정 보 보 호 학 회 지
제28권 제3호, 2018. 6

사물 인터넷을 위한 블록체인 기술 동향

홍 은 기*, 이 수 진**, 서 승 현*

요 약

블록체인 기술은 분산형 네트워크를 통해 정보 등을 관리하고 저장함으로써 정보의 투명성 및 신뢰성을 제공해줄 수 있는 분산 컴퓨팅 기반의 데이터 위변조 방지 기술이다. 특히 수천만개 사물 기기들이 서로 통신을 하여 서비스를 제공하는 사물인터넷(IoT) 서비스 환경에서 블록체인 기술은 중앙 집중 방식의 관리 구조를 탈피하고 보안성을 향상시킬 수 있는 인프라 기술로 주목 받고 있다. IoT 서비스에 데이터 무결성 및 디바이스 제어 등의 보안서비스를 제공하고, 분산화된 방식으로 서비스의 확장성을 높이고자 최근 글로벌 기업들은 IoT 블록체인 개발을 위한 컨소시엄을 구성하여, IoT 서비스에 활용할 수 있는 블록체인 기반 기술들을 연구하고 있다. 본 논문에서는 블록체인을 기반으로 한 IoT 연구 프로젝트들의 연구기술 동향을 분석하고, IoT 서비스에 블록체인을 적용한 사례와 응용 기술 등을 소개한다. 또한 IoT 응용 서비스에 효과적으로 적용하기 위해 기존 블록체인 기법들의 확장성 및 오버헤드 등의 문제를 개선한 Tangle 기술에 대해서 자세히 소개하고, IoT에 블록체인을 적용하기 위한 고려사항들을 논의한다.

Ⅰ. 서 론

2020년이면 전세계 사물인터넷(IoT) 기기가 250억대에 달할 것이라는 전망이 나오고 있는 만큼 사물인터넷 산업은 빠르게 발전하고 있다. 그러나 지금까지의 사물인터넷은 중앙 집중형 시스템 방식으로 편의성 중심의 발전을 이루어 확장성 문제와 관리 비용의 문제, IoT 특성상 발생하는 보안 취약성 등의 한계점을 가지고 있다[1,2]. 최근에, 블록체인 기술을 적용하여 사물인터넷 한계점들을 개선하고자 하는 연구들이 활발하다. 불록체인은 거래가 발생할 때마다 거래 내역을 서비스 참여자에게 모두 전송하고, 거래 내역을 중앙 서버가 아니라 각 이용자들이 보관하는 형태의 분산화된 원장을 제공한다. 또한 암호학적 해시 체인으로 구성되어있어 원장의 위·변조가 불가능하기 때문에 거래의 투명성을 제공해줄 수 있다. 따라서 블록체인 기반으로 IoT 플랫폼을 개발하면 중간 관리자로 인한 비용을 절감하고 확장성을 높일 수 있으며,블록체인이 제공하는 거래의 무결성 및 투명성으로 IoT 보안문제를 어느 정도 개선할 수 있을 것으로 기대를 모으고 있다. 그러나, 현재 1세대 블록체인이라 불리는 비트코인 등의 블록체인 시스템을 IoT 환경에 그대로 적용하기에는 여러 가지 어려움들이 있다. 먼저 병렬처리 방식의 부재로 기존 블록체인의 거래 인증 속도가 전통적인 중앙 집중형 시스템 방식보다 느리다는 점이다[3]. 빠른 속도로 거래를 주고받아야 하는 사물인터넷 서비스에 기존 블록체인의 거래 처리 속도는 적합하지 않다. 또한 대부분의 IoT 기기들은 저전력, 초소형이기 때문에 컴퓨팅 능력이 제한되어있어, 1세대 블록체인에서 합의 알고리즘으로 사용하는 컴퓨팅 파워를 필요로 하는 작업증명(PoW) 방식을 적용하기에는 어려움이 따른다. 뿐만 아니라 1세대 블록체인은 작은 거래를 요청할 때 본래 거래의 가치보다 더 큰 수수료가 부과되는 문제가 있어 작은 규모의 거래들이 활발하게 일어나는 사물인터넷에서 기존 블록체인 체계를 적용시키는 것이 비효율적이다. 그밖에도 확장성 제한 등의 문제점이 존재한다. 최근에는 기존 블록체인 기술의 확장성 및 거래 인증 속도 등의 문제점 들을 개선한 3세대 블록체인 기술들이 제안되고 있다. IOTA 재단, IBM, 삼성, Linux Foundation에서는 기존 블록체인이 갖는 한계점들을 3세대 블록체인 기술을 포함한 다양한 기술의 적용과 접근방식으로 보완하여 사물인터넷 사업에 적용하는 프로젝트를 진행하고 있다. 이에 본 논문에

* 한양대학교 대학원 전자공학과 (heg0403@gmail.com, seosh77@hanyang.ac.kr)
** 한양대학교 에리카캠퍼스 전자공학부 (tssn195@hanyang.ac.kr)

서는 현재 IOTA, IBM, IoTChain, Walton Chian, Streamr, SLOCK.IT 등에서 진행하고 있는 블록체인 기술을 적용한 IoT 프로젝트들의 연구 동향과 적용 사례들에 대해 소개하며, 특히 3세대 블록체인이라 불리우는 IOTA의 Tangle 기술에 대해서 자세히 분석한다. 마지막으로 IoT에 블록체인 기술을 적용하기 위해 고려해야할 사항들에 대해서 논의하고자 한다.

Ⅱ. 블록체인 기반 IoT 프로젝트

본장에서는 블록체인 기술을 활용한 IoT 프로젝트들과 적용 사례에 대해 설명한다.

2.1. IOTA

IOTA는 블록체인 연구를 목적으로 하는 IOTA 재단에서 진행 중인 프로젝트로, 3세대 블록체인이라 불리우는 Tangle을 기반으로 한다. 기존 블록체인이 가지고 있는 높은 거래 수수료 문제를 해결하며 M2M 소액결제시스템의 효율성을 높이기 위해 제안되었다. Tangle이란 사이트(site)와 노드(node)의 개념으로 이루어져 있으며 다중 방향성 비순환 그래프(Multi-threaded Directed acyclic graph)의 구조를 갖는다[4]. 채굴자(miner)가 따로 존재하지 않고 새로운 트랜잭션을 발행할 때 컴퓨팅 파워를 소모하는 작업증명이 아닌 팁 선택 알고리즘(TSA; Tip selection algorithm)을 이용함으로써 사용자들의 전력 낭비를 줄이고 기존 블록체인보다 더 빠른 속도로 거래를 인증한다. 이는 거래를 하는데 있어서 높은 속도를 지향하는 IoT 환경에서 큰 장점이 된다. Tangle은 기기간의 마이크로트랜잭션(micro- transaction), 전자 투표(e-voting) 등 여러 IoT 제품에서 필요한 기능에 적용될 수 있다. 최근에는 ITIC(International Transportation Innovati on Center)와 협력하여 IOTA 기반의 모빌리티 서비스(mobility service) 연구도 진행하고 있다[5].

2.2. IoT Chain

IoT Chain은 블록체인을 기반으로 하며 PBFT(Practical Byzantine Fault Tolerance), DAG (Directed Acyclic Graph), SPV(Simple Payment Verification) 그리고 CPS(Cyber Physical System)의 기술을 적용하였다. ICT(IoT Chain Token) 토큰을 이용하여 IoT 제품을 이용할 수 있도록 하고, 또한 IoT 환경에서의 보안성을 강화하는 것이 목표이다. 기존 블록체인이 원장을 분산화 함으로써 갖는 보안성을 유지하면서 PBFT와 DAG 기술을 통해 보다 빠른 거래 처리 속도와 블록체인의 확장성 문제를 해결하였다. IoT Chain은 메인 체인과 사이드 체인으로 구성되는데, 사이드 체인은 메인 체인에서 생성되는 코인을 이용하여 스마트 계약(Smart Contract)을 실행하는 체인이다. 메인 체인에서는 빠른 거래 인증이 장점인 PBFT를 사용하고 사이드 체인의 경우, DAG를 사용하기 때문에 트랜잭션 처리가 효율적이다. SPV는 지불 검증을 할 때, 블록의 모든 구성요소를 보는 것이 아니라 블록의 헤더만 확인하여 검증을 하는 것을 말한다. 이 기술을 통해 검증에 필요한 수수료가 낮아지게 되며 사용자들의 오버헤드가 줄어드는 장점이 있다. IoT Chain은 IoT 기기를 위한 공유 경제(economy sharing), 스마트 홈(smart home) 등에 적용되고 있다. 2018년 11월에 개발자를 위한 생태계를 조성하고 12월에는 대중적으로 IoT Chain을 제공할 계획을 가지고 있다[6].

2.3. Walton Chain

Walton Chain은 한국과 중국이 공동으로 개발한 비즈니스 블록체인 플랫폼이며 RFID 하드웨어 기술이 융합되었다. 사물인터넷의 중앙 집중화된 문제를 해결하는 것에 초점을 맞춰 블록체인과 IoT 기술을 결합하는 VIoT(Value internet of things)의 개념을 제시했다. RFID를 통해 물품의 역사를 추적할 수 있으며 위조방지의 기능을 가지고 있다. Walton Chain에서는 Walton Coin(WTC)라는 토큰을 사용하고 있고 이더리움의 스마트 계약 기능을 제공한다. Walton Chain 생태계는 앞서 언급한 IoT Chain처럼 메인 체인과 사이드 체인으로 나눌 수 있다. 메인 체인에서는 지분증명(PoS)의 업데이터 버전인 Proof-of-Stake & Trust(PoST)를 합의 알고리즘으로 선택했다. 기존의 PoS보다, PoST는 사용자의 이전 행동도 고려하기 때문에, 신뢰도가 더 높은 사용자가 코인을 생성할 확률이 높아진다는 장점이 있다. 이 기술을 통해 소비자들은 옷, 가구 등의 모든 재화의 바코드나 RFID 태그를 통해 제품의 생산과정과

같은 정보들을 알 수 있어 제품이 신뢰성을 갖도록 한다[7].

2.4. Streamr

Streamr는 IoT 환경에서 효율적인 실시간 데이터 전송과 지불을 멈춤 없이 제공하기 위한 분산화된 오픈소스 peer-to-peer 플랫폼이다. $DATA라는 암호화된 토큰을 데이터 거래에 사용하며 거래 수수료가 존재하지 않는다. 또한 이더리움을 기반으로 스마트 계약 기능을 수행한다. 확장성을 가지며 거래 시 낮은 대기시간을 제공한다. 차량 교통 정보나 일기예보, 주유소 별 주유 요금 등의 정보를 다른 기관의 도움 없이 실시간으로 자유롭게 사고파는 네트워크를 구축하는 것이 주요 역할이다[8].

2.5. IBM-ADEPT

IBM-ADEPT에서 ADEPT는 Autonomous Decentralized Peer-to-Peer Telemetry의 약자로, IoT 기기를 위한 Peer-to-Peer 블록체인 플랫폼이다. 삼성과 IBM이 협력하여 ADEPT의 개념을 2015년에 발표하였다. BitTorrent, Telehash, 그리고 이더리움의 기술이 적용되었다. IoT 기기들의 용량에 따라 나누어 특정한 구조를 적용하고 있으며 각자 데이터를 관리, 분석 그리고 공유 할 수 있도록 지원한다. IBM-ADEPT는 웨어러블 장비와 가전 제품에 적용되고 있다. 그 예 중 하나로, 삼성에서는 스마트 세탁기를 공개하였는데 ADEPT 기술을 이용하여 세제 등 필요한 물품들이 부족할 시, 자동으로 주문할 수 있도록 하였다[9].

2.6. SLOCK.IT

SLOCK.IT는 독일의 스타트업으로 이더리움을 기반으로 한 공유경제 인프라를 구축하는 것을 목표로 한다. 현재 Universial Sharing Network을 개발 중이다. 이더리움 기술에 자동화 결제 시스템을 결합하였다. 사용하지 않거나 남는 재화, 집 또는 자동차들을 블록체인을 이용하여 신뢰할 수 있는 타인이 공유와 거래를 할 수 있도록 하였다. SLOCK.IT는 스마트 락(Smart lock)의 기능을 제공하는데 사용자가 토큰을 지불하여 이더리움의 스마트 계약을 실행하면 사용자에게 재화의 lock이 해제가 되어 타인이 해당 재화를 이용할 수 있게 된다. 모바일 앱을 통해 거래 시 사용되는 키를 관리할 수 있다[10].

2.7. Hyperledger

Hyperledger은 Linux Foundation에서 지원하는 블록체인 개발 프로젝트로 비즈니스용 Private 블록체인이라는 특징을 가진다. Membership service를 통해 블록체인 네트워크에 참여하는 사용자들의 신원관리를 하고 체인코드(chaincode)라는 응용 프로그램를 이용하여 스마트 계약을 실행한다. 비즈니스 블록체인에서 사용되는 합의 메커니즘은 각 비즈니스의 요구사항에 따라 다르다. 그에 맞춰서 Hyperledger 프로젝트마다 Kafka,

〔표 1〕 주요 프로젝트 비교

project	IOTA	IoT Chain	Streamr	Walton Chain	IBM-ADEPT	SLOCK.IT	Hyperledger
기존 블록체인 개선사항	M2M 소액결제의 수수료 문제 해결, 거래처리 속도 향상	거래처리 속도 향상, 확장성 문제 개선	실시간 데이터 거래 제공	각 노드의 신뢰도 제공	기기의 용량에 맞춘 구조 제공	물리적 장치 공유	peer의 오버헤드감소, 모듈형 구조
적용된 블록체인 기술	다중 DAG 구조를 갖는 Tangle	PBFT, DAG, SPV, CPS	Ethereum	Ethereum, RFID 기술	Ethereum, BitTorrent, Telehash	Ethereum	Hyperledger fabric
블록체인 종류	Public						Private
응용 분야	산업 분야	스마트홈, 공유경제	데이터 마켓	디지털 거래	가전제품, 웨어러블 기기	Smart lock	금융, 헬스케어

PBFT, PoET, Sumeragi와 같은 다양한 함의 알고리즘을 이용했다. Hyperledger에서는 함의를 이루는 활동을 크게 Ordering transaction 과 validating transaction으로 나누어 각각 따로 실행된다는 특징을 갖는다. Hyperledger의 서브 프로젝트들 중 하나인 Fabric은 거래 인증과 합의, 이 두 가지의 역할을 하던 기존의 Peer의 일을 분리하여 효율적으로 거래를 처리할 수 있도록 하였다[11]. 금융, 헬스 케어(Healthcare) 등의 분야에 활용되고 있으며 실제로 China Minsheng Bank, Sberbank, Deutsche Bank 등의 은행들과 Change Healthcare 외 여러 분야의 회사들이 Hyperledger project에 멤버로서 참여하고 있다[12]. 이처럼 여러 산업 분야와 기능에 맞게 블록체인의 시스템을 적용되어 기존의 IoT 산업 문제를 해결하려는 시도들을 통해 다양한 블록체인 플랫폼이 존재한다. [표 1]은 2장에서 설명한 프로젝트들을 비교하여 나타내고 있다.

Ⅲ. Tangle

이 장에서는 3세대 블록체인이라고 불리우는 IOTA의 Tangle[4,13]에 대해 설명한다. Tangle은 새로운 트랜잭션 합의 방법을 도입하여 기존 1세대 블록체인의 수수료 문제와 오버헤드, 제한된 확장성 그리고 오프라인 거래가 불가능하다는 단점을 개선하였다.

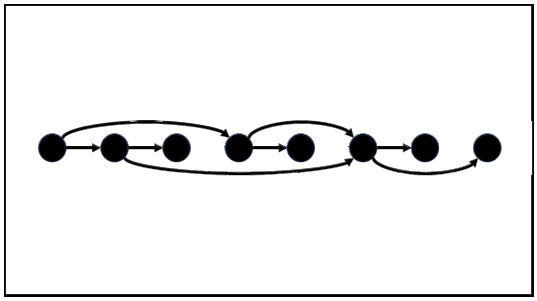
3.1. 모델

이 장에서는 Tangle 구조가 각각 가지고 있는 특징들과 IOTA에 적용되어있는 개념들을 소개한다.

3.1.1. 다중 방향성 비순환 그래프(Multi-threaded DAG)

Tangle에서는 기존 블록체인의 제한된 확장성과 느린 속도 단점을 방향성 비순환 그래프(DAG)라는 개념으로 개선하였다. DAG은 [그림1]에서 보는 바와 같이 이전 단계로 되돌아갈 수 없는 체인 연결 블록 방식을 이야기 한다.

Tangle은 이 DAG을 여러 갈래로 연결한 다중(Multi-threaded) DAG 구조이다. Tangle 은 여러 끝점을 통해 데이터의 병렬처리가 가능하며 네트워크 참여자가 많아질수록(즉, 끝점이 많아질수록) 처리 속도 또한 증가한다. 또한 검증에 참여하는 트랜잭션 또한 많아



〔그림 1〕 방향성 비순환 그래프(DAG)의 개요도

지기 때문에 네트워크의 안정성이 증가하게 된다. 그리고 개별적인 채굴이 필요하지 않아 채굴자가 존재하지 않으며 거래의 수수료 또한 없다.

3.1.2. 팁 선택 알고리즘 (TSA: Tip Selection Algorithm)

어떤 노드가 Tangle 네트워크에 새로운 트랜잭션을 발행한다고 가정해보자. 그럼 우선 노드는 개인키로 해당 트랜잭션에 서명을 한다. 그 후에 기존에 Tangle 네트워크에 포함되어 있던 팁(즉, 승인되지 않은 트랜잭션) 두개를 팁 선택 알고리즘(TSA)에 의해 선택한 이후에 검증을 한다. Tangle은 노드에서 승인할 트랜잭션을 선택하기 위한 규칙으로 누적 거래 가중치의 크기에 따라 임의로 팁을 선택하는 알고리즘인 Markov Chain Monte Carlo(MCMC) 알고리즘을 사용하는 것을 선호한다.

그러나 현재까지 존재하는 팁 선택 알고리즘들은 다수의 노드를 추가하여 이중 지불(Double spending) 공격을 행하는 Mirror 공격에 취약하며 전체 네트워크의 34% 이상의 공격을 받으면 Tangle 네트워크는 무너지게 된다. 그래서 IOTA에서는 Tangle 네트워크를 보호하고 안정성을 유지하기 위해 Coordinator라고 하는 특수 노드를 사용하고 있다. 따라서 중앙화 된 Coordinator 때문에 완벽한 탈중앙화가 이루어지지 않고 있다. IOTA 팀은 빠른 시일 내에 이 Coordinator를 오라클로 대체하는 등 제거 할 예정이라고 한다.

3.1.3. 무게와 검증

새로운 트랜잭션이 Tangle 네트워크에 들어가기 위해서는 팁 검증이 필요하다. 이를 위해 기존 비트코인 등의 블록체인보다 비교적 쉬운 난이도의 작업증명

(PoW: Proof of Work)를 진행하게 된다. 여기서 PoW의 난이도는 그 팁의 무게이며 이 PoW는 노드가 막대한 수의 트랜잭션 Spamming 공격을 하지 못하도록 프로토콜에 포함되어 있다. 팁의 무게란 노드가 해당 팁에 투자한 일의 양에 비례한다. 모든 트랜잭션에는 크기에 상관없이 무게가 있어야한다. 트랜잭션이 자신을 직접 혹은 간접적으로 검증해주고 있는 모든 트랜잭션의 무게의 합을 누적 무게라고 하는데 이러한 누적 무게들은 TSA가 유효한 팁을 선택하는데 사용된다.

현재 IOTA는 각 트랜잭션의 서명 검증을 Winternitz-OTS(One-Time-Signature)라고 하는 해시 기반 전자 서명기법을 사용한다. 이 방식은 양자 내성 암호(PQC; Post Quantum Cryptography) 방식 중의 하나인 암호학적 해시함수를 이용한 전자서명 방식이다. 그러나 Tangle은 자체 개발한 Curl이라는 3진(Trinary) 해시함수를 이용하는데 이 Curl은 차분 분석 공격으로 충돌 문제가 발생하여 보안상 취약하다[13,14]. 또한 이진(Binary)이 아닌 삼진 기반이기 때문에 오버헤드가 생기는 문제가 있다. IOTA팀은 2017년 8월에 SHA-3 알고리즘을 추가하는 업데이트를 통해 Curl 해시가 가질 수 있는 취약성을 해결했다고 한다[15].

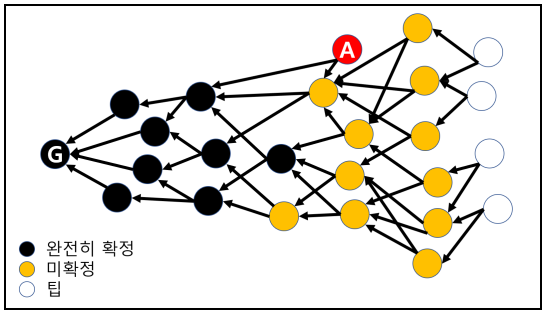
3.2. 검증과 합의

이 장에서는 MCMC 알고리즘을 TSA로 사용하는 Tangle 네트워크의 트랜잭션 확정 및 합의에 대해서 초기 상태, 새로운 트랜잭션 추가, 전파 지연, 이중 지불 그리고 오프라인 네트워크로 나누어서 서술한다[16].

3.2.1. 초기 상태

블록체인은 하나의 블록에 여러 트랜잭션을 포함하고 있고, 그러한 블록들을 시간 순으로 정렬하여 구성한다. Tangle은 기존 블록체인과 다르게 시간 순으로 블록들을 연결하지 않으며, 하나의 트랜잭션이 다른 트랜잭션에 병렬적으로 추가된다.

Tangle에서 모든 트랜잭션들은 가장 초기의 Genesis 트랜잭션을 직접 혹은 간접적으로 검증하고 있다. Genesis 트랜잭션을 제외한 초기상태의 트랜잭션들은 세 가지로 나뉜다. 완전히 확정된 트랜잭션과, 낮은 신뢰도로 확정된 트랜잭션 그리고 아직 검증을 받지 못한



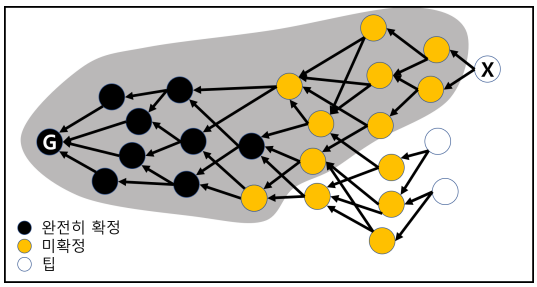
〔그림 2〕 Tangle의 초기상태

트랜잭션인 팁이다. 완전히 확정된 트랜잭션은 초기 상태에 팁들 모두에게 직접 혹은 간접적으로 검증 받은 트랜잭션을 이야기하며 낮은 신뢰도로 확정된 트랜잭션은 그 팁들 중 하나 이상 검증 받지 않은 트랜잭션이다. [그림 2]를 보면 G는 Genesis 트랜잭션이고 완전 확정, 미확정, 팁을 색으로 구분해두었다. A 트랜잭션은 자신이 검증할 때 팁이었던 트랜잭션과 그 팁이 검증한 트랜잭션을 참조하고 있는 관계로 비정상적 트랜잭션이지만 현재 네트워크에서는 허용된다.

3.2.2. 새로운 트랜잭션 추가

새로운 팁이 추가될 때 그 팁은 TSA에 의해 기존의 팁들 중 두 개를 선택하여 검증한다. 팁 검증을 위해 해당 팁들의 서명의 유효성을 확인하고, Spamming 공격 방지를 위해 쉬운 난이도의 PoW를 수행한다.

[그림 3]은 팁 X를 추가할 때의 모습이다. 팁 X는 선택한 팁 두 개를 검증하고, 네트워크에 추가 된다. 회색으로 표시된 영역에 속해 있는 트랜잭션들은 팁 X가 추가 될 때 팁 X에 의해 직접 혹은 간접적으로 검증된 트랜잭션들이다. Tangle 네트워크의 현 시점에 존재하는 모든 팁들에게 직접 혹은 간접적으로 검증되고 있는 트



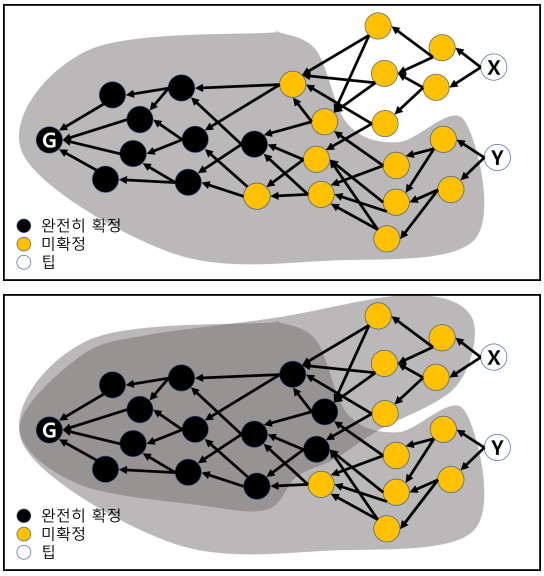
〔그림 3〕 팁 X가 추가되며 검증되는 영역

랜잭션들은 완전히 검증되었다고 한다.

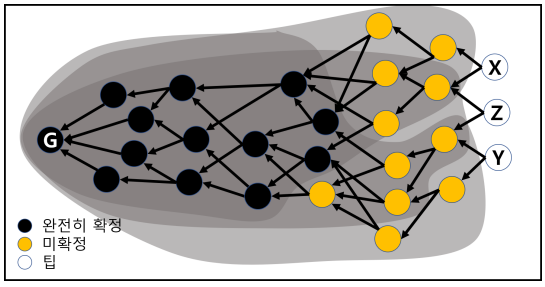
[그림 4]를 보면 팁Y가 추가되면서 X와 Y의 영역 중 겹치는 영역이 두 팁이 모두 검증을 하고 있는 영역이며 팁 Y가 추가됨에 따라 완전히 검증된 트랜잭션이 늘어난다. 따라서 팁이 계속해서 추가되면 완전히 검증된 트랜잭션들은 늘어나는 것을 확인 할 수 있다.

Tangle 네트워크에서 더 깊이 위치한 트랜잭션일수록 확정도(Confirmation level)가 늘어난다. 여기서 확정도는 해당 트랜잭션의 검증 정도인데, 얼마나 많은 팁들에 의해 검증 되었는지에 따라 결정된다.

현재 Tangle 네트워크에서 네트워크 사용자는 트랜잭션의 허용 확정도를 결정하는 것이 가능하다. 허용 확정도는 사용자가 트랜잭션의 확정도가 얼마이냐에 따라 유효한 트랜잭션으로 판단할 것인지를 말한다. 네트워크 사용자는 트랜잭션의 속도가 더 중요할 경우 완전히 검증될 때 까지 기다리는 것이 아니라 상대적으로 적은 허용 정확도의 트랜잭션을 유효하다고 판단할 수 있다. [그림 5]를 보면 다수의 팁이 추가됨에 따라 네트워크 내부의 트랜잭션들의 확정도가 변동이 되며 영역이 짙을수록 확정도가 높은 것을 알 수 있다. 만약 67%의 확정도로 트랜잭션을 허용시킬 경우 X와 Y, Y와 Z 혹은 X와 Z에게만 검증받은 트랜잭션도 확정되었다고 볼 수 있다.



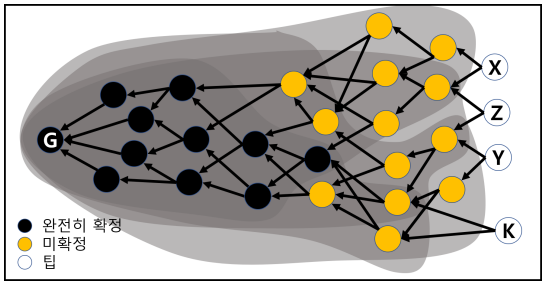
〔그림 4〕 팁 X가 추가되는 시점과 거의 동시에 팁 Y가 추가되는 모습.



〔그림 5〕 팁이 다수 추가되었을 때의 모습

3.2.3. 전파 지연

PoW가 오래 걸리거나 전파가 지연되면 뒤늦게 네트워크에 추가될 수 있다. [그림 6]에서는 팁 K가 전파 지연으로 뒤늦게 추가된 모습인데, [그림 5]와 비교했을 때 일부 트랜잭션들의 확정도가 바뀐다. 완전히 확정된 상태였다가 확정도가 낮아진 트랜잭션들은 실제로 신뢰할 수 없는 상태는 아니며 정상적으로 확정되었다고 인정한다.

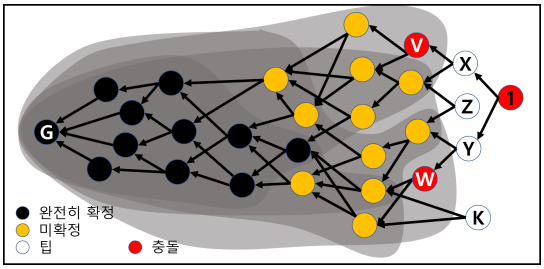


〔그림 6〕 팁 K가 전파지연 등으로 뒤늦게 네트워크에 추가된 모습

3.2.4. 이중 지불

네트워크 사용자가 두 개의 충돌되는 트랜잭션을 발생시키면, 즉 이중 지불의 경우에는, 그 이후에 추가되는 팁들은 TSA나 전파지연에 의해 충돌되는 트랜잭션들 중 한 개의 트랜잭션만 검증경로에 포함할 가능성이 있다.

[그림 7]을 보면, 트랜잭션 X와 Y는 네트워크에서 충돌하고 있는 트랜잭션 V와 W를 각각 한 개 씩 포함하여 검증하고, 충돌은 인지하지 못한 채 V와 W를 유효한 트랜잭션으로 판단한다. 시간에 따라서 충돌되는 트랜잭션 두 개 모두를 포함한 경로를 검증하는 팁 1이

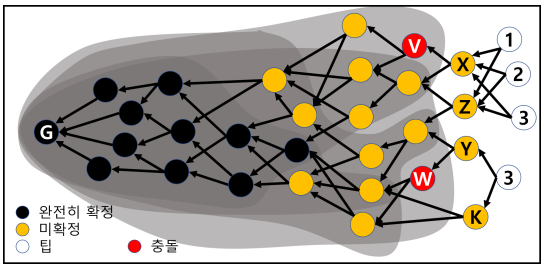


〔그림 7〕 트랜잭션 V와 W가 충돌하고 있는 모습

네트워크에 추가되면 그 해당 팁은 차후에 추가될 팁들에 의해 유효한 트랜잭션으로 검증받기 위해 충돌이 되지 않는 팁 두 개를 다시 선택한다.

충돌되는 트랜잭션 들이 발견되지 못하고 그 중 하나만 검증경로에 포함하는 팁들이 여럿 추가될 수 있지만 둘 모두 포함되는 경로를 검증하는 팁이 발행되는 순간 충돌이 발견되고, TSA는 네트워크는 누적 거래 가중치에 의해 충돌되는 트랜잭션 중 한 쪽 경로로만 더 많은 팁들에게 선택 된다. 시간이 지나면 TSA에 의해 누적 거래 가중치가 낮은 쪽에는 새로운 팁들이 추가하는 것이 불가능해지고 확정되지 않으며 버려진다. [그림 8]에서는 시간이 지남에 따라 충돌되는 V와 W 중 V에 만 다수의 새로운 팁들이 추가되고 W를 검증하는 쪽은 버려진다.

버려진 쪽에 추가된 트랜잭션들은 네트워크에서 아예 사라지는 것은 아니고 다른 사용자(IOTA 수금자 등)에 의해서 다시 네트워크에 추가되고 검증받을 수 있다.

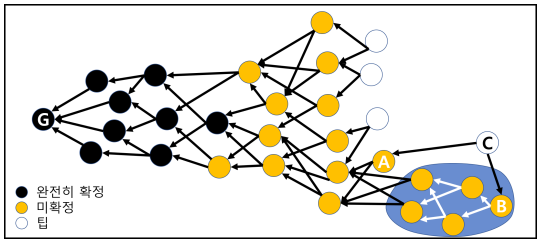


〔그림 8〕 충돌하는 트랜잭션이 발견될 경우 TSA는 다시 팁을 선택한다.

3.2.5. 오프라인 네트워크

Tangle 네트워크 사용자는 메인 네트워크에 연결되어 있지 않은 오프라인 네트워크에도 트랜잭션을 추가할 수 있다. [그림 9]에서 파란색 영역으로 표시된 부분이 오프라인 네트워크이다.

이 오프라인 네트워크가 메인 네트워크로 검증 될 때 팁 C는 메인 네트워크의 팁 A와 오프라인 네트워크의 팁 B를 선택하여 검증하게 된다. 이렇게 되면 다른 오프라인 네트워크의 트랜잭션들 또한 팁 C의 검증경로에 포함되어 함께 검증된다.



〔그림 9〕 오프라인 네트워크가 메인 네트워크에 추가되는 모습

Ⅳ. IoT에 블록체인을 적용하기 위한 고려사항

블록체인을 IoT에 적용하기 위해서는 오버헤드 문제와, 확장성 문제, 프라이버시 보호 문제 등이 해결되어야 한다[17].

기존의 비트코인과 같은 1세대 블록체인들은 트랜잭션 간의 합의를 할 때 어려운 난이도의 PoW를 진행한다. 이는 컴퓨팅 파워를 바탕으로 어려운 문제를 푸는 것이기 때문에 성능에 제한이 있는 IoT기기 간에 통신에서 사용 할 경우 네트워크에 참여하는 기기가 많아질수록 큰 통신 오버헤드가 발생하여 속도가 저하된다. 또한 직렬구조로 블록체인의 체인들이 연결되어 있어 많은 수의 기기가 서로 연결되어야 하는 IoT 환경에서 검증이나 합의를 거치는 것이 비효율적이다[2,3]. 이러한 문제들은 본 논문 3장에서 언급한 3세대 블록체인 Tangle의 병렬작업과 오프라인 네트워크를 운용할 수 있는 특징으로 많은 부분 해결되었다.

그러나 여전히 프라이버시 보호 문제는 남아있다[18]. 블록체인 구조에서 익명성은 보장되는 것으로 알려져 있으나 블록체인 내에 저장된 특정 노드의 검증이나 합의에 필요한 공개키 주소와 거래내역을 수집해 통계적 분석을 시행하면 트랜잭션 소유자에 대한 행동 패턴을 파악할 수 있다. 2018년에 체인널리시스(Chainalysis)에서

개발한 체인널리시스 리액터[19]는 이를 자동화하여 수사기관 등에서 사용하고 있는데, 이는 블록체인이 완벽한 익명성을 제공하지 않는다는 것을 보여준다.

이를 해결하기 위한 대안으로 Z-cash는 영지식 증명을 이용해 블록체인에 저장되는 거래내역의 추적을 방지하도록 하는 방법[20]과 다수의 신원 정보가 입력되는 스마트 계약(Smart contract)에서는 여러 사용자가 검증과 합의를 거쳐 계약의 이행 결과만을 공개하여 참여자의 익명성을 보장 할 수 있는 방법[21] 또한 제안되었으나, 현재 이 기술들을 IoT에 적용하기 위해서는 아직 많은 개선이 필요하다.

Hyperledger 등에서는 프라이빗 블록체인을 이용해 신원이 검증된 노드만 참여시킨 후 중앙 관리자를 두어 프라이버시를 보호하는 방법[11]들이 제안되었으나 이 또한 탈중앙화를 이루지 못하는 단점이 있다.

Ⅴ. 결 론

비트코인이 주목받으면서 블록체인은 주류 기술이 된지 오래이다. 블록체인의 탈중앙화와 무결성 보장 등의 특징으로 IoT에 응용하려는 시도들이 있어 왔고, 앞으로도 계속 될 것이다. 본 논문에서는 1세대 블록체인들이 IoT에 적용되었을 때의 한계점을 개선하기 위해 제안된 IOTA와 IoT Chain, Walton chain 등에 대한 소개와 IOTA와 IoT Chain에 사용 된 Tangle에 대해 논했다. Tangle은 1세대 블록체인이 IoT에 적용될 되었을 때의 한계점인 확장성과 오버헤드 문제를 새로운 합의방식과 병렬형태의 구성으로 개선하였으나, 여전히 Coordinator 노드 운용에 따른 중앙화 문제와, 프라이버시 보호 문제 등 취약점이 존재한다. 이를 해결하기 위해 51%공격(Tangle의 경우 34%)으로부터 보호하는 것과 내부의 프라이버시 관련정보들을 효과적으로 보호할 수 있는 방안에 대한 연구가 더 필요하며 이 취약점들이 개선된다면 앞으로 IoT에 적용될 블록체인 기술에 한 축을 담당할 것으로 전망된다.

참 고 문 헌

[1] 융복합지식학회논문지, 2018.1, 135-140, 김정숙. “블록체인 기반의 서비스 현황 및 문제점 분석”

[2] 금융보안원, 국내·외 블록체인 기반 사물인터넷 동향, 보안기술연구팀, 2017.6

[3] 강승준, “블록체인 기술의 이해와 개발 현환 및 시사점”, 정보통신산업진흥원 이슈리포트, 2018-제13호

[4] Serguei Popov, “The Tangle” 2018

[5] Dominik Schiener, “IOTA partners with ITIC” https://blog.iota.org/iota-partners-with-itic-e83f228a11d9

[6] IoT Chain, “IoT Chain A high-security lite OS” 2018

[7] the Waltonchain team, “Waltonchain White Paper (V 1.0.4)“ 2018

[8] Streamr, “Unstoppable Data for Unstoppable Apps: DATAcoin by Streamr“ 2017

[9] IBM, “ADEPT: An IoT Practitioner PerspectiveD” 2015

[10] SLOCK.IT, https://slock.it/usn.html

[11] Hyperledger, “Hyperledger Architecture, Volume 1“ 2018

[12] Hyperledger, https://www.hyperledger.org/members

[13] Neha Narula, “IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency”

[14] Michael Colavita, Garret Tanzer, “A Cryptanalysis of IOTA’s Curl Hash Function”, 2018

[15] IOTA foundation, “Official Statement Regarding the MIT DCI Email Leaks”

[16] noneymous, “IOTA Transactions, Confirmation and Consensus”, github

[17] Konstantinos Christidis, Michael Devetsikiotis, “Blockchains and Smart Contracts for Internet of Things”, IEEE Access, 2224-2303 2016

[18] 다니엘 드래셔, “블록체인 무엇인가?”, 이병욱(역), 이지스퍼블리싱, 2018

[19] Chainalysis, “The Changing Nature of Cryptocrime”, 2018

[20] Alex Vikati, “How Private Are Privacy Coins: A Closer Look at Zcash and Zclassic’s Blockchains”

[21] Vitalik Buterin, 차세대 스마트 컨트랙트와 탈중앙

화된 어플리케이션 플랫폼, Etherieum Korea

〈저자소개〉

홍 은 기 (Eungi Hong)
2018년 2월 : 한양대학교 ERICA 전자시스템공학과 졸업
2018년 3월~현재 : 한양대학교 전자공학과 석사과정
관심분야 : IoT 보안, 임베디드 시스템 보안

이 수 진 (Soojin Lee)
2014년 3월~현재 : 한양대학교 전자공학부 학사과정
관심분야 : IoT 보안, 블록체인 보안, AI 보안

서 승 현 (Seung-Hyun Seo)
2000년 : 이화여자대학교 수학과 (이학사)
2002년 : 이화여자대학교 컴퓨터학과 (공학석사)
2006년 : 이화여자대학교 컴퓨터학과 (공학박사)
2006년 12월~2010년 1월 : 금융보안 연구원 주임연구원
2010년 2월~2012년 2월 : 한국인터넷 진흥원 선임연구원
2012년 2월~2014년 5월 : 미국 퍼듀대학교 컴퓨터학과 박사후연구원
2014년 6월~2015년 2월 : 고려대학교 정보보호대학원 BK21+ 사업단 연구교수
2015년 3월~2017년 2월 : 고려대학교 세종캠퍼스 수학과 조교수
2017년 3월~현재 : 한양대학교 ERICA 캠퍼스 전자공학과 부교수
관심분야 : IoT 보안, 블록체인 보안, 암호프로토콜 설계 및 응용