 기준이 조금 다를 수는 있지만, 암호학 기법들의 연산 속도만으로 평가하였을 때 많은 연산량이 필요하지는 않으므로 높은 성능을 낸다고 할 수 있다.

5. 결 론

본 논문에서는 비트코인에서 발생할 수 있는 프라이버시 노출 위험에 대하여 대응 해결책이 될 수 있는 블록체인 플랫폼들에 대한 연구를 진행하였다. 여러 플랫폼들 중 대시, Zcash, 모네로, 하이퍼레저 패브릭 네 가지를 선정해서 각 플랫폼과 적용하고 있는 프로토콜들도 자세하게 살펴보았다. 그리고 기법들을 프라이버시 보호 기법과 익명성 보호 기법으로 상세히 분류하고 장단점을 분석하였다. 또한 기법들의 연산 속도를 바탕으로 플랫폼의 성능을 비교·분석하였다.

비트코인의 프라이버시 문제에 대한 취약점은 여전히 논란이 많은 주제이다. 왜냐하면 이 취약점은 비트코인뿐만 아니라 모든 블록체인 기반의 시스템에서 발견될 수 있기 때문이다. 블록체인 기술이 더 다양한 분야에 적용되기 위해서는 이 위험은 반드시 해결되어야 할 것이다. 전 세계적인 개발자들이 이 취약점을 방어하기 위한 안전하고 실용적인 블록체인 플랫폼을 개발하기 위하여 노력하고 있다.

향후 본 논문에서 언급된 4가지 플랫폼 외에도 또 다른 프라이버시 보호 목적의 암호화폐 등에 대해서도 꾸준히 연구를 진행할 계획이다. 예를 들면, 2016년에 등장한 Verge[37]나, 또는 스마트 계약 플랫폼인 이더리움에 zk-SNARKs를 적용하는 시스템[38] 등에 대하여 분석 연구를 진행할 수 있을 것이다. 본 연구는 더 효과적인 블록체인 기반의 프라이버시 보호 플랫폼 개발에 기초가 될 것이다.

참고문헌(Reference)

[1] Wikipedia, Cryptocurrency, 2019. https://en.wikipedia.org/wiki/Cryptocurrency#History (accessed on July, 1, 2019).

[2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf (accessed on July, 1, 2019).

[3] CoinMarketCap, All Cryptocurrencies, 2019. https://coinmarketcap.com/all/views/all/ (accessed on July, 1, 2019).

[4] M. C. K. Khalilov & A. Levi “A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems,” IEEE Communications Surveys & Tutorials, 20(3), 2543-2585, 2018. http://dx.doi.org/10.1109/COMST.2018.2818623

[5] D. Guegan, “Public Blockchain versus Private blockchain. Université Panthéon-Sorbonne (Paris 1),” Centre d’Economie de la Sorbonne. halshs-01524440, 2017.

[6] D. Bradbury, “Anonymity and privacy: a guide for the perplexed,” Network Security, 2014(10), 10 – 14, 2014. http://dx.doi.org/10.1016/S1353-4858(14)70102-3

[7] A. Kumar, C. Fischer, S. Tople, & P. Saxena, “A Traceability Analysis of Monero’s Blockchain,” European Symposium on Research in Computer Security(ESORICS) 2017. Lecture Notes in Computer Science, 10493. Springer, Cham, 153-173, 2017. http://dx.doi.org/10.1007/978-3-319-66399-9_9

[8] E. Duffield, & D. Diaz, Dash: A Privacy-Centric Cryptocurrency, 2014. https://pic.nanjilian.com/20180716/343445b5bc4b5e0cba45893a083b480d.pdf (accessed on July, 1, 2019)

[9] Market Capitalization. Top 100 Cryptocurrencies, 2019. https://coinmarketcap.com/ko/ (accessed on July, 1, 2019)

[10] Dash Doc., X11 Hash Algorithm, 2019. https://docs.dash.org/en/stable/introduction/features.html#x11-hash-algorithm (accessed on July, 1, 2019)

[11] Dash Doc., PrivateSend, 2019. https://docs.dash.org/en/stable/wallets/dashcore/privatesend-instantsend.html (accessed on July, 1, 2019)

[12] CoinMarketCap, Zcash (ZEC) price, charts, market cap, and other metrics, 2019. https://coinmarketcap.com/currencies/zcash/ (accessed on July, 1, 2019)

[13] Zcash, What are zk-SNARKs?, 2019. https://z.cash/technology/zksnarks/ (accessed on July, 1, 2019)

[14] D. Yang, J. Gavigan & Z. Wilcox-O’Hearn, “Survey of Confidentiality and Privacy Preserving Technologies for Blockchains,” R3, Zcash Company, Research Report, 2016. https://z.cash/static/R3_Confidentiality_and_Privacy_Report.pdf (accessed on July, 1, 2019)

[15] S. Bowe, T. Hornby & N. Wilcox. (2019). Zcash Protocol Specification, Version 2019.0.2, https://raw.githubusercontent.com/zcash/zips/master/protocol/protocol.pdf (accessed on July, 1, 2019)

[16] Electric Coin blog, Why Equihash?, 2019. https://electriccoin.co/blog/why-equihash/ (accessed on July, 1, 2019)

[17] Cryptolux, Equihash, 2019. https://www.cryptolux.org/index.php/Equihash (accessed on July, 1, 2019)

[18] S. Goldwasser, S. Micali, and C. Rackoff. “The knowledge complexity of interactive proof-systems,” Proceedings of the 17th annual ACM symposium on Theory of computing (STOC ’85), ACM, New York, NY, USA, 291-304. 1985. http://dx.doi.org/10.1145/22145.22178

[19] Monero, https://web.getmonero.org/ (accessed on July, 1, 2019)

[20] CoinMarketCap, Monero (XMR) price, charts, market cap, and other metrics, https://coinmarketcap.com/currencies/monero/ (accessed

on July, 1, 2019)

[21] Nicolas van Saberhagen. CryptoNote v 2.0, 2013. https://cryptonote.org/whitepaper.pdf (accessed on July, 1, 2019)

[22] GitHub, The Kovri I2P Router Project, https://github.com/monero-project/kovri (accessed on July, 1, 2019)

[23] CryptoNote Technology, CryptoNote Phylosophy, https://cryptonote.org/inside.php (accessed on July, 1, 2019)

[24] R. L. Rivest, A. Shamir & Y. Tauman. "How to Leak a Secret," Proceeding of International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), 552 – 565. 2001. http://dx.doi.org/10.1007/3-540-45682-1_32

[25] Blockgeeks, What is Monero? [The Most Comprehensive Step-by-Step Guide], https://blockgeeks.com/guides/monero/ (accessed on July, 1, 2019)

[26] S. Noether. "Ring Signature Confidential Transactions for Monero," IACR Cryptology ePrint Archive: Report 2015/1098. https://eprint.iacr.org/2015/1098 (accessed on July, 1, 2019)

[27] Moneropedia, Pedersen Commitment, https://web.getmonero.org/resources/moneropedia/pedersen-commitment.html (accessed on July, 1, 2019)

[28] S. Noether, A. Mackenzie & Monero Core Team. "Ring Confidential Transactions," Monero Research Lab, MRL-0005, 2016. https://lab.getmonero.org/pubs/MRL-0005.pdf (accessed on July, 1, 2019)

[29] G. Maxwell. Confidential Transactions, 2015. https://people.xiph.org/~greg/confidential_values.txt (accessed on July, 1, 2019)

[30] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," Proceedings of the Thirteenth EuroSys Conference (EuroSys'18), Article No. 30, 1-15, 2018. http://dx.doi.org/10.1145/3190508.3190538

[31] Hyperledger fabric Docs, Channels, https://hyperledger-fabric.readthedocs.io/en/release-1.1/channels.html (accessed on July, 1, 2019)

[32] Hyperledger fabric Docs, Private data, https://hyperledger-fabric.readthedocs.io/en/release-1.2/private-data/private-data.html (accessed on July, 1, 2019)

[33] B. Kiraly, PrivateSend, https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend (accessed on July, 1, 2019)

[34] Electric Coin blog, Anatomy of a Zcash Transaction, https://electriccoin.co/blog/anatomy-of-zcash/ (accessed on July, 1, 2019)

[35] I. Miers, C. Garman, M. Green & A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," Proceedings of the 2013 IEEE Symposium on Security and Privacy, IEEE Computer Society, Washington, DC, USA, 397-411, 2013. http://dx.doi.org/10.1109/SP.2013.34

[36] Electric Coin blog, Cultivating Sapling: Faster zk-SNARKs, https://electriccoin.co/blog/cultivating-sapling-faster-zksnarks/ (accessed on July, 1, 2019)

[37] Wikipedia, Verge(cryptocurrency), https://en.wikipedia.org/wiki/Verge_(cryptocurrency) (accessed on July, 1, 2019)

[38] Electric Coin blog, Ethereum Adoption of zk-SNARK Technology, https://electriccoin.co/blog/ethereum-snarks/ (accessed on July, 1, 2019)

◐ 저 자 소 개 ◑

박 지 선(Ji-Sun Park)
2017년 2월 부경대학교 IT융합응용공학과(공학사)
2019년 2월 부경대학교 대학원 정보보호학협동과정(공학석사)
관심분야 : 블록체인, 암호 프로토콜
E-mail : 201211812@pukyong.ac.kr

신 상 욱(Sang Uk Shin)
1995년 2월 부경대학교 전자계산학과(이학사)
1997년 2월 부경대학교 대학원 전자계산학과(이학석사)
2000년 2월 부경대학교 대학원 전자계산학과(이학박사)
2000년 4월~2003년 8월 한국전자통신연구원 선임연구원
2003년 9월~현재 : 부경대학교 IT융합응용공학과 교수
관심분야 : 암호 프로토콜, 블록체인 보안, 디지털 포렌식
E-mail : shinsu@pknu.ac.kr