Journal of The Korea Society of Computer and Information
Vol. 24 No. 2, pp. 67-74, February 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.02.067

A Survey of Cryptocurrencies based on Blockchain

Junsang Kim*

Abstract

Since the announcement of bitcoin, new cryptocurrencies have been launched steadily and blockchain technology is also evolving with cryptocurrcies. In particular, security-related technologies such as consensus algorithm and hash algorithm have been improved and transaction processing speed has also been drastically improved to a level that can replace a centralized system. In addition, the advent of smart contract technology and the DApp platform also provides a means for cryptocurrency to decentralize social services beyond just payment.

In this paper, we first describe the technologies for implementing cryptocurrency. And the major cryptocurrencies are described with a focus on the technical characteristics. In addition, the development of cryptocurrency technology is expanding the scope of use, so we tried to introduce various cryptocurrencies

▸Keyword: Cryptocurrency, Blockchain, Smart Contract, Consensus Algorithm, Hash Algorithm, DApp

I. Introduction

암호화폐의 개념은 1983년 데이비드 차움(David Chaum)에 의해서 처음 제안되었다. 그는 DigiCash라는 회사를 설립한 후 디지털화된 달러에 고유한 해시값을 붙인 세계최초의 암호화폐인 Ecash[1]를 출시했다. 이후 1997년에는 아담 백(Adam Back)에 의해 해시캐시(Hashcash)[2]가 제안되었다. 해시캐시는 암호화폐는 아니지만 이후 블록체인의 합의 알고리즘으로 널리 쓰이는 작업증명(Proof-of-Work, PoW)를 처음으로 제안했다. 1998년 웨이다이(Wei Dai)는 익명성을 보장하고 분산 저장을 지원하는 비머니(B-money)[3]를 고안했다. 비머니는 참여자들이 소유한 암호화폐에 대한 정보를 해시함수로 암호화 하여 별도의 데이터베이스로 각자 저장한다. 같은 해 닉 재보(Nick Szabo)는 비트골드(Bit Gold)[4]라는 암호화폐를 고안했다. 참여자들이 해시파워를 이용하여 네트워크를 유지하고 비트골드를 얻게 되는 구조이다. 비머니와 비트골드는 이중지출 문제를 해결하지 못했고 실제로 출시되지도 못했다. 하지만 제안된 아이디어들은 대부분 비트코인(Bitcoin)[5]에서 구현되었다.

비트코인은 2009년 나카모토 사토시라는 신원미상의 인물이 만든 암호화폐로 비트골드와 비머니의 아이디어를 실제로 구현하고 이중지출 문제 등의 단점을 보완한 것이다. 비트코인은 중앙기관이 없이 참여자들의 네트워크를 통해 모든 거래가 이루어지고 검증된다. 비트코인은 블록체인(blockchain) 기술로 구현한 최초의 암호화폐로 1세대 암호화폐의 대표주자로 인정받고 있다. 이후에 개발된 암호화폐들도 대부분 블록체인을 기반으로 하고 있다.

2015년 비탈릭 부테린(Vitalik Buterin)이 개발한 이더리움(Ethereum)[6]은 비트골드를 개발한 닉 재보가 1994년 처음 제안한 스마트 계약(smart contract)을 블록체인을 기반으로 하여 구현한 최초의 암호화폐 플랫폼이다. 비트코인은 처음에는 기존 화폐와 은행 시스템을 대체하기 위한 수단에 불과했지만 이더리움은 블록체인 위에 서비스 및 어플리케이션을 제공하기 위한 플랫폼으로 진화했다. 그래서 이더리움은 최초의 2세대 블록체인이라고 인정받고 있다.

이후 다양한 목적의 암호화폐들이 쏟아져 나오고 있으며 이더리움의 알려진 단점들인 거래 속도, 개발 환경, 상호호환성, 의사결정 알고리즘 등을 보완한 암호화폐들도 나오고 있다. 이들을 가리켜 3세대 암호화폐라는 의견들도 있지만 아직까지는 명확히 인정받고 있지는 못하다. 대표적으로 언급되는 3세대

• First Author: Junsang Kim, Corresponding Author: Junsang Kim
*Junsang Kim (jskim@inhatc.ac.kr), Dept. of Computer Science, Inha Technical College
• Received: 2018. 12. 06, Revised: 2019. 01. 02, Accepted: 2019. 01. 02.

암호화폐는 이오스(EOS)[7]와 카르다노(Cardano)[8]가 있다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 먼저 암호화폐를 이해하기 위한 개념 및 기술들에 대해서 설명한다, 그리고 3장에서는 현재 사용 중이거나 개발 중인 주요 암호화폐들을 기술적 측면에서 초점을 맞추어서 소개한다. 4장에서는 결론을 맺는다.

II. Background Technology of Cryptocurrency

암호화폐는 다양한 기술 요소로 구현되어 있고 계속적으로 성능이 개선되고 용도도 확장되고 있다. 본 장에서는 암호화폐를 구성하는 핵심적인 개념과 기술들에 대해서 설명한다.

1. Blockchain

블록체인은 수많은 노드가 P2P 네트워크로 연결되어 트랜잭션을 처리하고 기록하는 '분산 원장 시스템'을 의미한다[9]. 전통적인 원장(장부) 시스템은 은행을 예로 들 수 있다. 은행은 신뢰성 있는 중개인(middleman)으로써 각종 전자 결재 및 금융거래 등을 기록하고 관리한다.

비트코인을 창시한 나카모토 사토시는 전통적인 은행시스템에 대해서 비판적인 생각을 가지고 있었다. 당시 리먼 브라더스 사태 등 금융권의 신뢰가 무너지는 사건들이 있었기 때문이다. 그는 결국 3자를 통하지 않고 각종 전자결제를 처리할 수 있는 방안을 구상하게 되었고 이를 구현한 비트코인이 출시되게 되었다. 비트코인은 3자를 통하지 않고 전자결제를 기록하고 보증하기 위하여 분산 원장 시스템을 채택했다.

분산 원장의 데이터는 전통적인 원장 시스템과 달리 여러 시스템(노드)에 저장되어 있다. 어떠한 거래기록이 원장에 기록되면 모든 시스템이 그 기록을 동기화하여 동일한 원장을 유지한다. 만약 여러 사용자가 동일한 데이터에 대해 기록을 요청하게 되면 정해진 합의 알고리즘에 의해 처리된다. 이러한 분산 원장 시스템을 구현한 기술이 바로 블록체인이다.

블록체인은 블록으로 이루어진 연결 리스트(linked list)이다. Fig. 1과 같이 새로 생성되는 블록의 헤더는 연결할 블록의 블록의 해시를 포함하는 방법으로 서로 연결되게 된다.

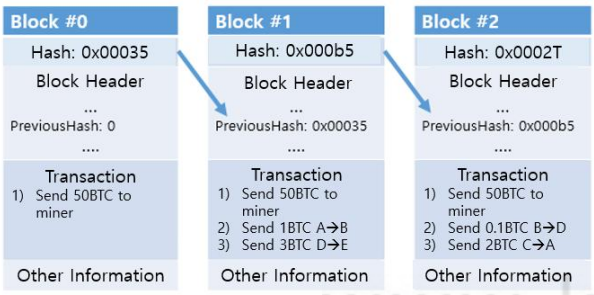

Fig. 1. Blockchain Architecture

블록체인 네트워크를 구성하는 노드들은 지리적으로 분산되어 있기 때문에 거래내역의 전파에는 시간이 걸릴 수 밖에 없다. 블록체인은 하나의 원장을 유지해야 하기 위해 다음과 같은 절차로 블록을 생성한다.

1) 거래 정보를 받은 노드 A – 해당 거래의 유효성을 검증, 후보 블록에 거래 정보를 기록, 다른 노드들에게 전파
2) 거래 정보를 받은 노드 B – 위와 동일 작업 수행
3) 거래 정보들이 모아지면 합의 알고리즘에 의하여 블록 생성,
4) 모든 노드들에게 블록 전파
5) 만약 여러 노드에서 거의 동시에 블록이 생성되어서 전파되고 있다면 합의 알고리즘에 의해서 연결될 블록 선택, 다른 블록들은 버려짐

블록체인에 기록된 데이터는 블록체인에 참여한 모든 노드에 의해서 보증이 된다. 모든 노드가 동일한 원장을 보유하고 있기 때문에 이를 임의로 변경하려면 모든 노드들을 해킹해야 한다. 뒷 블록의 해시는 앞 블록의 해시를 포함해서 생성되기 때문에 특정 블록을 임의로 수정하는 행위 또한 불가능하다.

블록체인은 비트코인에서 최초로 구현되었고 2009년 1월 3일 최초의 블록(genesis block)이 만들어 진 후 지금까지 계속해서 10분마다 블록이 생성되고 있다. 블록체인은 탈중앙화된 암호화폐에 요구되는 사항인 보안성과 안정성을 제공할 수 있다. 그래서 이후 많은 암호화폐들이 블록체인을 기반으로 설계되었다. 하지만 블록체인 기술은 단지 비트코인과 같은 암호화폐에만 한정되지는 않는다. 탈중앙화, 보안 및 검증이 필요한 다양한 산업에서 사용되고 있고 활용 범위도 점점 넓어지고 있다.

2. Consensus Algorithm

합의 알고리즘(consensus algorithm)은 네트워크의 모든 참여자들이 하나의 결과에 대한 합의를 도출하기 위한 알고리즘이다. 많은 노드들로 이루어진 블록체인 네트워크는 어떠한 경우에도 하나의 데이터베이스, 즉 블록체인을 유지할 수 있어야 한다. 특히 공개 블록체인은 누구나 노드가 될 수 있으므로 블록체인의 데이터를 변조하려는 악의적인 노드에 의한 공격을 방어할 수 있는 수단이 필요하다. 이 문제는 흔히 비잔틴 장군 문제(byzantine generals' problem)[10]로 표현된다. 흩어져 있는 장군들이 같은 시간에 성을 공격하기 위해 메시지를 서로 공유해야 한다. 메시지는 전파되는 시간이 필요하기 때문에 장군들 중 첩자가 메시지를 조작하여 전파하면 잘못된 메시지가 공유될 수 있다는 문제가 있다. 장군들은 이러한 첩자가 소수 있더라도 동일한 메시지를 공유할 수 있어야 한다.

블록체인 네트워크의 관점에서 보면 악의적인 노드가 소수 존재하더라도 동일한 내용의 블록체인을 유지할 수 있어야 한다. 블록체인은 각 노드들이 만든 블록을 검증하고 블록체인에 반영하기 위해 합의 알고리즘을 사용한다. 누군가 거래내역을 조작한 블록을 생성하게 되면 합의 알고리즘에 의해서 채택되

지 않고 버려지게 된다. 이를 통해 수많은 노드들이 동일한 내용의 블록체인을 유지할 수 있게 된다.

2.1 Proof-of-Work(PoW)

PoW(작업증명)는 Hashcash에서 제안되고 비트코인에서 사용되는 합의 알고리즘이다. PoW는 특정 노드가 특정 알고리즘으로 생성된 해시 문제를 풀면 블록을 생성할 권리를 부여하고 대가로 비트코인을 지급한다. 이 문제는 반복적인 연산을 필요로 하는 단순 작업으로 결국 해시 함수를 푸는 연산 능력이 우수한 노드, 즉 해시 파워(hash power)를 많이 가진 노드가 블록을 더 많이 생성할 수 있고 비트코인도 더 많이 지급받게 된다. 즉 더 많은 연산 작업을 했다고 증명한 노드에게 블록 생성 권한을 주는 것이다. 만약 두 개 이상의 노드에서 거의 동시에 문제를 풀어서 블록을 생성하게 된다면 이 블록들이 모든 노드들에게 전파되면서 어느 순간 충돌을 일으키게 된다. 이 때 해당 블록 이후로 연결된 블록들을 확인해서 더 긴 노드의 블록을 선택하게 된다. 더 많은 작업 증명을 한 노드에게 블록의 생성 권한을 주는 것이다. 이렇게 블록을 생성하는 일련의 과정을 채굴(mining)이라고 한다. 그래서 PoW는 비트코인, 이더리움, 라이트코인 등 채굴이 가능한 모든 암호화폐에 적용된다.

해시 파워를 요구하는 것은 악의적이거나 신뢰성이 부족한 노드가 비트코인 블록체인 네트워크에 참여하는데 일종의 진입 장벽의 역할도 한다. 높은 해시 파워를 갖추려면 장비구입 및 전력 비용이 많이 들기 때문이다. 만약 비트코인 블록체인 네트워크에서 특정 세력이 전체 해시 파워의 51% 이상 점유하게 된다면 누구보다도 빨리 블록을 생성할 수 있기 때문에 거래기록이 조작된 블록을 생성하여 블록체인에 연결할 수 있다. 이를 '51% 공격'이라고 한다. 하지만 비트코인의 경우 전체 해시 파워의 51%를 한 세력이 갖추는 것은 이론적으로만 가능하고 경제적으로는 불가능에 가깝다. 다만 전체 해시 파워가 미약한 암호화폐들의 경우 51% 공격이 성공한 경우가 있다.

2.2 Proof-of-Stake(PoS)

PoS(지분증명)는 PeerCoin이라는 암호화폐에서 최초로 발표한 합의 알고리즘이다. PoS의 경우 암호화폐를 많이 보유한 노드가 블록을 생성할 권리를 많이 얻게 된다. 즉 지분(stake)을 많이 보유한 사람이 블록을 생성할 수 있는 권리를 얻게 되며 보상도 많이 받게 된다. 이자 및 배당과 유사한 개념이다. 암호화폐를 많이 소유하고 있는 노드일수록 그 가치를 유지하기 위해 시스템의 신뢰성을 손상시키지 않을 것이라는 전제를 기반으로 한다. 결국 위와 같은 역할을 하는 채굴 과정(작업증명)이 필요없기 때문에 PoW의 에너지 낭비 문제를 해결할 수 있다.

PoS를 기반으로 하는 암호화폐는 일반적으로 초기에 ICO(Initial Coin Offering)을 통해 대량의 코인이 판매되고 이후 블록 생성에 대한 대가로 조금씩 분배된다. 일반적으로 ICO를 통해 암호화폐를 판매할 때는 일반적으로 내부 구성원들과 기관 투자자 및 개인 투자자들에게 분배 및 판매한다. 만약 누군가가 51% 이상의 지분을 가지고 있으면 PoW와 마찬가지로 51% 공격이 가능하다. 하지만 성공한 ICO의 경우 암호화폐의 가격이 높고 보유자 층이 넓기 때문에 51%의 지분을 확보하는 것이 거의 불가능에 가깝다. 만약 실패한 ICO라 하더라도 51% 씩이나 지분을 보유하고 있는 노드가 굳이 블록체인 네트워크의 신뢰성을 떨어뜨려 자신의 보유한 자산의 가치를 떨어뜨릴 이유가 존재하지 않는다. 그러므로 51% 공격에 대해서는 PoW보다 더 안전하다고 판단할 수 있다.

2.3 Delegated Proof-of-Stake(DPoS)

DPoS(위임된 지분증명)는 이오스의 개발자인 댄 라리머(Dan Larimer)에 의해 고안된 합의 알고리즘이다. PoS는 일정 지분을 가진 모든 노드에게 블록 생성 권한을 부여하지만 DPoS의 경우 지분 위임 결과(투표 결과)에 따라 선출된 상위 노드에게 권한을 위임하여 합의를 수행한다. 상위 노드는 암호화폐 보유자들의 투표로 선출되며 보유자들은 본인이 가진 암호화폐의 수만큼 투표 권리를 행사할 수 있다. 상위 노드 외에는 블록을 생성하지는 못하지만 상위 노드가 는 본인에게 투표한 사용자에게 블록 생성에 따른 보상을 분배할 수 있다.

DPoS를 기반으로 하는 암호화폐의 경우 상위 노드의 수가 제한되어 있기 때문에 합의 시간을 줄일 수 있어 단위 시간당 많은 트랜잭션을 처리할 수 있다는 장점이 있다. 또한 소량의 암호화폐 보유자들이 비용이 드는 노드 운영을 하지 않아도 보상을 받을 수 있다는 장점이 있다.

PoS가 직접 민주주의라면 DPoS는 간접 민주주의라고 할 수 있다. 앞서 언급한 장점은 간접 민주주의의 장점과 연관이 있다. 하지만 간접 민주주의의 경우 현실 정치에서도 그렇듯 단점들이 존재한다. 우선 상위 노드의 수가 적기 때문에 효율성은 높지만 해커들이 공격해야 할 노드가 적다는 의미도 된다. 그리고 암호화폐는 특성상 거래소에 보관하는 비중이 상당히 큰데 거래소에서 투표시스템을 갖추지 않을 경우 그 권리를 거래소에서 남용할 수 있다. 투표율이 저조한 경우나 상위 노드들 간의 담합 또한 민주주의가 왜곡되는 경우라고 볼 수 있다.

2.4 Other Consensus Algorithms

앞서 언급한 3가지의 대표적인 합의 알고리즘 외에도 다양한 합의 알고리즘이 존재한다. Proof of Importance(PoI, 중요성증명)는 노드의 중요성을 평가하여 높은 평가를 받은 노드가 블록을 생성하는 합의 알고리즘이며 Proof of Authority(PoA, 권위증명)는 허가받은 노드들만 블록을 생성하는 합의 알고리즘이다. PBFT(Practical Byzantine Fault Tolerance)의 경우는 DPoS처럼 대표 노드들 간의 합의로 블록이 승인된다. 하지만 모든 노드들이 합의하지 않아도 일정 비율 이상의 노드가 합의되면 블록이 검증되어 블록체인에 연결된다.

하이브리드 형태의 합의 알고리즘도 존재한다. 예를 들어 PoW + PoS의 경우 일정 기간동안 PoW의 형태로 채굴이 가능하다가 정해진 양 만큼 채굴이 끝나면 되면 PoS로 전환되는 구조이다.

3. Hash Algorithm

해시는 어떤 문자열을 입력했을 때 특정 비트 길이의 문자열로 생성해준다. 특정 알고리즘에 의해 특정 데이터를 입력하면 같은 해시값이 생성 된다. 만약 한 글자라도 다르면 다른 해시값이 생성되도록 구현된 알고리즘이다.

해시값은 출력값이 주어졌을 때 입력값을 찾는 것이 구조적으로 굉장히 어렵다. 이러한 특성 때문에 PoW를 기반으로 하는 암호화폐에서는 다음 블록을 생성할 노드를 선출하는데 해시 알고리즘울 사용한다. 비트코인의 경우 각 블록의 헤더를 보면 Nonce라는 값이 있다. 노드들은 이 Nonce 값을 1비트씩 바꾸어보면서 목표치 보다 작은 해시값이 나올 때 까지 입력을 무한 반복한다. 이 해시값을 가장 먼저 찾은 노드(채굴자)에게 해당 블럭을 생성할 수 있는 권한과 보상이 주어진다. 그래서 높은 해시파워를 가지고 있는 채굴자들이 해시값을 맞추어 채굴할 확률이 높아진다.

비트코인에서는 SHA-256이라는 256비트의 해시값을 생성하는 해시 알고리즘을 썼는데 이 알고리즘에 적합하고 높은 해시파워를 가진 ASIC 채굴기가 개발되면서 그래픽 카드로 사용하는 개인 사용자들의 채굴이 어려워졌다. 그래서 비트코인 골드[11]의 경우 ASIC 채굴기를 사용하지 못하도록 비트코인을 하드 포크해서 Equihash라는 해시 알고리즘으로 변경하였다. 라이트코인[12]도 ASIC 채굴기의 병렬처리를 막기 위해 Scrypt라는 해시 알고리즘을 도입했다.

4. Smart Contract

최초의 암호화폐인 비트코인은 블록체인을 이용해서 중계기관이 없는 대금 결제 및 송금의 기능을 구현하였다. 하지만 스마트 계약은 그 범위를 확장시켜 모든 종류의 계약을 중계 기관 없이 처리할 수 있는 기능이다. 스마트 계약은 쉽게 말해 음료수 자판기와 유사한 동작 개념을 가지고 있다. 음료수 자판기는 구매자가 일정 이상의 동전을 투입하면 해당하는 금액의 음료를 선택할 수 있는 권리를 부여하고, 구매자가 음료를 선택하면 해당 음료와 잔액을 반출한 후에 거래가 종료되게 되도록 프로그래밍 되어 있다.

스마트 계약의 경우 계약 당사자들이 계약 내용을 프로그래밍하여 블록체인에 기록한다. 계약 내용과 결과는 블록체인에 영구히 기록되기 때문에 조작이 불가능하다. 만약 계약이 성립되면 자동적으로 암호화폐가 계약된 만큼 당사자들 사이에 전송된다.

현실에서의 계약은 조작 및 부인을 방지하기 위하여 신뢰성 있는 3자의 공증이 필요하다. 하지만 스마트 계약은 3자가 필요 없고 블록체인 네트워크를 구성하는 노드들이 공동으로 증명한다. 또한 현실에서의 계약은 조건이 부합했을 때 당사자가 직접 계약조건을 처리하기 위해 송금 등의 역할을 해야 되지만 스마트 계약은 조건이 충족되면 자동으로 계약이 실행된다. 3자의 공증비용이 과도한 경우 비용을 감소시킬 수 있는 장점도 있다.

5. Decentralized Application(DApp)

우리가 흔히 사용하는 인터넷 뱅킹이나 각종 예약 앱의 경우 특정 기업의 서버를 통해 장부를 기입하는 중앙화 된 서비스의 형태로 구축되어 있다. 이러한 애플리케이션은 운영 주체가 신뢰성 있는 3자가 되어 사용자들을 서로 연결 및 중계해주는 역할을 한다. 이렇게 중앙화된 어플리케이션은 안정적인 서비스를 제공할 수 있지만 해킹의 위협에 비교적 취약한 편이고 운영 주체의 권한이 막강하기 때문에 이로 인한 부정적 측면 또한 존재한다. 운영 주체가 서비스를 중단할 수도 있고 과도한 수수료를 요구할 수도 있다. 가장 중요한 주체들인 서비스를 제공해주거나 받는 사람들은 이러한 결정과정에 참여할 권리를 얻지 못하는 경우가 많다.

탈중앙화 된 어플리케이션, 즉 DApp은 이러한 비민주적인 의사결정구조를 해결할 수 있는 좋은 방법이다. DApp는 이미 구축된 블록체인 플랫폼을 기반으로 하는 어플리케이션이다. DApp는 스마트 계약을 기반으로 구현되다. 그러므로 미리 설정된 스마트 계약의 조건에 따라 수행된다. 어플리케이션이 제공하는 모든 서비스의 거래과정은 투명하게 블록체인에 기록되고 본인이 가지고 있는 지분만큼의 서비스 운영에 관한 의사결정에 참여할 수 있기 때문에 민주적인 서비스 운영이 가능하다.

DApp 개발자는 별도의 블록체인 네트워크 구축 없이 서비스를 운영하고 수익을 얻을 수 있다. 다만 블록체인 플랫폼을 사용하는 경우 일정 부분의 수수료가 필요하며 이 수수료는 블록체인 네트워크을 운영하는 노드들에게 배분된다.

III. Introducing of Cryptocurrencies

본 장에서는 주요 암호화폐들을 소개하고 기술적 특징들에 대해 설명한다. 설명한 주요 암호화폐들의 세부사양은 Table 1에서 자세하게 정리한다.

1. Bitcoin[5]

비트코인은 블록체인 기술을 구현하여 만들어진 최초의 암호화폐이다. 비트코인은 순수 지불을 위한 암호화폐로 성능적으로나 기능적으로는 다른 암호화폐에 비해 부족하지만 여전히 다양한 암호화폐의 거래를 위한 주축통화로써의 역할을 하고 있다.

비트코인의 블록체인 네트워크는 평균 10분마다 트랜젝션들을 모아서 블록을 생성한다. 블록을 생성하는데 사용되는 합의 알고리즘은 PoW이다.

비트코인의 거래량이 증가하면서 기존의 1MB의 블록사이즈와 10분의 블록 생성 시간으로는 빠른 거래처리가 불가능했다. 이 문제를 해결하기 위해 비트코인의 개발자 그룹은 세그윗(segwit)과 라이트닝 네트워크(lightning network) 라는 방법을 제안했다. 거래 기록에는 거래를 승인하기 위해 많은 부분이

서명으로 이루어져 있는데. 이 서명 부분을 따로 분리해 따로 저장하는 방식을 세그윗이라고 한다. 또한 라이트닝 네트워크는 비트코인 네트워크에 추가로 서브체인을 추가하여 메인체인의 부하를 감소시키는 방법이다. 하지만 비트코인의 블록체인 네트워크를 운영하는 채굴자들은 세그윗과 라이트닝 네트워크를 반대하고 블록의 사이즈를 늘려서 비트코인 블록체인 네트워크가 처리할 수 있는 트랜잭션의 용량을 증가시키기 원했다. 세그윗을 하면 기존 블록구조에 적합한 채굴기의 효율이 감소하여 수익이 악화되기 때문이다. 개발자 그룹에서는 블록 크기가 커질 경우 비트코인 코어의 용량이 기하급수적으로 증가하기 때문에 이를 감당할 수 없는 소규모 채굴자들이 떠날 것을 우려했다.

이러한 상황에서 개발자들과 채굴자들이 조금씩 양보하면서 나온 방안이 세그윗2x이다. 세그윗을 적용하면서 블록사이즈도 2배로 늘리는 방안이었다. 하지만 결국은 합의에 이르지 못하고 2017년 8월 1일 478558 블록을 기점으로 비트코인과 비트코인 캐시로 하드포크(hardfork) 되어 분리 되었다.

2. Bitcoin Cash[13]

비트코인 캐시는 비트코인에서 하드포크 된 암호화폐이다. 하드포크는 블록체인을 업그레이드 하는 방식 중에 업그레이드 후 기존의 블록체인과 다른 추가적인 블록체인이 된다.

비트코인 캐시는 처리속도를 높이기 위해서 블록크기를 8MB까지 늘렸고 현재는 32MB까지 업그레이드 했다. 블록 사이즈가 증가하면서 기존의 비트코인 블록 보다 더 많은 트랜잭션을 기록할 수 있게 되어 처리 속도가 빨라졌다. 비트코인 캐시는 처음에는 블록 크기를 제외하면 비트코인과 동일했다. 블록 생성 간격도 10분이고 합의 알고리즘도 PoW로 동일하다. 하지만 비트코인 캐시는 스마트 계약 기능을 개발하는 등 독자적으로 기능들을 추가하면서 발전하고 있다.

3. Bitcoin Gold[11]

비트코인 골드 또한 비트코인에서 하드포크 된 암호화폐이다. 비트코인 골드는 채굴의 탈중앙화를 모토로 탄생되었다. 원래 비트코인은 누구나 쉽게 구할 수 있는 그래픽 카드를 이용해서 채굴할 수 있었으나 대규모 채굴업자들이 높은 해시파워를 가지고 있는 ASIC 방식의 전용 채굴기를 이용하여 채굴을 독점하는 현상이 발생했다. 비트코인 골드는 이러한 문제를 해결하기 위해 해시 알고리즘을 변경하여 ASIC 채굴을 막았다. 비트코인과 비트코인 캐시는 'SHA-256'이라는 해시 알고리즘을 사용하는데 비트코인 골드는 'Equihash'라는 해시 알고리즘을 사용한다. 또한 비트코인 골드도 세그윗과 라이트닝 네트워크를 적용하여 트랜잭션 처리 성능을 향상시켰다. 또한 향후 스마트 계약 기능도 추가할 예정이다.

4. Litecoin[12]

구글 소프트웨어 엔지니어 출신인 찰리 리(Charlie Lee)에 의해 개발된 암호화폐로 비트코인을 기반으로 만들어졌다. 비트코인의 낮은 처리속도를 개선시키기 위해 블록 생성시간을 2분 30초로 줄여 4배 빨라졌고 블록 사이즈도 4MB까지 늘렸다. 또한 세그윗과 라이트닝 네트워크를 도입해 트랜잭션 처리 속도를 더욱 향상시켰다. 앞으로 스마트 계약을 가능하게 해주는 MAST(Merkelized Abstract Syntax Trees)라는 기술도 추가할 예정이다. 라이트코인은 라이트코인 재단을 통해 오픈소스 프로젝트로 개발되고 있다.

5. Ethereum[6]

이더리움은 2015년 비탈릭 부테린이 개발한 블록체인을 기반으로 스마트 계약을 지원하는 분산 응용 어플리케이션 플랫폼이다. 이더리움은 플랫폼을 의미하며 이더리움에서 사용하는 암호화폐는 '이더'라고 정의하지만 보편적으로는 이더리움이 플랫폼과 암호화폐 모두를 지칭하는 표현으로 사용되고 있다. 이더리움은 현재 스위스에 위치한 이더리움 재단에서 오픈소스 프로젝트로 개발하고 있다.

이더리움은 스마트 계약을 구현하기 위해 솔리디티(Solidity)라는 고유의 프로그래밍 언어를 제공한다. 솔리디티는 계약 지향 프로그래밍 언어로 바이트코드로 컴파일 된 후에 이더리움 블록체인에 기록된다. 기록된 바이트 코드는 이더리움 가상머신(Ethererium Virtual Machine, EVM) 위에서 동작한다.

DApp은 자바 스크립트나 파이썬 등의 프로그래밍 언어를 사용하여 프로그래밍 할 수 있으며 이더리움 플랫폼 위에서 동작하기 때문에 탈중앙화된 형태의 어플리케이션을 쉽게 구현할 수 있다. DApp 또한 거래와 보상을 위해 이더리움을 기반으로 하는 자체 암호화폐를 발행할 수 있다. 이더리움 플랫폼은 ERC-20, ERC-721라는 토큰의 표준을 제공한다.

이더리움에 참여하는 모든 노드들은 이더리움 가상머신을 실행한다. 이더리움 가상머신은 eWASM(Ethereum flavored WebAssembly)이라는 새로운 가상머신으로 교체를 준비하고 있다. eWASM이 도입되면 솔리디티 외에 다른 범용 프로그래밍 언어로도 DApp을 개발할 수 있게 되고 보다 효율적인 프로그래밍이 가능하다.

이더리움은 12초 마다 하나씩 블록을 생성하고 있고 블록의 사이즈도 가변적이기 때문에 비트코인보다 빠른 트랜잭션 처리 성능을 보여준다. 그럼에도 불구하고 현재 이더리움 플랫폼은 많은 사용자들로 인해 트랜잭션 처리가 상당히 느려지고 있다. 이더리움은 현재 합의 알고리즘으로 PoW를 채택하고 있지만 처리속도 향상을 위해 PoS기반의 합의 알고리즘인 캐스퍼(Casper)로 전환을 준비하고 있다. 또한 전체 블록체인 네트워크를 여러 개의 소규모 네트워크로 분할하여 처리하는 방법인 샤딩(Sharding)을 적용하여 트랜잭션 처리속도를 더 향상시킬 예정이다.

6. Ripple[14]

리플은 블록체인을 기반으로 하는 차세대 글로벌 결제 네트

워크이다. 리플은 송금 기능에 특화된 블록체인 네트워크로 기존의 국제 송금 방식인 SWIFT(Society for Worldwide Interbank Financial Telecommunication)를 대체할 목적으로 개발되었다. 리플은 SWIFT 같은 중계기관 없이 P2P로 거래하기 때문에 저렴한 비용으로 국제 송금 및 결제 서비스를 제공할 수 있다. 리플에서 사용되는 암호화폐는 리플코인이며 교환되는 화폐간의 중간 역할을 하기 위해 사용된다. 리플은 일반적인 암호화폐와는 달리 리플랩스라는 운영주체가 있는 중앙화된 구조의 블록체인이며 블록체인에 참여하는 것도 허가 받은 노드만 가능한 프라이빗 블록체인(private blockchain)이다. 소수의 노드로 운영되기 때문에 매우 빠른 트랜잭션 처리(3.5초)가 가능하다.

7. EOS[7]

이오스는 유명 블록체인 개발자인 댄 라리머 주도로 개발된 퍼블릭 블록체인 플랫폼이다. 기존 블록체인 플랫폼의 비싼 수수료와 느린 트랜잭션 처리속도를 개선하기 위한 목적으로 개발되었다. 이오스는 많은 부분이 웹 어셈블리로 개발되었기 때문에 스마트 계약을 웹브라우저상에서 빠르게 실행할 수 있다

이더리움 기반의 DApp들은 그 DApp의 서비스를 이용하기 위해 직접 이더리움을 구매해서 지불해야 하는 단점이 있다. 하지만 이오스 기반의 DApp들의 경우 트랜젝션 자체에는 비용을 내지 않고 DApp 개발사가 이오스를 보유한 만큼의 대역폭을 확보하여 서비스를 제공하는 형태이다. 이러한 구조는 기존의 중앙화된 무료 서비스들이 탈중앙화된 블록체인 기반으로 이동할 수 있는 기회를 제공한다.

이오스는 DPoS를 합의 알고리즘으로 채택했으며 이오스 보유자들의 투표로 블록 프로듀서(Block Producer, BP)라 불리는 21명의 대표자 노드를 선출해서 블록을 생성할 수 있는 권한을 얻는다. 투표는 정해진 날짜에 진행되는 것이 아니라 라운드 단위로 투표자들이 자신의 지분만큼 BP에서 투표하거나 철회할 수 있다. 신뢰를 잃은 BP는 언제든지 다른 BP로 대체될 수 있는 구조를 가지고 있다.

8. NEO[15]

네오는 스마트 경제를 실현하기 위해 블록체인 기술을 이용한다. 실물 자산을 디지털 자산화 하고 그 소유권을 블록체인 위에서 거래하는 것이다. 이러한 디지털 자산들은 스마트 계약을 통해 거래된다.

네오의 가장 큰 특징은 이중 토큰 구조를 가지고 있다는 것이다. 블록이 생성될 때마다 가스(GAS)라는 암호화폐가 추가적으로 생성되며 1년마다 생산량이 반감된다. 가스는 네오 보유자들에게 배당되며 네오 블록체인 네트워크에서 수수료로 사용된다.

네오의 합의 알고리즘은 dBFT(delegated Byzantine Fault Tolerance)로 DPoS와 유사하다. 네오의 스마트 계약 또한 이더리움과 거의 유사하며 이더리움, 이오스와 마찬가지로 DApp을 개발할 수 있는 플랫폼을 제공한다. 또한 네오는 이더리움과 달리 대부분의 주요 프로그래밍 언어를 지원한다는 장점이 있다.

9. Stellarlumen[16]

스텔라루멘은 리플에서 하드포크 된 암호화폐로 리플과 동일한 국제 송금용 서비스를 제공하는 목적으로 개발되었다. 리플과 다른 특징은 크게 두 가지인데, 첫 번째는 합의 알고리즘로 스텔라 합의 프로토콜(Stellar Consensus Protocol, SCP)을 사용한다는 것이다. SCP는 사용자가 어떤 노드를 신뢰할 것인지 직접 선택하여 이를 바탕으로 형성된 신뢰망을 통해 합의에 이르는 방식으로 동작한다. 두 번째는 리플과는 다른 퍼블릭 블록체인이라는 점이다. 퍼블릭 블록체인이지만 합의 과정은 모든 노드가 참여가 가능하고 전송 과정은 참여 제한을 두어 리플처럼 빠른 트랜잭션 처리가 가능하다는 장점이 있다.

10. Tether[17]

테더는 홍콩의 비트파이넥스 거래소와 관련된 업체인 테더 리미티드가 발행하는 미국 달러와 연동되는 암호화폐이다. 일반적으로 가격의 등락이 있는 암호화폐들과는 달리 1테더는 1달러의 가치를 유지하도록 설계되어 있다. 테더 리미티드는 지급 보증을 위해 발행한 테더의 개수만큼 계좌에 달러를 보관하고 있다. 테더는 계좌에 있는 달러를 담보로 안정적인 가치를 유지하기 때문에 가격의 변동이 매우 적다. 그래서 거래소에서 기축통화로 많이 사용되며 특히 실물 화폐를 다루지 않는 국제거래소에서 많이 사용된다. 이러한 특성의 태환형 암호화폐는 테더 외에도 TrueUSD, USD Coin 등이 있으며 이들을 통칭하여 스테이블 코인(stable coin)이라고 한다.

11. Cardano[8]

카르다노는 암호화폐가 설계되고 개발되는 방식을 바꾸려는 노력의 일환으로 2015년에 시작된 프로젝트이다. 카르다노는 블록체인 플랫폼의 이름이고 그 위에서 동작하는 암호화폐의 이름은 에이다(ADA)라고 한다. 카르다노는 분산형 퍼블릭 블록체인으로서 완전한 오픈 소스이며, 이전에 개발된 그 어떤 블록체인 플랫폼보다 더 많은 고급 기능을 제공하는 스마트 계약 기반의 블록체인 플랫폼이다. 하스켈(Haskel) 언어를 사용하여 구현되었기 때문에 성능 및 안정성이 뛰어나며 소프트포크를 통한 업그레이드가 용이하도록 설계되어 있다.

카르다노의 가장 큰 특징은 바로 합의 알고리즘으로 사용되는 우로보로스 지분증명(Ouroboros PoS, OPoS)이다. PoS는 지분 보유가 많을수록 높아지는 확률에 따라 다음 블록 생성자를 추첨해야 되는데 마지막 블록의 정보를 바탕으로 랜덤변수를 계산한다. 만약 마지막 블록 생성 노드가 블록 생성 시간 중에 랜덤 변수를 조작한다면 공정하지 않은 이득을 취하는 것이 가능해진다. 이를 Stake-Grinding Attack이라고 한다. OPoS는 랜덤변수 생성에 모든 노드가 참여할 수 있게 설계되었기 때문에 Stake-Grinding Attack 문제를 해결할 수 있다.

Table. 1. Specifications of Cryptocurrencies

Name	Code	Consensus Algorhthm	Block Size	Block Production Cycle	Hash Algorithm	MarketCap	Type	Smart Contract	Major developer/ Organization
Bitcoin	BTC	PoW	1MB	10m	SHA-256	21,000,000	Currency		Satoshi Nakamoto
Bitcoin Cash	BCH	PoW	32MB	10m	SHA-256	21,000,000	Currency	O	Wu Jihan
Bitcoin Gold	BTG	PoW	1MB	10m	Equihash	21,000,000	Currency	△	Jack Liao
Litecoin	LTC	PoW	4MB	2.5m	Scrypt	84,000,000	Currency	△	Charlie Lee / Litecoin Foundation
Ethereum	ETH	POW->POS (Scheduled)	Dynamic	12s	Ethash	Not determined	Platform	O	Vitalik Buterin / Ethereum Foundation
Ripple	XRP	RPCA	N/A	3.5s	N/A	100,000,000,000	Remittance		Chris Larsen / Ripple Labs
EOS	EOS	DPoS	Dynamic	3s	N/A	1,000,000,000	Platform	O	Dan Larimer / Blockone
Neo	NEO	dBFT	N/A	12~ 15s	SHA-256 & RIPEMD160	100,000,000	Platform	O	Da Hangfei / Onchain
Stella Lumen	XLM	SCP	N/A	3~5s	N/A	100,000,000,000	Remittance		Jed McCaleb / Stellar Development Foundation
Tether	USDT	PoR	N/A	N/A	Omnicore	Not determined	Stable		Tether Limited
Cardano	ADA	OPoS	64KB	20s	N/A	45,000,000,000	Platform	O	Charles Hoskinson, Jeremy Wood / IOHK
Monero	XMR	PoW	Dynamic	2s	CryptoNight	Not determined	Currency		Monero Core Team
Tron	TRX	DPoS	Dynamic	15s	N/A	100,000,000,000	Platform	O	Justin Sun / Tron Foundation
Binance Coin	BNB	POW->POS (Scheduled)	Dynamic	14s	Ethash	200,000,000	Exchange		Binance

※ N/A는 알려지지 않았거나 해당되지 않은 항목임.

12. Monero[18]

모네로는 기존의 비트코인에서 제공하는 기능에 거래 내역 추적 방지기능을 추가한 것이다. 비트코인은 모든 거래내용을 누구나 확인할 수 있는 투명한 시스템이지만 모네로는 링 시그니처(ring signature), 스텔스 주소(stealth address), 링 기밀거래(confidential transaction)라는 기술을 통해 모든 거래의 송신자, 수신자 및 금액을 숨길 수 있다.

모네로와 같은 추적 불가능한 암호화폐를 통칭하여 다크 코인(Dark Coin)이라고 하며 대시(Dash), 지캐시(Zcash), 코모도(Komodo) 등이 있다. 하지만 다크 코인의 보안성을 악용하여 자금 세탁 및 마약 거래에 사용되는 경우가 발생하면서 일본을 비롯한 몇몇 국가의 거래소에서는 퇴출되고 있다.

13. Tron[19]

트론은 콘텐츠 기반의 엔터테인먼트 산업 시스템을 만들기 위한 블록체인 프로젝트이다. 트론은 암호화폐 시장에서 가장 많은 분산 어플리케이션 사용자를 보유한 프로토콜이며 트론의 앱 파트너들은 천만명 이상의 사용자를 보유하고 있다.

트론은 합의 알고리즘으로 DPoS를 사용한다. 투표로 선정된 27개의 SR(Super Representative)들은 블록 생성 및 관리를 담당하게 되며 보상으로 블록 당 트론 암호화폐 32개를 지급받는다.

트론은 우수한 확장성과 효율이 높은 스마트 계약에 초점을 맞추어 개발하고 있다. 트론 프로토콜과 트론 가상머신(TVM; Tron Virtual Machine)을 사용해 DApp을 운영할 수 있는 블록체인 플랫폼을 제공한다. 트론을 기반으로 하는 DApp들은 다양한 모듈을 사용하여 개발이 가능하기 때문에 개발의 유연성이 보장되며 지속적인 확장이 가능하다.

14. Binance Coin[20]

바이낸스 코인은 이더리움 기반의 ERC-20 토큰 규격으로 발행되었다. 바이낸스 코인은 암호화폐 거래소인 바이낸스 거래소에서 사용되는 암호화폐로 거래소 내 수수료 지불 및 기축 통화로써의 역할을 한다. 최근 암호화폐 거래소들은 이러한 목적으로 사용할 자체 코인을 출시하는 경우가 많다. 거래소 코인은 바이낸스 코인 외에 쿠코인 거래소의 쿠코인 쉐어(KuCoin Shares), 후오비 거래소의 후오비 토큰(Huobi Token) 등이 있다.

IV. Conclusions

본 논문에서는 암호화폐의 이해를 위해 필요한 주요 기술인

블록체인, 합의 알고리즘, 해시 알고리즘, 스마트계약 DApp에 대해서 설명하고 주요 암호화폐들을 기술 발전의 흐름의 순서 따라 자세히 설명했다. 대부분의 암호화폐 프로젝트들은 아직 개발 중인 프로젝트이다. 트랜잭션 처리 속도나 보안적인 측면 같은 기술적 측면도 있지만 탈중앙화와 직접 민주주의의 구현이라는 사회적인 측면까지 계속적으로 발전하고 있다.

대부분의 암호화폐 프로젝트들은 기술적으로는 계속 보완되고 있지만 아직까지 상업적으로 성공한 프로젝트들이 매우 부족한 것이 현실이다. 플랫폼 코인들은 성공한 DApp들이 나타나야 하고 특성 서비스를 블록체인으로 구현하는 프로젝트들은 그 서비스가 성공해야 한다. 특히 암호화폐와 그 관련 기술에 대한 인식의 개선과 더불어 사회적 변화를 이끌어낼 수 있는 파급력을 지닌 프로젝트가 나타나야 한다.

앞으로 남아있는 기술적, 사회적 난제들을 극복한다면 암호화폐와 그 기반 기술들이 사회 시스템의 변화를 이끌어내는 4차 산업혁명의 핵심기술로 널리 사용될 것으로 기대된다.

REFERENCES

[1] Chaum, David. "Blind signatures for untraceable payments." Advances in cryptology. Springer, Boston, MA, 1983.

[2] Back, Adam, "Hashcash - a denial of service counter-measure.", *http://www.hashcash.org/papers/hashcash.pdf*

[3] Wei Dai, “b-money, an anonymous, distributed electronic cash system”, *http://www.weidai.com/bmoney.txt*

[4] Nick Szabo, "Bit gold“, *https://unenumerated.blogspot.com/2005/12/bit-gold.html*

[5] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*

[6] Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform-Ethereum Whitepaper“, 2014. *https://github.com/ethereum/wiki/wiki/White-Paper*

[7] Eos.io, *https://eos.io*

[8] Cardano, *https://www.cardano.org/en/home/*

[9] Narayanan, Arvind, et al., “Bitcoin and cryptocurrency technologies: a comprehensive introduction”, Princeton University Press, 2016.

[10] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), Vol 4, No 3, pp. 382-401, Jul, 1982.

[11] Bitcoin Gold, *https://bitcoingold.org/*

[12] Litecoin, *https://litecoin.org/*

[13] BitcoinCash, *https://www.bitcoincash.org/*

[14] Ripple, *https://ripple.com/*

[15] Neo, *https://neo.org/*

[16] Stellarlumen, *https://www.stellar.org/*

[17] Tether, *https://tether.to/*

[18] Monero, *https://www.getmonero.org/*

[19] Tron, *https://tron.network*

[20] Binance Coin, *https://www.binance.com/resources/ico/Binance_WhitePaper_en.pdf*

Authors

Junsang Kim received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Hanyang University, Korea, in 2003, 2005 and 2017, respectively He is currently a Assistant Professor in the Department of Computer Science, Inha Technical College. He is interested in blockchain, big data, and cloud computing.