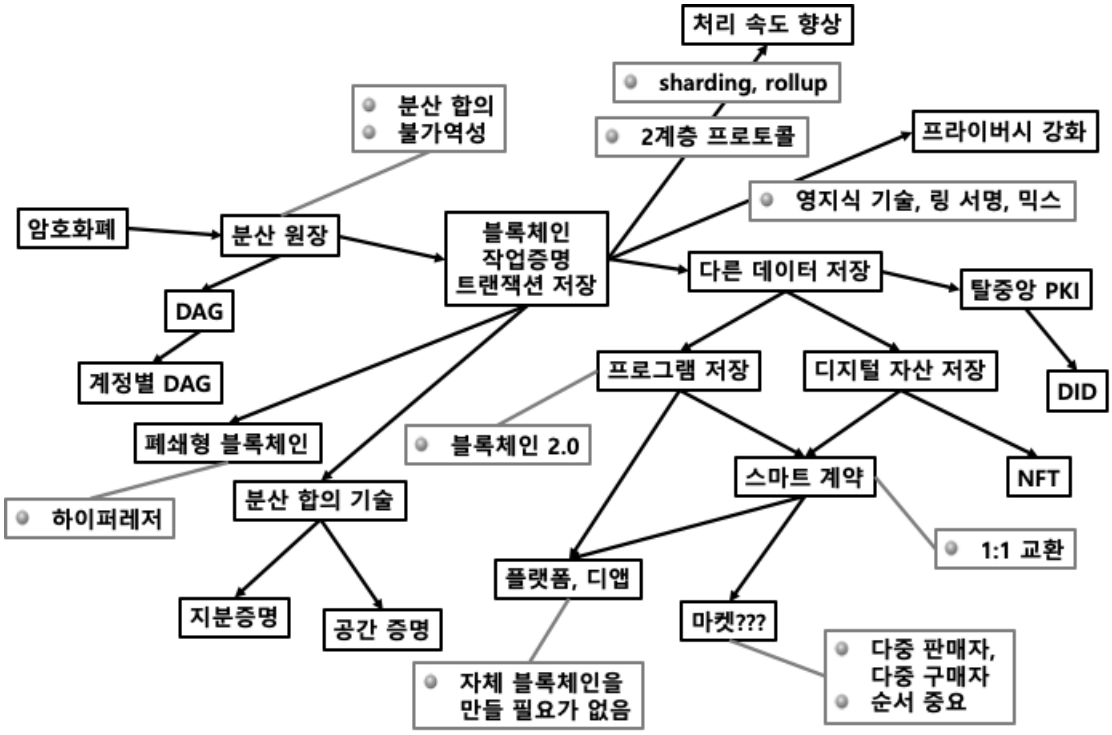
정보보호개론

제16장 블록체인 2.0

1. 블록체인 2.0

비트코인의 등장 이후, 수 많은 암호화폐가 새롭게 등장하였다. 또 블록체인을 암호화폐를 구현하기 위한 기술로 한정하지 않고 여러 응용에서 블록체인을 분산 첨삭 전용 데이터베이스로 활용하고자 하는 움직임도 일어나고 있다. 지금은 인터넷과 웹이 우리 삶에 가지고 온 변화 이상으로 새로운 혁명을 일으킬 기술로 블록체인 기술을 바라보고 있다. 이 장에서는 비트코인 이후 등장한 알트코인과 이들 코인에서 사용하는 기술을 살펴본다. 또한 블록체인 기술의 발전과 미래를 생각해 본다.

1.1 비트코인 이후 블록체인의 발전



<그림 16.1> 블록체인 기술 맵

사토시 나카모토에 의해 블록체인이 분산 암호화폐를 구현하기 위해 사용된 이후 블록체인 기술과 암호화폐는 그림 16.1에 제시된 것처럼 여러 측면에서 개선되고 발전하고 있다. 이 발전 내용을 우선 이 절에서 간단하게 살펴보고 일부 내용에 대해서는 이 장에서 상세히 설명한다. 비트코인은 블록체인에 트랜잭션만 저장한다. 이 블록체인은 작업증명이라는 방법을 통해 참여하는 노드들이 저장할 데이터에 대한 분산 합의를 할 수 있도록 해주고, 저장된

데이터의 불가역성을 보장해 준다. 저장된 데이터의 불가역성은 여러 가지 응용에서 활용할 수 있다. 이에 블록체인에 트랜잭션 외에 다른 데이터의 저장을 고려하게 되었다. 예를 들어 Namecoin(www.namecoin.org)은 블록체인을 통해 탈중앙화된 DNS 서비스를 제공하고 있다. 이처럼 블록체인에는 트랜잭션만 저장할 수 있는 것은 아니다.

불가역성이 필요하거나 데이터가 자동으로 중복 저장될 필요성이 있으면 블록체인에 저장할 수 있다. 특히, 블록체인은 탈중앙 PKI를 실현하는 기술로도 활용되고 있다. 개인정보의 주권을 개인이 직접 통제할 수 있도록 해주는 **DID**(Decentralized ID)도 블록체인을 이용하는 탈중앙 PKI의 한 응용이다.

다른 데이터의 저장 가능성은 프로그램의 저장 가능성으로 발전하였다. 특히, 블록체인에 암호화폐와 디지털 자산이 공존하면 블록체인에 저장된 프로그램을 통해 이들을 공정(fair)하게 교환할 수 있다. 이와 같은 교환을 가능하게 하는 프로그램을 **스마트 계약**(smart contract)이라 한다. 스마트 계약은 프로그래밍 언어로 작성된 계약으로 조건이 충족되면 자동으로 실행된다. 스마트 계약은 기본적으로 두 사용자 간 거래에 사용할 수 있는 기술이다. 프로그램을 블록체인에 저장하고 이를 실행할 수 있다면 할 수 있는 일은 이것으로 제한되지 않고 무궁무진하다. 스마트 계약을 기본 도구로 블록체인을 활용하는 새로운 형태의 탈중앙화된 앱들이 만들어졌으며, 블록체인이 이와 같은 응용을 제공하고 운영하는 플랫폼 역할을 할 수 있게 되었다.

블록체인에 디지털 자산의 저장은 디지털 자산 자체를 블록체인에 저장하는 것이 아니라 그것의 메타 데이터를 저장하는 형태이다. 이와 같은 메타 데이터의 저장은 새로운 개념의 **NFT**(Non-Fungible Token)라는 토큰의 등장을 가져왔다. NFT는 블록체인을 통해 디지털 자산의 소유권을 발행하고, 소유권 변동 내역 관리할 수 있게 해준다.

스마트 계약을 이용한 쌍방간 거래를 확장하면 인터넷 쇼핑몰과 같은 마켓의 구현도 가능해진다. 즉, 다중 판매자와 다중 구매자가 있는 마켓의 구현이 가능할 수 있다. 그러나 마켓의 구현을 위해서는 순서가 중요할 수 있다. 하지만 비트코인의 경우 블록체인에 저장되는 데이터의 순서에 대한 보장은 해주지 않는다.

비트코인의 모든 거래 내역은 누구나 볼 수 있으며, 누구나 참여할 수 있고, 누구나 채굴자 역할을 할 수 있다. 하지만 기업의 내부적으로 사용하는 응용에서 블록체인이 필요할 경우 비트코인처럼 공개형 블록체인을 사용할 필요는 없다. 이에 폐쇄형 블록체인들도 개발되어 사용되고 있으며, 이를 다른 말로 하이퍼레저(hyperledger)라 한다.

비트코인에서 사용한 블록체인은 기록된 데이터를 블록 단위로 확정한다. 블록 단위로 확정하지 않고 개별 데이터 단위로 연결하고 확장하는 방법도 제안되었다. 이렇게 개별 데이터를 연결하면 주기가 없는 방향 그래프(**DAG**, Directed Acyclic Graph)를 형성하게 된다. 모든 거래를 하나의 방향 그래프로 나타낼 수 있고, 각 계정별로 분리하여 유지할 수 있다.

비트코인에서 사용한 블록체인은 비용이 고가인 작업증명을 사용하고 있다. 따라서 작업 증명 대신에 비용이 저렴하면서 분산 합의와 불가역성을 제공할 수 있는 기술에 대한 연구가 활발하게 이루어지고 있다. 비트코인의 또 다른 문제는 확장성과 처리 속도이다. 이와 같은 문제를 극복하기 위한 다양한 기술도 비트코인 이후 계속 연구되고 제안되고 있다. 또 비트코인은 공개 원장을 사용하기 때문에 일부 정보의 노출은 불가피하다. 따라서 다양한 기술을 사용하여 거래의 익명성을 높이고자 하는 시도도 있다.

2. 이더리움

비탈릭 부타린(Vitalik Buterin)은 블록체인에 프로그래밍 코드를 기록하고 이것을 각 컴퓨터에서 실행할 수 있도록 하여 **디앱**(DApp, Decentralized Application)이라고 하는 탈중앙화 앱을 만들고 서비스하는 플랫폼을 생각해냈다[1]. 부타린은 이 아이디어를 비트코인 자체에 실현하고자 하였지만, 이 실현이 어렵다는 것을 인식하고 여러 개발자와 함께 2015년 **이더리움**(ethereum)이라는 새로운 암호화폐를 개발하여 공개하였다. 많은 사람은 이더리움의 이 생각을 블록체인 2.0이라고 하였다. 이더리움은 이더(Ether, ETH)라는 단위의 암호화폐를 사용하며, 비트코인과 달리 이더는 사용자가 디앱을 사용할 때 서비스 대금을 지불하는 목적으로만 사용된다. 이 때문에 최초

<표 16.1> UTXO 기반 지불과 계정 기반 지불 비교

UTXO 기반	계정 기반
• 모든 입력은 유효해야 하며, 아직 지불에 사용하지 않은 기존 트랜잭션의 출력이어야 함 • 모든 입력 소유자의 유효한 서명이 있어야 함 • 입력의 총액이 출력의 총액보다 커야 함	• 트랜잭션의 전송 계정이 충분한 금액이 있으면 유효한 지불이 됨

상장 과장에서 7,200만 개의 ETH가 배포되었고, 15초마다 암호퍼즐을 해결할 수 있도록 고안된 작업 증명 방식을 이용하여 블록이 생성될 때마다 5ETH가 새롭게 발급된다. 이 발급은 비트코인과 달리 중단되지 않으며 블록마다 발급되는 코인의 수도 바뀌지 않는다. 이것은 일반 유통을 목적으로 하지 않았기 때문이다. 물론 이더도 비트코인과 같이 현재 암호화폐 거래소에서 명목화폐로 환전이 가능하다[1]. 이더의 가치는 이더리움 블록체인을 사용하는 디앱이 많아지고 대중화되면 상승할 것으로 예측되고 있다. 이더리움은 처음에는 작업 증명을 사용하였지만 현재는 이더리움 2.0으로 전환하고 있으며, 이더리움 2.0에서는 Casper라는 지분 증명 방식을 사용할 예정이다.

이더리움의 가장 획기적인 것은 튜링 완전한(turing complete) Solidity와 같은 객체지향 프로그래밍 언어를 이용하여 이더리움 블록체인을 사용하는 다양한 디앱을 개발할 수 있다는 것이다. 프로그램 소스가 블록체인에 등록되면 소스에 악의적인 코드를 추가하는 것이 가능하지 않기 때문에 이더리움을 이용한 디앱의 신뢰성은 매우 높다고 할 수 있다. 이더리움 블록체인에 등록된 코드는 각 참여자의 컴퓨터에서 실행될 수 있다. 이때 자바와 유사한 개념인 EVM(Ethereum Virtual Machine)을 사용하며, EVM이 설치된 모든 환경에서 실행할 수 있다.

이더리움 이전에는 새로운 암호화폐를 만들거나 암호화폐를 이용하는 응용을 만들고자 하면 자체적으로 새로운 블록체인을 만들어야 했다. 하지만 작업 증명 방식을 사용하고자 하면 건전한 채굴 생태계가 형성될 때까지 많은 시간이 걸릴 수 있으며, 끝내 건전한 채굴 생태계가 형성되지 않을 수 있다. 하지만 이제 사람들은 이더리움을 이용하여 블록체인을 사용하는 서비스를 쉽게 개발하고 운영할 수 있다.

2.1 UTXO 기반 vs. 계정 기반

이더리움은 비트코인과 달리 **계정 기반**을 사용한다. 비트코인에서 특정 주소의 자산은 그 주소가 대상인 사용하지 않은 트랜잭션 출력의 총합이다. 예를 들어 지갑의 주소가 A일 때, 이 지갑이 보유한 총액은 트랜잭션의 출력 중 대상이 A인 것 중 아직 사용하지 않은 금액의 총합이 된다. 반면에 계정 기반은 각 계정이 보유한 금액을 별도로 유지한다. 계정 기반은 우리가 현재 사용하고 있는 금융 모델과 같아서 UTXO 기반보다 더 직관적이다. 두 방식의 차이점은 표 16.1과 같다.

이 특성 때문에 UTXO 기반은 다음과 같은 장점이 있다.

- 높은 수준의 프라이버시를 제공할 수 있다. 특히, 한 사용자는 거래마다 다른 주소를 사용하여 프라이버시의 수준을 높일 수 있다.
- 한 사용자의 여러 거래를 독립적으로 처리할 수 있다. 즉, 개별 거래는 독립적으로 검증할 수 있다.

반면에 계정 기반은 다음과 같은 장점이 있다.

[1] 2019년 5월, 2020년 5월, 2021년 5월, 2022년 5월, 2023년 5월 기준으로 1ETH는 국내 거래소에서 205,100원, 244,700원, 4,627,000원, 3,502,000원, 2,424,000원에 거래되었다.

- 거래는 하나의 입력과 하나의 출력으로 구성되기 때문에 단순하다.
- 잔액만 유지하면 되기 때문에 유지해야 하는 정보의 양도 적다.
- 계정이 존재하기 때문에 프로그래밍하기 용이하다.

하지만 계정 기반은 계정이 유효한 상태를 유지해야 하므로 한 계정의 여러 거래를 병행으로 처리할 수 없다. 이 때문에 이더리움은 거래에 카운터를 포함하여 거래가 순차적으로 진행되도록 하고 있다. 이더리움도 한 사용자가 여러 계정을 유지할 수 있지만 보통 같은 계정을 계속 사용하도록 유도하기 때문에 프라이버시 측면에서는 UTXO 기반이 더 우수하다는 것이 일반적인 견해이다.

2.2 트랜잭션 처리 비용

비트코인에서 수수료는 입력과 출력의 차이에 의해 결정된다. 이더리움은 계정기반이기 때문에 이 방식을 사용하기 어렵다. 이 때문에 이더리움에서는 가스 비용이라는 개념을 사용한다. 이것은 우리가 자동차를 사용하기 위해 주유하는 개념과 유사하다. 주유하는 양이 같더라도 당일 시세에 따라 사용하는 주유소에 따라 주유액은 달라질 수 있다. 차를 운행하면 주유비가 소요되는 것처럼 트랜잭션을 처리하고 싶은 사용자는 처리 비용을 지불해야 한다. 특히, 이더리움에서 트랜잭션의 처리는 프로그램의 실행 비용이며, 실행해야 하는 프로그램의 크기와 복잡성은 일정하지 않으므로 그 차이에 따라 비용도 달라져야 한다. 이더리움에서 이 비용은 가스로 표현된다. 사용자는 가스 상한(gas limit)과 가스 비(gas price)를 제시한다. 가스 상한과 가스 비를 이용하여 수수료를 계산하는 것은 ETH의 가격이 변하더라도 수수료는 일정 수준으로 유지할 수 있는 이점이 있다. 가스 비용은 Gwei(0.1^9 ETH)라는 단위를 이용하여 제시한다.

이더리움은 3 종류의 트랜잭션을 사용한다. 이 중 가장 단순한 트랜잭션이 일반 거래 트랜잭션으로 한 계정에서 다른 계정으로 ETH를 이체하는 트랜잭션이다. 나머지 2 종류는 스마트 계약과 관련되어 있다. 하나는 스마트 계약을 등록하는 트랜잭션이고, 다른 하나는 등록되어 있는 스마트 계약을 실행하는 트랜잭션이다. 이더리움에서 트랜잭션은 코드이며, EVM에서 실행된다. 코드의 기본 연산(사칙연산, 대입 등)에 대한 비용은 정해져 있다. 이를 바탕으로 EVM에서 특정 코드가 실행되었을 때 필요한 가스를 계산할 수 있다. 소요된 가스가 가스 상한을 초과하면 실행은 취소되기 때문에 충분한 가스 상한을 제시해야 한다. 더욱이 실행이 취소되어도 수수료는 여전히 지급된다. 사용자는 자신의 트랜잭션을 구성하는 코드를 보면 어느 정도 가스가 필요할지는 예측할 수 있다. 이 예측을 바탕으로 트랜잭션을 제출할 때 가스 상한을 제시해야 한다. 실제 지불하는 수수료는 트랜잭션이 실행되었을 때 소요된 실제 가스에 제시한 가스 비를 곱한 금액이 된다.

이더리움에서 트랜잭션의 실행은 채굴자가 담당한다. 다음 블록의 채굴은 크게 트랜잭션을 선별하고 실행하는 단계와 작업 증명 단계로 나누어진다. 채굴자는 먼저 내부 풀에 유지된 아직 블록에 포함되지 못한 트랜잭션 목록에서 블록에 포함할 트랜잭션을 선별한다. 선별하는 기준은 각 채굴자가 자율적으로 결정할 수 있다. 블록에 포함된 트랜잭션의 수수료는 채굴자의 몫이므로 더 많은 이윤을 확보하기 위해 높은 가스 비를 제시한 트랜잭션을 선호한다. 더 많은 트랜잭션을 블록에 포함하는 것이 수수료 총액 측면에서 유리하므로 가스 상한이 작으면서 가스 비가 높은 것을 보통 선호한다. 하지만 트랜잭션 수수료는 실제 소요된 가스에 의해 결정되므로 제시된 가스 비만을 이용하여 수수료를 결정하기 어렵다. 또 복잡한 알고리즘을 통해 선별하는 것보다 작업증명을 빨리 시작하는 것이 유리할 수 있으므로 보통은 단순한 전략을 사용할 것이다. 일반적인 전략은 가스비 기준으로 정렬하여 차례대로 실행하면서 블록의 가스 상한과 소요된 시간을 고려하여 결정하게 된다. 트랜잭션을 실제 실행하기 전에 트랜잭션의 유효성(트랜잭션 서명값, 수수료를 지급할 충분한 금액을 계정이 보유하고 있는지 여부 등)부터 검사해야 한다. 비트코인은 전송 속도를 고려하여 블록 크기를 제한하고 있지만 이더리움은 블록 크기를 이용하여 제한하지 않고 한 블록에 포함할 수 있는 총 가스만 제한하고 있다.

2.3 이더리움 작업증명

이더리움 1.0은 비트코인과 마찬가지로 작업 증명을 이용하여 분산 합의를 하고 있다. 하지만 비트코인과 달리 ASIC을 이용한 채굴이 경제성을 가질 수 없도록 많은 메모리를 요구하는 Ethash라는 알고리즘을 사용하고 있다. 따라서 이더리움에서 대부분의 채굴은 GPU를 이용하고 있다. 또 다른 점은 유효한 블록이지만 긴 체인 우선 원칙에 따라 거부된 블록에 대해서도 보상을 한다. 이더리움에서는 이와 같은 블록을 삼촌 블록(uncle/ommer block)이라 한다. 삼촌 블록은 현재 블록을 기준으로 그것의 부모 노드의 형제 블록을 말한다. 이러리움은 블록 생성 주기가 짧아서 더 빈번하게 일시적 포크가 발생할 수 있다. 이 때문에 이더리움은 삼촌 블록에 대해서도 원래보다는 적은 금액이지만 보상하여 채굴 동인을 높이고 있다. 그뿐만 아니라 채굴이 중앙 집중화되는 것을 완화할 수 있으며, 현재 채굴 생태계의 상태를 보여주는 지표로 활용하고 있다.

이더리움과 비트코인의 또 다른 점은 비트코인은 기본적인 merkle 트리를 이용하지만 이더리움은 merkle-patricia 트리를 사용한다. merkle-patricia 트리는 merkle 트리와 접두사(prefix) 트리를 결합한 트리이며, 이전 블록에서 다음 블록을 생성할 때 트리를 모두 새롭게 구성하지 않고 변경되지 않는 부분은 그대로 사용한다. 계정 기반이기 때문에 이와 같은 특징이 필요한 것으로 보인다.

2.4 스마트 계약

이더리움에서는 프로그래밍 언어로 작성되는 **스마트 계약**(smart contract)이라는 것을 블록체인에 등록할 수 있다. 스마트 계약은 1996년에 Nick Szabo가 처음 소개한 개념이며[2], 이더리움에서 스마트 계약은 중재자 없이 가치가 있는 것을 교환할 수 있도록 해주는 컴퓨터 코드이다. Solidity를 이용한 스마트 계약의 작성은 일반 객체지향 프로그래밍 언어에서 클래스를 정의하는 것과 유사하다. 이 계약은 이전 계약과 달리 법률가가 작성하는 것이 아니라 프로그래머가 작성하는 것이며, 프로그래밍 언어로 작성하기 때문에 계약 내용이 모호하지 않다는 장점이 있다. 스마트 계약은 조건이 충족되면 자동 실행되기 때문에 계약이 불이행되거나 손해를 볼 수 있다는 것을 걱정하지 않아도 된다. 예를 들어 디지털 상품을 거래하는 경우 에스크로 방식으로 필요한 이더만큼을 계약에 예치한 후 조건이 충족되면 해당 이더가 판매자에게 전달되고 디지털 상품은 지불자에게 전달되는 방식이다. 하지만 위험요소가 전혀 없는 것은 아니다. 프로그램 코드이므로 충분히 확인되지 않은 상태에서 등록되면 심각한 결과를 초래할 수 있고 등록된 이후에는 논쟁할 수 없다. 또 관련 법률이 정비된 것은 아니므로 문제가 발생하였을 때 법적인 보호를 받을 수는 없다.

스마트 계약의 장점은 다음과 같다고 주장되고 있다.

- 자율성(autonomy): 중재자 없이 자동 실행된다. 계약을 강제화하기 위한 다른 추가적인 장치가 필요없다.
- 신뢰(trust): 계약이 투명하고 자동적으로 실행되며 안전하기 때문에 믿을 수 있다.
- 백업(backup): 자동으로 중복 저장되어 있다.
- 안전성(safety): 계약의 조작 가능성이 계산적으로 어렵다.
- 신속성(spped): 소프트웨어를 통해 자동 실행된다.
- 경제성(savings): 중재자가 필요 없어 경제적이다.
- 정확성(accurracy): 소프트웨어로 처리되기 때문에 사람 실수에 의한 오류는 발생하지 않는다.

이더리움에는 두 종류의 계정이 있다. 비트코인 지갑처럼 특정 사용자의 이더 잔액을 유지하는 **사용자 계정**(EOA, Externally Owned Account)과 스마트 계약을 유지하는 **계약 계정**(CA, Contract Account)이 있다. 계약 계정도 사용자 계정과 마찬가지로 이더 잔액을 유지할 수 있다. 사용자 계정은 계약 계정과 달리 연결된 코드가 없다.

사용자는 사용자 계정을 이용하여 다른 사용자 계정과 이더를 거래할 수 있고, 계약 계정을 대상으로 트랜잭션을 생성하여 계약 계정에 유지된 스마트 계약을 실행할 수 있다. 계약 계정의 코드는 사용자 계정이 생성한 트랜잭션에 의해 활성화되거나 다른 계약 계정으로부터 메시지를 받으면 활성화될 수 있다. 즉, 계약 계정은 스스로 활성화될 수 없다. 이더리움에서 모든 행위는 코드의 수행이며, 코드의 수행은 비용 지불이 필요하다. 따라서 스마트 계약의 실행을 위해서도 비용 지불이 필요하다.

2.5 디앱

디앱은 탈중앙화된 P2P 네트워크에서 백앤드가 구동되며, 누구의 개입 없이 서비스 제공자와 고객 간에 직접적인 상호작용을 할 수 있는 자율적으로 동작하는 앱이다. 서비스를 중앙 통제하는 주체가 없다. 페이스북, 트위터와 같은 응용은 해당 회사가 중앙에서 통제하지만 디앱은 디앱이 운영되면 그것을 독자적으로 통제할 수 있는 주체는 없다. 디앱은 기본적으로 오픈소스이기 때문에 신뢰할 수 있고, 블록체인에 유지되기 때문에 수정 및 조작할 수 없다. 블록체인에 등록된 이후에는 수정할 수 없기 때문에 이것이 오히려 단점이 될 수 있다.

디앱은 토큰 형태의 내부 통화를 사용하며, 앱 사용료를 지불해야 한다. 따라서 디앱을 사용하고자 하면 관련 플랫폼 지갑 및 코인을 보유해야 한다. 하지만 기존 지불 시스템과 연계 없이 자연스럽게 토큰의 유통이 가능하다. 더욱이 사용자에게 자동으로 토큰 형태의 인센티브를 지급하여 참여를 유도할 수 있다, 디앱은 블록 체인을 활용하며 P2P 네트워크에서 동작하므로 단일 실패점이 없어 가용성이 우수하다.

디앱과 기존 모바일 또는 웹 서비스와 비교하면 프론트 앤드는 동일하지만, 기존 서비스의 백 앤드는 보통 단일 서버(centralized)에서 구동되는 웹 기반 서버 프로그램으로 구성되는 반면에 디앱의 백 앤드는 P2P 네트워크의 블록체인에서 구동되는 여러 개의 스마트 계약으로 구성된다. 즉, 이더리움 기반 디앱은 여러 개의 스마트 계약을 통해 비지니스 로직을 구현하여야 한다. 디앱에서 백 앤드와 프론트 앤드 간의 데이터 교환은 보통 IPFS(InterPlanetary File System)을 통해 이루어진다. IPFS는 P2P 방식의 차세대 파일 시스템이며, 블록체인과 결합되어 널리 활용될 것으로 예측되고 있다.

2.6 토큰과 ICO

비트코인과 같은 암호화폐의 등장으로 P2P 방식의 금전 교환이 가능하고 스마트 계약과 같은 기법에 의해 자동 지불이 가능해지면서 서비스 모델의 큰 변화가 오고 있다. 서비스를 이용하는 고객에게 유료 서비스를 제공할 수 있을 뿐만 아니라 거꾸로 고객에게 서비스에 필요한 무언가를 하도록 보상을 쉽게 지급할 수 있게 되었다. 이를 위해 이더리움에서는 이더리움 토큰을 쉽게 만들어 이더리움 플랫폼 위에서 동작하는 디앱에서 사용할 수 있도록 하였다. 현재 이더리움 플랫폼 위에 동작하는 새로운 디앱을 만들거나 만들 기획을 발표하고 이 앱에서 사용될 토큰을 상장하여 개발에 필요한 자금을 조달할 수 있으며, 이를 ICO(Initial Coin Offering)라 한다. 이 토큰은 해당 앱에서만 사용할 수 있지만 이더리움의 특징 때문에 이 토큰을 이더로 교환할 수 있으며, 이더는 다시 명목화폐로 환전할 수 있다.

3. 이더리움 2.0

현재 이더리움은 점진적으로 이더리움 2.0으로 전환되고 있다. 가장 최근 이더리움의 하드 포크는 2023년 4월 12일에 실행된 “Shanghai”이다. 이더리움 2.0의 가장 큰 변화는 샤딩의 도입과 PoS로의 전환이다. 샤딩의 도입으로 전체 블록체인은 64개의 샤드로 분할이 되며, 이 샤드들을 관리하고, PoS에 필요한 검증자 관리를 위해 비콘 체인이라는 것을 도입하였다.

비콘 체인은 시간 개념으로 동작하며, 그 단위가 epoch와 슬롯(slot)이다. 이 때문에 비콘 체인을 이더리움의

심박(heartbeat)이라 한다. 한 epoch는 32개의 슬롯으로 구성되며, 12초마다 한 슬롯이 만들어진다. 한 슬롯에는 하나의 비콘 블록이 만들어지며, 이 비콘 블록은 64개의 샤드 블록과 연결된다.

비콘 체인의 역할은 다음과 같다.

- 병렬로 운영되는 샤드 체인을 연결하는 역할
- 활성 검증자 집합 관리
- 제안자 선정에 사용하는 의사난수 프로세스 RANDAO 제공
- 비콘 블록 확정 및 샤드 교차(cross shard) 트랜잭션 처리

현재 누구나 32ETH를 예치하면 활성 검증자로 참여할 수 있다. 비콘 체인은 현재 활성 검증자 목록을 유지 및 관리한다. 각 샤드마다 PoS를 위해 128명 이상의 검증자로 구성된 검증 위원회가 만들어지며, 각 슬롯마다 이 중 한 명이 제안자(proposer)로 선정된다, 제안자는 블록을 제안할 때 원하는 금액의 ETH를 예치할 수 있으며, 예치액에 따라 블록에 포함할 수 있는 트랜잭션 수가 달라진다. 더 많은 트랜잭션을 포함할 수 있으면 그만큼 더 많은 수수료를 보상으로 받을 수 있다. 검증자가 유효하지 않은 트랜잭션 등 부정 행위가 발견되면 예치 금액을 잃게 된다. 검증 위원회 중 제안자로 선정되지 않은 남은 검증자들은 입회자(attester)가 되며, 이들은 제안자가 제안한 블록에 대해 up/down 투표를 진행한다. 2/3 이상의 up 투표를 받아야 블록이 확정되어 비콘 체인에 포함될 수 있다.

4. 알트코인

비트코인 이후 등장한 알트코인의 수는 1,000개가 넘고 있다. 이 중 중요 알트코인을 살펴보면 다음과 같다.

- Ripple: 글로벌 송금을 목적으로 하고 있으며, 단위는 XRP이다. Ripple은 변형된 비자틴 합의 프로토콜을 사용한다.
- Namecoin: 분산형 DNS 등록과 같은 서비스를 제공하기 위해 고안된 암호화폐이다. 거래 정보 외에 다른 정보를 블록체인에 저장하여 서비스하는 최초의 시도이었다.
- 피어코인(Peercoin): 최초로 지분 증명을 사용한 암호화폐이다. 피어코인에 사용된 지분 증명 방식은 6.1 절에 설명한다.
- 이더리움 클래식: 오리지널 이더리움을 말한다. 이더리움을 개발한 부탈린은 2016년에 이더리움에 발생한 DAO 공격에 따른 피해를 처리하기 위해 특정 위치부터 다시 채굴하기로 하였지만 이것에 동의하지 못한 일부는 공격에 흔적이 남아 있는 상태로 계속 채굴을 이어갔다. 이것이 이더리움 클래식이며, ETH 대신에 ETC 단위를 사용한다.
- IOTA: 사물 인터넷 응용에 적합한 암호화폐를 만들기 위해 개발된 암호화폐이다. 탱글(tangle)이라는 새로운 형태의 분산 합의 메커니즘을 사용한다. 탱글은 블록 단위로 작업 증명을 하지 않는다. IOTA에서 트랜잭션이 확정되기 위해서는 다른 트랜잭션들의 승인이 필요하며, 이를 위해 각 트랜잭션을 생성할 때 무조건 다른 두 개의 트랜잭션을 승인하도록 하고 있다.
- EOS: 이더리움과 같은 디앱 개발을 위한 플랫폼 제공이 목적인 암호화폐이다. EOS의 목표는 블록체인 기술을 이용하여 다앱을 개발하고 운영할 수 있는 분산 운영체제를 제공하는 것이다. EOS는 지분 증명을 사용하며, 1초에 100만개의 트랜잭션을 처리할 수 있다고 주장되고 있다. 주장에 의하면 작업 증명을 사용하고 있는 이더리움에 비해 훨씬 확장성 있으며, 유연하고, 디앱 인터페이스 개발을 위한 웹 툴킷과 같은 다양한 개발 리소스를 제공하고 있다. 이 때문에 이 암호화폐를 블록체인 3.0이라고도 한다.

- ENJIN: 게임에서 사용할 목적으로 개발된 암호화폐이다.
- Zcash: zk-SNARK라는 영지식 증명 기술을 이용하여 프라이버시를 개선한 암호화폐이다.
- Monero: 링 서명 기술을 이용하여 프라이버시를 개선한 암호화폐이다.
- Algorand: 순수 지분 증명을 사용하는 암호화폐이다.
- Hedera: 트랜잭션의 순서에 대한 분산 합의 기능을 가진 암호화폐이다.
- 기타: Litecoin, Dogecoin, Dash, Stella, Cardano, Tron, FileCoin 등

5. DAG 기반 분산 원장

5.1 IOTA

IoT를 위해 설계된 암호화폐 IOTA는 탱글이라고 하는 DAG 기반 분산 원장을 사용한다[3]. 탱글은 비트코인처럼 작업 증명을 통해 경쟁하여 검증자를 선정하는 방식이 아니며, 지분 증명처럼 검증자를 어떤 기준을 이용하여 선정하지도 않는다. 또한, 트랜잭션을 모아 블록 단위로 확정하는 형태도 아니다. 트랜잭션을 생성하는 모든 사용자가 검증자 역할까지 해야 한다. 트랜잭션을 생성한 사용자는 기존 2개의 트랜잭션을 검증하고 자신의 트랜잭션과 연결해야 한다. 탱글이 의도한 대로 동작하기 위한 최소 개수가 2개이기 때문에 2개를 사용하고 있다. 따라서 트랜잭션들이 주기가 없는 방향 그래프를 형성하게 된다. 이와 같은 방식을 사용하기 때문에 트랜잭션 수수료가 없으며, 모든 화폐는 최초 트랜잭션에서 전부 발행하여 사용하고 있다.

새 트랜잭션은 2개의 다른 트랜잭션을 검증하기 때문에 이 과정이 반복되면 한 트랜잭션은 여러 트랜잭션에 의해 직간접적으로 승인이 되는 형태가 된다. 직간접적으로 많은 트랜잭션에 의해 승인된 트랜잭션은 수정할 수 없게 되어 기존 블록체인과 마찬가지로 첨삭 전용이 된다. 2개의 다른 트랜잭션을 승인하여 형성되는 DAG가 이상적인 모습이 되기 위해서는 새 트랜잭션은 아직 승인되지 않은 트랜잭션을 선택하여 승인해야 한다. 탱글에서 다른 트랜잭션에 의해 승인되지 않은 트랜잭션을 tip 트랜잭션이라 한다. 즉, 새 트랜잭션은 2개의 tip 트랜잭션을 선택하여 승인해야 한다. 여기에는 2가지 문제가 있다. 하나는 tip 트랜잭션을 효과적으로 찾는 것이고, 다른 하나는 효과적으로 찾는 알고리즘이 있을 때 이를 사용하도록 유도하는 것이다.

tip 트랜잭션을 찾는 방법은 간단하다. 최초 트랜잭션(genesis transaction)부터 그것을 승인한 트랜잭션을 따라 tip을 만날 때까지 그래프를 탐색하면 된다. 꼭 최초 트랜잭션부터 탐색할 필요는 없다. 중간 임의의 트랜잭션부터 탐색을 하여도 최종적으로는 tip에 도달하게 된다. 그래프를 탐색할 때 트랜잭션을 승인한 트랜잭션이 여러 개이면 이 중 하나를 선택하여 탐색을 진행해야 한다. 이때 탱글은 축적 무게가 큰 노드가 더 높은 확률로 선택되는 알고리즘을 사용한다. 트랜잭션의 축적 무게란 자신의 무게에 그것을 직간접적으로 승인한 트랜잭션의 무게를 합한 값이다. 새 트랜잭션이 추가되면 자신의 무게를 전달하여 자신이 승인한 트랜잭션의 축적 무게를 갱신한다. 각 트랜잭션의 무게는 트랜잭션을 생성할 때 사용한 PoW에 의해 결정된다. 탱글은 트랜잭션을 서명할 때 낮은 수준의 작업 증명을 활용한다. 권장하는 방법을 사용하여 tip 트랜잭션을 선택하지 않고 마음대로 선택하면 해당 트랜잭션은 다른 트랜잭션에 의해 승인될 가능성이 작기 때문에 대부분의 사용자는 제시된 방법을 이용하여 tip 트랜잭션을 선택하게 된다.

5.2 Nano

Nano는 원래 RaiBlock이라는 이름으로 시작한 암호화폐이다[4]. 기존 암호화폐와 달리 Nano에는 수수료가 없고 특별한 보상 체계도 없다. Nano는 IOTA처럼 개별 트랜잭션을 DAG로 연결하여 유지한다. 하지만 IOTA와 달리

한 트랜잭션이 세부적으로 입금과 출금 트랜잭션으로 나누어지며, 각 계정별 별도 DAG를 유지한다. 사용자 A가 사용자 B에게 일정 코인을 양도하고자 하면 계정 A의 DAG에 출금 트랜잭션이 추가되고, 계정 B의 DAG에 입금 트랜잭션이 추가된다. 이를 통해 계정별 DAG들이 서로 연결되어 격자 형태의 큰 DAG를 형성하게 된다. 이와 같이 동작하기 때문에 특정 트랜잭션과 관련이 없는 다른 계정의 DAG는 해당 트랜잭션의 실행에 전혀 영향을 받지 않는다. 즉, 계정 별 독립 DAG이므로 트랜잭션에 의해 영향을 받는 계정은 항상 2개이며, 다른 계정과 독립적으로 거래를 진행할 수 있다.

각 계정의 DAG는 계정의 소유주만 갱신할 수 있으며, 포크의 발생은 프로그래밍 오류 또는 계정 소유자의 부정 행위에 의해서만 일어날 수 있다. 한 계정은 다른 한 계정을 대리인으로 지정할 수 있고, 본인이 온라인 상태가 아닐 때 투표를 대신해주는 역할을 한다. 하지만 앞서 언급한 바와 같이 대리인 수행에 대한 별도 보상은 없다.

트랜잭션이 출금과 입금 트랜잭션으로 나누어져 있기 때문에 양도 받는 사용자가 입금 트랜잭션을 해당 사용자의 DAG에 추가해 주어야 거래가 완료된다. 따라서 트랜잭션은 크게 완료 상태, 진행 중 상태로 구분된다. 진행 중 상태라는 것은 아직 입금 트랜잭션이 수취인 계정 DAG에 추가가 안 된 상태를 말한다. 각 트랜잭션은 다른 암호화폐처럼 계정 소유자의 개인키로 전자서명되어 DAG에 추가된다. 각 트랜잭션은 또한 간단한 PoW도 해결해야 한다. 이 PoW는 지난 트랜잭션과 난스를 이용하여 계산하므로 트랜잭션을 전송한 후에 바로 다음 트랜잭션을 위한 PoW를 수행할 수 있다. PoW를 사용하는 이유는 스팸 방지용이다. 한 계정이 너무 많은 트랜잭션을 생성하여 네트워크 운영에 악의적인 영향을 주는 것을 막기 위한 것이다.

각 계정 DAG의 트랜잭션은 현재 계정 잔액 정보를 유지하고 있으므로 다른 노드들은 다른 계정의 최종 트랜잭션만 유지할 수 있다. 따라서 다른 블록체인과 달리 오래된 데이터를 버릴 수 있다. 앞서 언급하였듯이 프로그래밍 오류나 계정 소유자의 부정 행위로 개별 계정의 DAG에 포크가 발생할 수 있다. 이 경우 모두가 참여하는 투표가 진행되어 포크를 해소한다. 각 투표자의 투표 가중치는 그 투표자가 대리하는 계정이 많을 수록 높아진다. 계정별로 포크가 발생할 수 있으므로 이와 같은 포크는 다른 계정의 거래 진행에 전혀 영향을 주지 않는다.

6. 분산 합의 프로토콜

비트코인의 블록체인은 비트코인 네트워크에 참여하는 수많은 노드가 유지하고 있으며, 이들은 모두 동일한 데이터를 유지해야 한다. 이를 위해 분산 합의 프로토콜이 필요하며, 비트코인은 앞서 설명한 바와 같이 작업 증명이라는 기법을 사용하여 블록 값들에 대한 분산 합의를 이루어내고 있다. 하지만 작업 증명 방식은 확정 속도가 느리고 에너지 소비가 심각하여 환경에 나쁜 영향을 주는 등 여러 가지 문제점을 가지고 있다. 또한 자본력이 많은 사람과 기관이 유리한 방식이므로 애초 목표인 분산화 대신에 채굴은 중앙 집중화가 되어 가고 있다. 이 때문에 비트코인의 블록체인과 마찬가지로 불가역성 특성을 안전하게 제공하면서 비트코인에서 사용하는 작업 증명 방식의 문제점을 극복할 수 있는 새로운 분산 합의 방식을 찾기 시작하였다. 그것의 결과로 등장한 것 중 하나가 지분 증명과 공간 증명이다.

6.1 지분 증명

지분 증명 방식은 각 라운드마다 해당 화폐에서 정한 규칙에 의해 블록을 생성할 검증자(validator)를 결정한다. 따라서 블록 생성에 대한 보상으로 새 화폐가 발행되지 않는다. 이 때문에 지분 증명에서는 채굴이라는 용어를 사용하지 않고 주조(minting)라는 용어를 사용한다. 하지만 실제 화폐가 발행되지 않기 때문에 주조도 올바른 용어라 보기 힘들다. 지분 증명 방식은 검증자를 결정하는 방식에 따라 체인기반 PoS와 BFT 기반 PoS로 구분한다. 체인기반 PoS에서는 블록마다 단일 검증자를 사용하는 반면 BFT 기반 PoS는 블록마다 다수의 검증자를 사용하며, 이들은 비자틴 합의 프로토콜처럼 서로 메시지를 주고받아 합의에 도달한다. 일반적으로 지분 증명 방식에서 새 블록을 생성할 때 검증자는 블록 해시값을 자신의 개인키를 이용하여 전자서명하여 공개하며, 이 블록에는 작업

증명 방식과 동일하게 이전 블록의 해시값이 포함된다.

PoS 방식은 검증자를 결정하는 방법에 의해 차별화될 수 있다. 보통 확률과 부에 의해 검증자가 결정된다. 여기서 부는 보유한 암호화폐 금액 또는 검증자 역할을 하기 위해 예치한 금액을 말한다. 이와 같은 측면에서 stake(지분, 건 돈)이라는 용어를 사용하는 것이다. 따라서 검증자 결정 방법에 따라 51%의 지분을 가진 자가 작업 증명과 마찬가지로 합의 방식을 공격하고 교란할 수 있다. 하지만 보통 총 발행된 특정 암호화폐의 51%를 소유하는 것은 채굴 컴퓨팅 파워를 51%를 소유하는 것보다 더 어렵기 때문에 작업 증명보다 51% 공격이 더 어렵다고 주장되기도 한다. 또 해당 화폐의 많은 지분을 소유한 자는 해당 암호화폐를 공격하는 것이 자신이 보유한 화폐의 가치를 떨어뜨리는 결과를 초래할 수 있기 때문에 검증자들이 부정 행위를 할 확률이 적다고 주장되기도 한다. 이더리움에서 사용하는 PoS 방식인 캐스퍼(casper) 프로토콜에서는 검증자가 되기 위해서는 일정 금액을 예치하여야 하며, 규칙에 어긋난 행동을 한 것으로 밝혀지면 이 예치금을 잃게 된다. 지분 증명은 경쟁방식이 아니기 때문에 일시적 포크가 발생하지 않아 불필요하게 낭비되는 자원이 없으며, 거래가 확정되기 위해 거래 포함된 블록의 깊이가 일정 깊이 이상이 되어야 할 필요도 없다.

피어코인[2]은 코인의 나이를 이용하여 검증자를 결정하는 방식을 사용하였다. 코인의 나이보다 지갑의 나이라고 하는 것이 더 이해하기 쉽다. 예를 들어 n일 동안 이 지갑에 있는 코인들을 거래에 사용하지 않으면 이 지갑의 나이가 n이 된다. n과 지갑에 유지된 코인의 수가 많으면 많을수록 검증자가 될 확률이 높아진다. 검증자가 되면 새 코인이 이 지갑에 입금되기 때문에 한번 검증자가 되면 최소 30일이 지나야 또 다시 검증자가 될 수 있다.

지분 증명이 실제 블록체인의 변경불가능성을 제공할 수 있나? 우선 검증자는 정직하다고 가정하자. 그러면 검증자가 아닌 제3자가 블록을 수정할 수 있는가? 기본적으로 분산 저장되어 있으며, 검증자의 서명키로 서명되어 저장되어 있기 때문에 해당 검증자의 서명키를 확보하지 않는 이상 수정하는 것은 가능하지 않다. 또 블록체인의 특성 때문에 특정 블록을 수정할 경우 그 이후 모든 블록을 수정해야 한다. 이를 성공적으로 수정하더라도 전체 네트워크가 이를 수용해야 하는 문제도 남아있다. 더욱이 BFT 방식의 경우에는 여러 검증자의 서명키를 확보해야 한다. 해당 블록의 검증자를 임의로 바꿀 수 있다면 블록체인의 수정은 쉽게 이루어질 수 있다. 이 문제는 해당 블록을 검증하는 검증자의 선택 알고리즘에서 사용하는 랜덤 프로세스와 관련되어 있다. 다음 절에서 설명하는 알고랜드는 이 문제를 매우 효과적으로 해결하고 있다. Cardano에서 사용하는 지분 증명은 학술 논문을 통해 그것의 안전성을 증명하고 있다[5].

지분 증명에서 검증자는 어떤 부정 행위를 할 수 있을까? 다른 사람의 코인을 이용한 지불은 생성할 수 없고, 수정할 수 없다. 다른 사람의 거래를 블록에 일부러 포함하지 않을 수 있지만 블록에 포함할 거래의 선택은 검증자의 몫이므로 이것은 부정 행위라 할 수 없다. 검증자는 자신의 코인과 관련된 거래에 대해서만 부정 행위를 시도할 수 있다. 예를 들어 자신의 거래를 자신이 생성한 블록에 포함한 후에 나중에 그 블록에서 해당 거래를 삭제하여 이중 사용을 시도할 수 있다. 하지만 지분 증명도 블록들이 체인으로 연결되어 있기 때문에 과거 블록을 수정하기 위해서는 그 이후 모든 블록을 다시 만들 수 있어야 한다. 따라서 해당 검증자가 홀로 지속해서 블록을 생성하지 않는 이상 이와 같은 공격도 가능하지 않다.

6.2 알고랜드

알고랜드(algorand)는 MIT의 S. Micali 교수가 중심이 되어 제안된 알트코인이다[6]. 알고랜드는 비트코인과 마찬가지로 UTXO 기반이지만 작업 증명을 사용하지 않고 지분 증명을 사용한다. 지분 증명의 핵심은 검증자 선정 방식이다. 하지만 보통 결정적 방식을 사용하거나 정해진 풀에서 선정하는 방식을 사용하였다. 이와 달리 알고랜드는 확률적 방법으로 결정하는데, 이 결정은 조작이 가능하지 않고 예측도 가능하지 않다. 이를 위해 어떤 장려책을 사용하지도 않는다.

알고랜드에서는 라운드마다 리더와 검증자들을 확률적 방법으로 선출한다. 리더는 블록을 생성하고, 검증자들은

[2]피어코인이 PoS를 사용한 최초 알트코인이다. 현재는 이 외에도 ShadowCash, Nxt, Qora 등이 PoS 기반이다.

BFT를 통해 블록을 확정한다. 이 방식에서는 기존과 달리는 일시적 포크도 발생하지 않는다.

알고랜드에서 r번째 블록은 다음과 같이 구성한다.

$$B^r = r, \text{PAY}^r, Q^r, H(B^{r-1})$$

여기서 PAY^r은 이번 라운드에 포함되는 트랜잭션들의 집합이고, Q^r는 리더 선정에 사용되는 요소이다.

알고랜드에서 리더 선출을 위해 각 참여자 i는 $\sigma_i = \text{SIG}_i(r||1||Q^{r-1})$를 계산하고, $H(\sigma_i)$를 계산한다. σ_i는 전자서명 값이므로 오직 i만 계산할 수 있다. 계산된 해시값을 소수점 이하 수로 취급하여 시스템에서 정한 특정 수 p이하이면 자신이 리더가 된다. 각 참여자는 자신이 리더가 될 수 있는지 계산할 수 있지만 다른 참여자들의 값은 계산할 수 없기 때문에 리더를 예측할 수 없다.

리더 자격을 얻지 못한 참여자들은 $\sigma_i' = \text{SIG}_i(r||s||Q^{r-1})$를 계산하고, $H(\sigma_i')$를 계산한다. 이 값이 특정 수 p' 이하이면 자신이 검증자가 된다. 여기서 s는 BFT의 각 단계를 나타내는 번호이다. 즉, BFT의 단계마다 참여하는 선정자들이 다르게 결정된다. 검증자는 자신이 수신한 블록 중 $H(\sigma_i)$가 가장 작고 유효한 블록을 보낸 참여자를 리더로 결정하고 그 블록에 대한 BFT를 수행한다. 이 과정을 통해 정해진 임계값 이상의 검증자가 서명하게 되면 해당 블록은 유효한 블록이 된다.

6.3 공간 증명

공간 증명(proof of space)은 일정한 크기의 디스크 공간을 소모하였음을 증명하는 것이다. 이를 위해 디스크 공간에 랜덤한 데이터를 저장해야 하며, 정기적으로 이 데이터가 계속 해당 공간에 유지되고 있다는 것을 증명해야 한다. 이와 같이 동작하기 때문에 이 공간을 다른 용도로 활용하지 못한다. 공간 증명은 작업 증명과 달리 에너지가 소모되는 것은 아니며, 특수 하드웨어를 통해 더 빠르게 증명할 수 있는 것도 아니다.

공간 증명은 크게 두 단계로 구성된다. 초기 설정 단계에서 증명자는 N개 블록으로 구성된 데이터를 디스크 공간에 저장해야 한다. 초기 설정 단계를 완료한 후에 증명자는 증명 단계를 계속 주기적으로 수행해야 한다. 증명 단계는 저장된 공간에 기대하는 데이터가 있는지 증명하는 단계이다. 간단하게 추상적으로 설명하면 확인자는 증명자가 저장한 N개 블록 중 블록 몇 개를 랜덤하게 선택하여 요청하면 증명자는 이들을 유지하고 있음을 증명하게 된다. 증명하는 방법은 13장에서 살펴본 POR을 생각하면 된다.

증명자, 확인자 입장에서 공간 증명은 모두 효율적이어야 하지만 초기 단계는 저장해야 하는 블록 개수 N에 비례할 수밖에 없다. 그러나 초기 단계는 계속 수행하는 부분은 아니다. 안전성 측면에서 증명자는 N개 블록을 실제 유지하지 않으면 증명을 할 수 없거나 너무 많은 시간이 요구되어야 한다.

간단한 공간 증명 방법을 생각하여 보자. 초기 단계에서 확인자가 실제 랜덤한 블록 데이터를 N개 증명자에게 전달해 줄 수 있다. 하지만 이렇게 하는 것은 비용이 많이 소요될 수 있다. 또 증명자는 데이터를 저장하지 않고 압축하여 저장할 수 있다. 확인자는 랜덤한 데이터를 의사난수 함수를 이용하여 생성하였다면 생성한 전체 데이터를 유지하지 않고 생성할 때 사용한 랜덤 seed만 유지할 수 있다.

이와 같은 문제 때문에 페블(pebble) 그래프와 머클 트리를 이용하는 방법이 제안되었다[7]. 이 방법에서 확인자는 페블 그래프를 만들기 위한 값들을 증명자에게 제공한다. 증명자는 이 값들을 이용하여 주기가 없는 방향 그래프를 만들어야 한다. 만든 그래프 정보를 디스크에 저장하고 확인자가 요청하면 이 그래프를 이용하여 증명값을 만들어 회신한다. 증명자는 그래프 정보를 저장하지 않고 초기 단계에서 확인자가 준 정보만 유지할 수 있지만 초기 정보만 유지하면 증명해야 할 때 그래프를 다시 만들어야 하기 때문에 시간이 너무 많이 소요된다.

공간 증명으로 불가역성이 보장되어야 하는 블록체인을 만드는 방법은 직관적이지는 않다. 지금까지 설명한 것을 보면 공간 증명은 증명자와 확인자 간의 프로토콜 형태로 진행된다. 이것을 비상호작용 증명으로 바꾸어야

한다. 그다음 이 증명을 전자서명처럼 사용할 수 있어야 한다. 채굴자들은 이전 블록의 공간 증명값, 트랜잭션의 머클 루트 값을 바탕으로 공간 증명을 수행한다. 시간이 많이 소요되는 것이 아니기 때문에 모두 성공적으로 증명을 수행할 것이다. 따라서 이들 중 승자를 결정하는 규칙이 있어야 한다. 이 규칙은 알고랜드에서 검증자를 선정하는 규칙과 유사하다고 생각하면 된다. 현재 spacecoin(`spacecoin.network`), chia(`chia.net`), filecoin(`filecoin.io`) 등 실제 공간 증명을 활용하는 암호화폐들이 여러 개 있다.

6.4 헤더라

헤더라(Hedera)는 지금까지 블록체인들과 달리 트랜잭션 순서에 대한 합의를 할 수 있도록 해준다[8]. 트랜잭션을 전달할 때 내가 최신에 받은 트랜잭션, 내가 최신에 보낸 트랜잭션을 연결하여 전송하면 모든 참여자가 동일한 해시 그래프를 그릴 수 있고, 이 그래프를 통해 순서에 대한 합의가 가능하다. 실제 순서는 모든 사용자가 수신한 시간의 평균값이 된다.

7. 블록체인과 암호화폐 기술의 미래

7.1 폐쇄형과 공개형 블록체인

블록체인이 많은 응용에서 활용됨에 따라 다양한 종류의 블록체인이 등장하고 있으며, 블록체인의 핵심 기술인 합의 프로토콜도 다양해지고 있다. 블록체인은 다음과 같은 기준에 따라 크게 폐쇄형(private, permissioned)과 공개형(public, permissionless) 블록체인으로 구분된다.

- 기준 1. 블록체인의 분산 합의 참여에 대한 개방 여부
- 기준 2. 해당 블록체인을 사용하는 서비스 참여에 대한 개방 여부
- 기준 3. 블록체인에 기록된 데이터 접근에 대한 개방 여부

보통 암호화폐들은 누구나 사용할 수 있도록 개방되는 것이 당연하기 때문에 공개형 블록체인을 사용하게 된다. 예를 들어 비트코인은 위 3가지 기준을 고려하였을 때 모두 개방되어 있으므로 전형적인 공개형 블록체인이라고 할 수 있다. 물론 비트코인의 모든 참여자가 채굴하지는 않지만 누구든지 원하면 채굴에 참여할 수 있다.

어떤 기업에서 내부 목적으로 블록체인을 운영할 경우에는 이들은 폐쇄형 형태로 운영하게 된다. 이와 같은 블록체인은 해당 기업 관계자들만 사용할 수 있으며, 이들만 블록체인에 기록된 데이터를 볼 수 있다. 특히, 이와 같은 블록체인의 경우에는 몇 개의 자체 서버를 두어 작업 증명을 하도록 하거나 단순하게 블록들을 전자서명만 하여 블록체인을 구축한다.

보통 공개형은 아무나 쓰고 읽을 수 있기 때문에 다른 말로 무허가 방식(permisionless)의 블록체인이라 하고 폐쇄형은 권한을 받은 소수만 읽고 쓸 수 있어서 허가 방식(permissioned)이라 한다. 최근에 공개형, 폐쇄형, 컨소시엄 블록체인으로 블록체인을 분류하기도 한다. 컨소시엄 블록체인은 미리 약속된 몇 개의 노드들만 분산 합의에 참여하며, 블록체인의 내용은 공개될 수 있다. 이처럼 분류하는 이유는 폐쇄형은 중앙집중 방식에 가까운 형태이지만 컨소시엄은 공개형과 폐쇄형의 특성이 혼합된 형태이기 때문이다.

7.1.1 하이퍼레저

폐쇄형 블록체인 기술을 발전시키기 위해 많은 기업이 Linux Foundation과 손잡고 블록체인 관련 다양한 프로젝트를 진행하고 있으며, 이 프로젝트들을 통틀어 하이퍼레저(hyperledger)라 한다. 현재 Fabric, Iroha, Sawtooth,

Burrow, Indy 다섯 개의 하이퍼레저 프레임워크와 Composer, Explorer, Cello라는 하이퍼레저 모듈이 연구 및 개발되고 있다. 이들 하이퍼레저들은 PoW를 사용하지 않고 복권 기반(lottery-based), 투표 기반(voting-based) 등 다양한 분산 합의 프로토콜을 개발하여 사용하고 있다.

7.2 블록체인 처리 속도 향상 기술

7.2.1 샤딩

샤딩(sharding)은 원래 데이터베이스를 분할하여 여러 서버에서 서비스를 제공하는 기술이다. 보통 게임 산업에서 부하 분산을 위해 많이 사용하였다. 블록체인에서는 하나의 블록체인에 모든 트랜잭션을 유지하지 않고 일정한 기준으로 나누어 병행 처리하는 기술을 샤딩이라 한다. 이때 나누어진 블록체인을 샤드(shard)라 한다. 샤딩을 할 경우 노드에 샤드를 할당하는 문제, 다른 샤드 간 거래 문제, 작업 증명 방식을 사용할 경우 해시 파워의 분산으로 개별 샤드가 공격에 취약할 수 있는 문제 등의 해결이 필요하다. 지분 증명의 경우에는 개별 샤드가 취약해지는 문제를 극복하기 위해 샤드 검증자를 랜덤하게 섞는 방법을 사용하고 있다.

7.2.2 롤업

롤업(rollup)은 각 개별 트랜잭션을 확인하지 않고 묶어서 확인하는 기술이다. 14장에서 살펴본 일괄 확인 기술을 통해 유효한 트랜잭션의 서명을 묶어 하나의 증명만 확인하여 모든 트랜잭션을 검증할 수 있도록 하는 방법이다. 여기에 영지식 증명 기술을 사용하면 ZK 롤업이라 한다. ZK 롤업 외에 낙관적 롤업 기법도 있는데, 이 기법은 검사를 하지 않고 진행하지만 부정행위가 발견되면 많은 페널티를 주도록 고안하여 유효하지 않은 트랜잭션이 생성되지 않을 것으로 기대하는 기법이다. 보통 일괄 확인은 확인하였을 때 실패하면 어느 요소 때문에 실패하였는지 알기 어렵다. 이 때문에 블록체인 롤업에서는 어느 한 참여자는 개별적으로 모두 확인을 해야 하며, 다른 참여자들은 이 참여자에 의해 롤업된 증명을 확인하게 된다.

7.3 익명성 향상 기술

비트코인과 같은 암호화폐는 어느 정도 수준의 프라이버시를 제공한다. 하지만 공개형 블록체인이므로 공개된 정보를 통해 정보의 노출은 불가피하며, 특정 주소의 소유주 정보를 알게 되면 이 소유주의 거래 기록을 모두 알게 되는 문제점이 있다. 이와 같은 정보의 노출을 줄이기 위해 여러 가지 프라이버시 기술이 암호화폐 구현에 적용되고 있다. 하지만 프라이버시 수준이 높아지면 해당 암호화폐가 불법적 거래에 악용될 소지를 높여주는 부작용도 있다. 모네로는 링 서명을 이용하고 있고, Zcash는 영지식 증명을 이용하며, Dash는 코인을 섞는 방법을 이용하여 거래의 프라이버시를 높이고 있다.

7.3.1 모네로

모네로는 링 서명, 스텔스(stealth) 주소, Pedersen 비트 약속을 이용하여, 트랜잭션의 지불자, 수취인, 금액을 숨겨준다. 14장에서 살펴본 링 서명은 서명자가 여러 개의 공개키를 이용하여 링을 만든 후 서명을 진행하게 된다. 서명의 확인자는 이 링에 포함된 서명자 중 어느 서명자가 실제 서명했는지 알 수 없다. 모네로는 처음에는 서명자가 자율적으로 링 크기를 설정할 수 있도록 했지만 현재는 링 크기를 11로 고정하고 있다. 이것은 링 크기가 또 다른 정보의 노출이 될 수 있기 때문이다. 서명 확인자는 어떤 UTXO가 실제 사용되었는지 모르기 때문에 이중 사용을 방지할 수 있는 방법이 필요하다. 모네로는 키 이미지를 서명에 포함하여 이 문제를 해결하고 있다. 키 이미지는 서명키를 이용하여 생성하며, 트랜잭션 서명에 사용된 개인키와 키 이미지 생성에 사용된 개인키가 같음을 영지식으로 형태로 증명하게 된다.

특정 사용자가 포함하는 키 이미지가 항상 같으면 프라이버시가 제공되지 않는다. 하지만 모네로의 UTXO 주소(공개키)는 스텔스 주소를 사용하며, 이 스텔스 주소는 수신자의 공개키와 전송자가 선택한 랜덤값으로 생성되기 때문에 대응되는 이 UTXO를 사용하기 위한 개인키도 매번 달라지게 된다. 따라서 키 이미지는 트랜잭션마다 독특하고 서로 연결할 수 없다.

모네로는 타원곡선 기반 공개키 암호알고리즘을 사용하고, 각 사용자는 두 개의 공개키 쌍을 사용한다. 여기서 G는 모네로에서 사용하는 타원곡선 군의 생성자이다. 수신자의 공개키가 $A = aG$와 $B = bG$일 때 스텔스 주소는 $P = H(rA)G + B$와 같이 계산된다. 여기서 r은 전송자가 선택한 랜덤값이며, 전송자는 $R = rG$를 트랜잭션에 포함한다. 수신자는 $D = H(aR)$를 계산한 후에 $DG + B$가 P와 같은지 확인하여 이 트랜잭션의 수신자가 본인인지 확인하게 된다.

금액을 숨기기 위해 사용하는 Pedersen 비트 약속은 동형 암호 방식이므로 다중 입력의 개별 금액을 확인할 수 없지만 그것의 합과 다중 출력의 합이 같다는 것은 쉽게 확인할 수 있다.

7.3.2 Dash

일반적으로 거래를 하다 가지고 있는 코인을 다른 사용자의 코인과 섞어 원장에 나타나는 거래 기록의 연결 고리를 끊는 방법으로 거래의 프라이버시를 높여주고 있다. 자신이 가지고 있는 코인을 다른 사용자와 섞기 위해서는 먼저 가지고 있는 금액을 정해진 액면가로 분할해야 한다. 특정 액면가로 분할된 코인은 마스터노드를 통해 다른 사용자의 코인과 섞을 수 있다. 마스터 노드는 3명의 사용자로부터 동일 액면가의 코인을 받아 이를 섞어 다시 재분배하여 준다. 제3자가 이 트랜잭션을 원장에서 보면 입력과 출력을 연결할 수 없다. 하지만 마스터 노드는 트랜잭션의 입력과 출력 관계를 알고 있다. 따라서 한번 섞는 것이 아니라 여러 번 다른 마스터 노드를 통해 섞어야 원하는 수준의 프라이버시를 얻을 수 있다.

7.4 스테이블 코인

기존 명목 화폐 또는 금과 같은 실물 자산과 연동하여 안전성을 보장하는 암호화폐를 스테이블 코인이라 한다. 암호화폐가 실제 거래에 사용되기 위해서는 암호화폐 가격 변동성이 적어야 한다. 이 때문에 개발된 것이 스테이블 코인이다. 크게 법정화폐 담보형, 암호자산 담보형, 무담보형 3종류로 구분된다. 법정화폐 담보형은 기관에 법정화폐를 담보로 예치하는 화폐이고, 암호자산 담보형은 기관에 암호화폐를 담보로 예치하며, 무담보형은 코인의 유통량을 조절하여 코인 가격을 유지하는 방식의 화폐이다. 현재 각 나라의 중앙은행도 암호화폐의 발행을 검토하고 있으며,

중앙은행이 발행하는 암호화폐를 CBDC(Central Bank Digital Currency)라 하며, CBDC는 당연히 스테이블 코인 형태의 암호화폐이다. CBDC의 이점은 중앙은행이 발행하기 때문에 신뢰할 수 있고, 명목화폐를 발행하는 비용을 절감할 수 있다. 또 국가 경계를 넘는 거래의 처리 속도를 향상할 수 있으며, 은행 시스템에 대한 접근이 어려운 지역의 경제 활동에 큰 역할을 할 수 있을 것으로 기대하고 있다.

7.5 NFT

대체 불가 토큰인 NFT는 디지털 자산에 대한 소유권 인증서이다. NFT는 블록체인을 통해 발행되며, 블록체인을 통해 소유권 변동 내역을 관리한다. 실제 디지털 자산이 블록체인에 저장되는 것은 아니고, 디지털 자산과 관련된 메타 데이터(소유권, 디지털 자산 링크 정보 등)만 블록체인에 유지한다. NFT는 쉽게 디지털 자산의 소유권을 나누어 유지할 수 있게 해준다. NFT는 스마트 계약으로 표현할 수 있으며, 이를 통해 제작한 예술가에게 계속 수익 보장도 가능하다. 현재 NFT는 주로 이더리움 토큰(ERC-71) 기반이다.

NFT는 다른 토큰 또는 코인과 달리 동등하게 교환할 수 없다. 이것은 각 토큰의 가치가 같지 않기 때문이다. NFT는 자신의 소유권이 아닌 디지털 자산을 발행할 수 있는 문제점과 원본이 소실될 수 있는 가능성도 있다. 또 현재 거래된 NFT의 가격들이 적절한 것인지, 버블이 있는 것인지, 계속 활성화될지는 미지수이다.

7.6 암호화폐 활성화가 가져올 변화

암호화폐를 이용하여 P2P 거래(no need for middlemen)가 가능해짐에 따라 기존에 중개자를 활용한 많은 서비스가 P2P 서비스로 전환할 것으로 예측하고 있다. 대표적으로 부동산, 해외송금 등이 여기에 해당한다. 사용자는 중개수수료를 지불하지 않거나 대폭 줄일 수 있기 때문에 이와 같은 서비스들이 매력적이라고 느낄 수 있다. 하지만 중개자가 없다는 것은 응용에 따라 사용자 입장에서는 매우 불편할 수 있다. 예를 들어 부동산 거래를 중개자 없이 하고자 할 경우 사용자가 스스로 해야 하는 일이 복잡하고 많을 수 있다. 또 부동산 거래는 보통 고액이 교환되어야 하므로 암호화폐를 통해 거래하는 것은 아직은 현실적이지 못하다. 그럼에도 불구하고 SMART REALTY(smartrealty.io), ATLANT(atlant,io), Ubitquity(www.ubitquity.io), Averspace(averspace.com) 등과 같은 부동산 관련 블록체인 스타업 기업들이 많이 설립되고 있다.

소액 P2P 거래로 인한 이보다 더 중요한 변화는 프로슈머에 대한 자동 보상이 가능해진다는 것이다. 예를 들어 storj.io는 자신의 개인 컴퓨터에 남은 하드디스크 공간을 공유받고 이에 대한 보상을 해주고 있다. steeit.com은 콘텐츠를 생성하고 큐레이트하는 사용자들에게 보상을 해주고 있다. vevue.com은 사용자들이 각종 음식점의 동영상을 촬영하여 공유하면 보상해주고 있으며, 구글맵과 이 영상을 연동하여 서비스를 제공하고 있다. 암호화폐를 이용한 소액거래, 이더리움의 스마트 계약은 이와 같은 서비스 구축을 용이하게 해주고 있다.

7.7 블록체인의 활용

비트코인 자체보다 지금은 비트코인을 실현하기 위해 사용된 블록체인 기술에 대한 관심이 많으며, 웹 이후 세상에 큰 변화를 가져다줄 수 있는 획기적인 기술로 간주하고 있다[9, 10]. 실제 블록체인은 암호화폐의 실현 외에 다양한 용도로 활용될 수 있다. 특히, 이전에 일괄 처리하던 것들을 블록체인을 통해 실시간 처리가 가능해진다. 가장 많이 생각되고 있는 응용들은 블록체인의 불가역성이 필요한 응용들이다. 몇 가지를 소개하면 다음과 같다.

- 앞으로 기존 금융기관들도 블록체인에 거래 기록들을 유지할 것으로 예측되고 있다.
- 예스토니아 정부는 정부의 모든 기록을 블록체인에 저장하고 공개하고 있다. 이들은 KSI(Keyless Signature Infrastructure)라는 형태의 블록체인을 사용하고 있다[11].
- agora.vote, polys.me 등은 블록체인을 이용한 전자선거 기법을 개발하였다.
- 중고자동차의 주행기록을 조작할 수 없도록 차량의 주행정보를 받아 블록체인에 기록할 수 있다[12].
- 각 종 로그 정보를 기록한다. 예를 들어 시스템 로그를 블록체인에 기록하면 공격자가 침입한 후에 침입 흔적을 지우는 것이 가능하지 않게 된다.

각 종 증명서 (출생, 부동산 소유, 여권 등)를 블록체인에 저장하는 것도 제안되고 있다[13]. 디지털화된 증명서를 블록체인에 저장하는 것과 일반 데이터베이스에 저장하는 것의 차이는 무엇일까? 쉽게 생각하면 블록체인은 불가역성을 제공하고 일반 데이터베이스는 그렇지 못한 것이 차이로 생각할 수 있다. 또는 블록체인은 근본적으로 분산저장되는 반면 일반 데이터베이스는 그렇지 않다고 생각할 수 있다. 일반 데이터베이스에 데이터를 저장할 때 쉽게 조작할 수 없도록 블록체인처럼 전자서명하여 저장한다고 하자. 또 데이터 손실이나 접근의 효율성을 위해 블록체인만큼은 아니지만, 데이터베이스를 중복하여 유지한다고 하자. 그러면 블록체인과 일반 데이터베이스가 제공하는 특징의 차이가 없어 보일 수 있다. 하지만 이렇게 생각하는 것은 블록체인의 중요한 특징을 간과하는

것이 된다. 블록체인은 체인으로 데이터가 엮여 있고 첨삭 전용이므로 해당 데이터를 생성한 사용자를 포함하여 누구도 수정을 할 수 없다. 반면에 일반 데이터베이스는 해당 레코드를 추가한 서명키를 가지고 있는 사용자는 쉽게 레코드의 내용을 수정할 수 있다. 따라서 일반 데이터베이스도 블록체인과 동일한 기능을 하기 위해서는 첨삭만 할 수 있어야 한다. 또 DID는 블록체인의 불가역성을 활용하지만 그것의 핵심은 개인에게 자신의 정보에 대한 주권을 주는 것이 핵심이다.

7.8 표준화

현재 블록체인 관련 기술에 대한 표준화 작업도 진행 중이다. 2016년에 블록체인 관련 기술을 표준화하기 위해 ISO 기술위원회 307이 발족되었으며, 이 기술위원회는 블록체인과 분산원장 기술에 대한 표준화 작업을 하고 있다. 블록체인 기술이 실제 현장에서 유용하게 사용되기 위한 또 다른 거림돌은 관련 법, 제도가 정비되어 있지 못하며, 지금은 나라마다 독자적이고 다른 규율을 일부 적용하고 있다. 참고로 우리나라와 중국은 ICO가 금지되어 있다.

8. 마무리

분산 암호화폐인 비트코인은 그것이 기술적으로 실현되었다는 측면에서 매우 의미가 있다. 하지만 사토시 나카모토도 이렇게 투기 목적 수단이 될 것으로는 생각하지 못하였을 것이다. 더욱이 암호화폐를 명목화폐로 바꾸는 것이 필요하며, 일반 대중의 쉬운 접근을 위해서라면 거래소라는 것이 생길 수밖에 없으며, 거래소 때문에 이들 암호화폐가 진정한 분산 암호화폐라고 보기 힘든 측면도 있고, 여러 가지 부작용도 나타나고 있다. 이 때문에 암호화폐가 일상에서 신용카드처럼 널리 사용되기에는 아직도 갈 길이 멀다. 그러나 해외송금을 하거나 기업에서 직원들에게 월급을 줄 때 암호화폐로 주는 경우도 많이 생기고 있기 때문에 미래에 암호화폐가 어떤 위치를 차지할 것인지는 아직 예측하기 어렵다.

블록체인이 우리가 사용하는 서비스에 획기적인 변화를 줄 것은 분명하다. 하지만 불필요하게 블록체인을 사용하고자 하는 경향도 있다. 예를 들어 steemit의 경우에는 콘텐츠 자체를 블록체인에 등록하고 있다. 하지만 데이터 자체를 블록체인에 등록하는 것이 꼭 필요한 것인지 생각해볼 여지가 있다. steemit에서 사용자들에게 보상하기 위한 토큰을 사용하며, 이 토큰을 안전하게 사용하기 위해서는 블록체인을 활용하는 것은 효과적이다. 하지만 콘텐츠까지 블록체인에 등록될 경우 악의적인 글이나 명예를 훼손하는 글까지도 영구적으로 삭제되지 않고 유지될 수밖에 없다.

참고문헌

[1] Vitalik Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” https://github.com/ethereum/wiki/wiki/White-Paper, 2013.

[2] Nick Szabo, “Formalizing and Securing Relationships on Public Network,” First Monday, Vol. 2. No. 9, Sept. 1997.

[3] Serguei Popov, “The Tangle,” Whitepaper, V.1.4.3, `https://iota.org`, Apr. 2018.

[4] Colin LeMahieu, “Nano: A Feeless Distributed Cryptocurrency Network,” `https://www.exodus.com/assets/docs/nano-whitepaper.pdf`, 2018.

[5] Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol,” Advances in Cryptology, Crypto 2017, LNCS 10401, pp. 357–388, Aug. 2017.

[6] Jing Chen, Silvio Micali, “ALGORAND,” ArXiv, `https://arxiv.org/abs/1607.01341`, 2017.

[7] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, Krzysztof Pietrzak "Proofs of Space," Advances in Cryptology, Crypto 2015, LNCS 9216, Springer, pp. 585–605, 2015.

[8] Leemon Baird, Mance Harmon, and Paul Madsen, "Hedera: A Public Hashgraph Network & Governing Council," Whitepaper V.2.1, `https://hedera.com/papers`, 2020.

[9] 마이클 케이시, 폴 비냐, 비트코인 현상 블록체인 2.0, 미래의창, 2017.

[10] 돈 탭스콧, 알렉스 탭스콧, 블록체인 혁명, 을유문화사, 2017.

[11] Ahto Buldas, Andres Kroonmaa, Risto Laanoja, "Keyless Signature Infrastructure: How to Build Global Distributed Hash-Trees," IACR eprint 834, 2013.

[12] "BMW Test Drives Blockchain for Car Mileage Tracking," https://www.coindesk.com/blockchain-startup-tracks-vehicle-mileage-with-bmw/, 2018.

[13] "Dubai Plans Digital Passports Using Blockchain Tech," https://www.coindesk.com/dubai-plans-gate-less-airport-security-using-blockchain-tech/, 2017.

퀴즈

1. UTXO 기반과 계정 기반을 비교한 다음 설명 중 틀린 것은?

   ① 계정 기반은 한 계정의 트랜잭션을 병행으로 수행할 수 없다.

   ② UTXO 기반에서 제3자는 한 계정의 보유한 총액을 알기 어렵다.

   ③ 계정 기반은 트랜잭션의 내용이 매우 단순하다.

   ④ 프로그래밍하기에는 UTXO 기반이 유리하다.

2. 비트코인은 UTXO 기반이고, 이더리움은 계정 기반을 사용하고 있다. 이와 관련된 다음 설명 중 틀린 것은?

   ① UTXO에서 계정의 지갑은 이 계정에 해당하는 트랜잭션 출력 중 아직 사용하지 않은 출력이 어느 블록에 있는지 유지해야 한다.

   ② 이더리움은 프로그래밍을 통해 거래가 이루어지며, 다양한 디앱 개발이 목적이기 때문에 각 계정의 총액을 쉽게 알기 위해 계정 모델을 채택하였다.

   ③ UTXO 기반, 계정 기반 모두 한 계정의 여러 거래(트랜잭션)를 병행으로 처리할 수 있다.

   ④ UTXO 모델에서는 수수료를 입력과 출력 차이로 표현할 수 있지만 계정 모델에서는 거래는 항상 단순하게 한 계정에서 다른 계정으로 일정 금액의 이동이기 때문에 거래 자체로는 수수료를 나타낼 수 없다.

3. 블록체인을 어떤 응용을 만들 때 활용하고자 한다. 블록체인은 두 가지 중요한 특징은 불가역성과 데이터의 분산(여러 노드에 동일 데이터가 자동 중복 저장됨)이다. 블록체인을 활용할 때 고려할 점으로 적절하지 않은 것은?

   ① 블록체인은 불가역성을 제공하기 때문에 계속 데이터가 쌓이기만 하는 구조이다. 기존 데이터 저장과 달리 적절한 aging 기법을 사용하여 더 이상 불필요한 데이터를 제거하는 것이 가능하지 않을 수 있다.

   ② 블록체인은 불가역성을 제공하기 때문에 데이터를 삭제하고 싶어도 삭제할 수 없다. 따라서 오류가 있는 데이터, 불법적인 데이터, 프라이버시를 침해하는 데이터도 한번 저장되면 삭제할 수 없다.

   ③ 충분한 노드가 운영되지 않으면 데이터 분산 효과를 얻지 못할 수 있다.

   ④ 블록체인을 응용에 활용하고 싶으면 반드시 자체적으로 새 블록체인을 만들어 사용해야 한다.

4. 비트코인에서 블록체인의 불가역성과 분산 합의을 제공하기 위해 해시퍼즐을 이용한 작업증명을 이용하고 있다. 하지만 작업증명은 에너지 소모가 많고 일시적 포크 발생 문제로 확정 시간도 느린 문제점이 있다. 이 문제를 극복하기 위해 지분 증명, 공간 증명, DAG 등 다양한 시도가 있다. 이와 관련된 다음 설명 중 틀린 것은?

   ① 지분 증명, 공간 증명, DAG는 기본적으로 소모적인 연산을 사용하지 않는다.

   ② 지분 증명, 공간 증명, DAG 3가지 모두 체인 형태로 연결하여 블록체인에 등록된 데이터를 수정, 삭제하고자 하면 그 이후 연결되어 있는 모든 것을 수정하도록 하여 수정, 삭제하기가 어렵게 되어 있다.

③ 지분 증명, 공간 증명, DAG 모두 여러 트랜잭션들을 모아 블록을 만들고 그것을 확정하는 형태이다.

④ 지분 증명은 라운드마다 검증할 검증자를 결정하며, 결정된 단일 검증자 또는 다수 검증자가 이번 라운드의 블록을 생성한다.

5. NFT와 관련된 다음 설명 중 틀린 것은?

① 디지털 자산이 NFT 토큰 내에 저장되어 있다.

② 디지털 자산의 소유권을 증명하는 증서 역할을 한다.

③ 다른 토큰/코인과 달리 동등하게 교환할 수 없다.

④ 소유권 변동 내역을 블록체인 기록하여 관리하며, 소유권을 나눌 수 있다.

연습문제

1. 비트코인 등 많은 블록체인 기반 암호화폐는 UTXO 기반이다. 하지만 이더리움은 UTXO 기반이 아니라 계정 기반이다. UTXO 기반과 비교하여 계정 기반의 장단점을 설명하시오.

2. 이더리움은 트랜잭션 수수료를 가스 상한과 가스비를 이용하여 제시한다. 이와 관련하여 다음 각각에 대해 답변하시오.

① 실제 소요된 가스가 트랜잭션에 제시한 가스 상한보다 크면 이 트랜잭션의 실행 결과는 블록체인에 반영되지 않는다. 따라서 충분히 큰 가스 상한을 제시해야 한다. 이 때문에 무조건 매우 큰 가스 상한의 제시를 생각해 볼 수 있다. 이것의 문제점을 설명하시오.

② ①과 같이 가스가 부족하여 트랜잭션이 취소되면 이 트랜잭션을 포기하거나 다시 제출해야 한다. 다시 제출하면 이 트랜잭션의 실행을 위해 실제 필요한 것보다 많은 비용을 지불하게 된다. 왜 이와 같은 방식을 이더리움이 사용하는지 설명하시오.

3. 한 사용자는 지갑을 여러 개 만들어 참여할 수 있으며, 두 지갑이 같은 사용자 소유라는 것을 알기 어렵다. 한 사용자가 매우 많은 수의 지갑을 만들어 참여한다고 지분 증명에서 검증자가 될 확률이 높아지면 여러 문제가 발생할 수 있다. 이 때문에 지분이 많다고 항상 검증자로 선택되는 방식은 올바른 검증자 결정 방식이 아니다. 따라서 확률적 요소가 검증자를 결정할 때 적용되어야 한다. 지분 증명에서 사전에 향후 라운드의 검증자를 높은 확률로 예측할 수 있다면 어떤 공격이 가능한지 설명하시오.

4. 각종 증명서를 블록체인에 저장하는 서비스도 등장하고 있다. 기존 공개키 기반구조를 활용하여 발급기관이 전자서명 기술을 통해 디지털 증명서를 발급할 수 있다. 이것과 비교하여 블록체인을 이용한 증명서의 차이점 또는 장점은 무엇인지 설명하시오. 여기서 블록체인을 이용한 증명서란 증명서의 해시값 또는 전자서명값을 블록체인에 저장하는 것을 말한다.

5. 에스토니아는 블록체인에 정부의 각종 문서를 전자서명하여 저장한다. 블록체인에 저장하는 것과 일반 데이터베이스에 저장하는 것은 어떤 차이가 있는지 설명하시오.