정보보호개론

제15장 블록체인과 암호화폐

1. 암호화폐

우리는 현재 명목화폐(fiat money)[1] 외에 신용카드 등을 포함하여 다양한 지불 수단을 사용하고 있다. 현재 대부분의 웹서비스는 자체 포인트 형태의 사이버 머니를 충전하도록 한 다음, 이를 이용하여 유료 서비스를 사용하도록 하고 있다. 하지만 신용카드를 포함하여 이와 같은 지불 수단은 우리가 실제 사용하는 명목화폐의 특징을 가지고 있지 못하여 불편한 점도 있다. 명목화폐의 주요 특징은 다음과 같다.

- 위조의 어려움
- 휴대 가능
- 익명성 보장
- 양도 가능
- 분할 가능
- 오프라인 지불
- 범용 지불

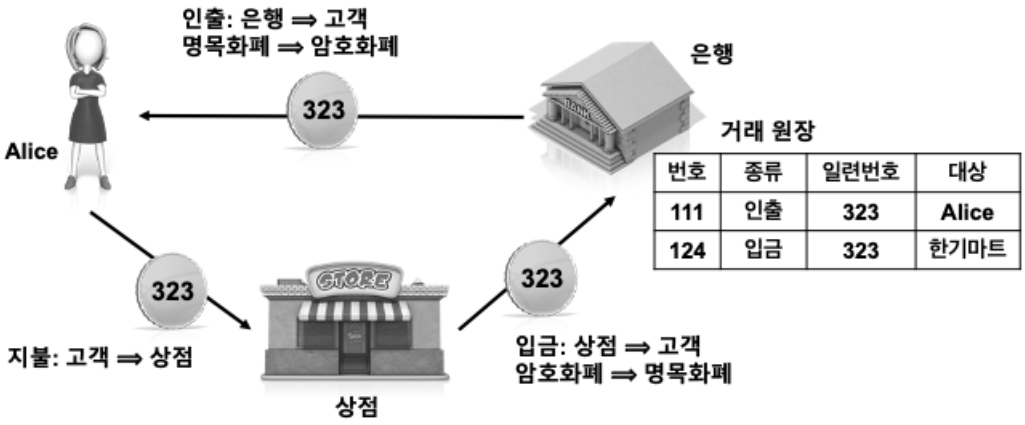
명목화폐가 가지는 이와 같은 특징을 암호화폐[2]가 가지게 하는 것은 매우 어려운 일이다. 명목화폐는 네트워크를 통해 지불할 수 없기 때문에 오프라인 지불 방식이라고 이해할 수 있다. 하지만 전자화폐에서 오프라인 지불이란 제3자의 도움 없이 지불자와 판매자 간의 거래가 이루어질 수 있다는 것을 말한다. 신용카드와 같은 지불방식은 지불할 때마다 상점이 별도 서버에 접속하여 거래 가능 여부를 확인해야 하므로 온라인 지불방식이 된다. 따라서 전자화폐의 분류 측면에서 명목화폐도 오프라인 지불 방식에 해당한다. 암호프로토콜의 분류에서 중재자 참여 여부에 따라 중재자를 온라인, 오프라인으로 분류하였는데, 이 개념을 전자화폐 지불 프로토콜에 적용한 개념이다.

초기 암호화폐는 그림 15.1처럼 사용자는 발행기관으로부터 디지컬값인 암호화폐를 발급받아 자신의 기기에 유지해야 하고, 지불할 때 이를 상점에 전달해야 한다. 온라인 방식에서는 **이중 사용**(double spending) 문제를 해결하기 위해 상점은 거래를 승인하기 전에 발행기관에 받은 암호화폐를 전달하여 이전에 사용된 화폐인지 확인해야 한다. 이 과정에서 상점은 암호화폐에 해당하는 명목화폐를 자신의 계좌에 입금받게 된다.

비트코인이라는 암호화폐가 나오기 전까지는 기본적으로 암호화폐는 이처럼 중앙은행 또는 중앙은행이 허가한 기관만 발행할 수 있어야 한다고 생각하였다. 화폐는 그것이 실제 유통되지 않으면 아무런 의미가 없으며 정부의

[1] 명목화폐는 화폐가 가지는 실질적 가치와는 관계없이 표시된 화폐 단위로 통용되는 화폐를 말한다. 명목화폐는 기존 실물화폐(commodity money)가 가지는 분할성, 동질성, 내구성, 휴대성 등의 취약점을 극복하기 위해 등장한 화폐이다.

[2] 전자화폐(electronic cash)는 디지털화된 모든 종류의 화폐를 말하며, 암호화폐(crypto currency)는 암호기술을 사용하는 암호화폐를 말한다. 더 구체적으로 화폐의 안전성이 암호기술을 통해 보장되는 화폐를 말한다. 각 용어에 대한 정의는 다른 자료에서 다르게 사용할 수 있다.



<그림 15.1> 초기 온라인 암호화폐 동작 방식

허가 없이 어떤 종류의 화폐를 유통한다는 것은 상식적으로 생각하기 어려운 측면이 있다. 또 암호화폐도 명목화폐처럼 디지털화된 어떤 값이 지불자에서 수취인으로 전달되어야 한다고 생각하는 경향이 많다. 하지만 사이버 머니만 보더라도 이것이 필요 없다는 것을 쉽게 인식할 수 있다. 사이버 머니는 대부분 서버 데이터베이스의 각 사용자 계정 정보 중 하나로 유지되며, 이 카운터 값의 감소를 통해 소비되기 때문에 어떤 값들이 지불자와 수취인 사이에 직접 오고 가는 것은 아니다. 경제학자 Kocherlakota는 원장에 거래 내역을 모두 기록하는 것만으로 화폐의 역할을 할 수 있다는 것을 주장하였다[1].

대부분의 기존 오프라인 암호화폐는 분할이 가능하지 않으며 양도를 할 수 없다. 이 때문에 고객은 명목화폐를 주고 암호화폐를 발급받게 되며, 암호화폐를 이용하여 지불하면 상점은 이것을 다시 은행에 입금하여 명목화폐로 바꾸는 방식이 주로 제안되었다. 여기서 알 수 있는 것은 앞서 설명한 개념과 달리 이와 같은 암호화폐들은 지불자들이 특정 값을 유지하고 있어야 하며, 이 값을 지불과정에서 상대방에게 전달해야 한다. 또 이와 같은 암호화폐는 고객과 상점을 명확하게 구분하고 있으며, 고객 간 암호화폐의 교환을 고려하지 않고 있다. 즉, 한 고객으로부터 암호화폐를 받아 다시 그 화폐를 사용할 수 있는 양도 기능을 제공하는 암호화폐를 비트코인 이전에는 성공적으로 만들지 못하였다. 이 때문에 거스름을 제공하기도 어렵다.

화폐가 디지털화되면 명목화폐가 가지고 있지 않은 특징들을 가지게 되며, 이 때문에 발생하는 문제를 해결하기도 어렵다. 디지털화된 암호화폐의 가장 핵심적인 보안 문제는 이중 사용 문제이다. 온라인 방식의 암호화폐는 화폐 발급자가 지불이 승인되기 전에 이중사용 여부를 검사할 수 있기 때문에 이중사용을 방지하기가 수월하다. 반면에 오프라인 방식에서는 이 화폐가 이전에 사용된 것인지 상점이 확인할 방법이 없다. 따라서 상점이 암호화폐를 입금할 때 이중사용 여부를 확인할 수밖에 없다. 이 때문에 양도가 가능하지 않은 기존 오프라인 암호화폐에서는 암호화폐를 인출한 소유주만 화폐를 이용할 수 있도록 제한하였고, 이중사용이 발생하면 소유주에게 책임을 묻는 방식을 사용하였다. 비트코인 이전 암호화폐들은 DigiCash처럼 유통을 시도한 경우도 있지만 대부분은 연구 논문으로만 발표되고 현실 세계에서 실제 유통되지 못하였다.

1.1 익명 인증 기술을 이용한 간단한 암호화폐

RSA 은닉서명을 이용한 간단한 온라인 암호화폐를 살펴보자.보통 암호화폐는 분할하거나 양도할 수 없어서 상점이 거스름을 만들어 주는 것이 어렵다. 이 때문에 지불할 때 정확한 금액을 맞추어 지불해야 한다. 우리가 살펴보고자 하는 암호화폐는 이와 같은 방식을 사용한다. 따라서 충분한 금액의 암호화폐가 있더라도 지불금액을 정확하게 맞출 수 없으면 지불이 가능하지 않다는 문제점이 있다.

이 암호화폐는 은행이 전자서명하여 발급하기 때문에 위조가 어렵다. 또한 발급할 때 사용한 서명키에 의해 발급된 화폐의 액면가가 결정된다. 따라서 발행기관은 발행하는 액면가의 종류만큼의 서로 다른 공개키 쌍을 생성하여

사용하며, 이들 공개키와 대응되는 액면가를 공표한다. 고객은 특정 액면가의 화폐를 발급받고 싶으면 발행기관과 인출 프로토콜을 수행하여야 한다. 이때 익명성을 위해 RSA 은닉서명을 수행하며, 은닉된 메시지는 화폐의 일련번호가 된다. 고객이 부정할 수 없도록 cut-and-choose 기법을 사용하여 인출한다고 가정한다. 발행기관은 암호화폐에 해당하는 금액을 해당 고객의 계좌에서 인출한다. 인출 과정이 완료되면 고객은 특정 일련번호에 대해 발행기관이 서명한 서명값을 가지게 되며, 이 값이 암호화폐가 된다.

지불과정에서 고객은 지불금액에 맞게 자신이 가지고 있는 서명값들을 전달해야 한다. 암호화폐가 다른 사용자에게 노출되지 않도록 안전하게 상점에게 전달되어야 하며, 상점은 이 지불을 받기 전에 발행기관에 암호화폐의 이중사용 여부를 확인해야 한다. 은행의 승인이 있으면 거래가 완료되며, 발행기관은 해당 금액만큼을 상점 계좌에 입금하여 주게 된다. 이 암호화폐는 은닉서명을 통해 위조불가능성과 무조건적인 익명성을 제공하게 된다. 하지만 이 화폐를 개선하여 오프라인 지불이 가능하도록 또는 양도가 가능하게 하는 것은 간단하지 않다. 이 측면에서 비트코인의 기술을 살펴볼 필요가 있다. 비트코인은 신뢰할 수 있는 발행기관을 사용하지 않으면서 명목화폐가 가지는 대부분의 특성을 가지는 암호화폐이다.

2. 비트코인

비트코인은 실제 유통되고 있는 암호기술을 이용하는 가상화폐(virtual currency)[3]이다. 비트코인은 다음과 같은 특징을 가지고 있다.

- 자체 강화 방식
- 오프라인 방식
- 양도 가능
- 분할 및 통합 가능
- 익명 지불 가능
- 첨삭만 가능한 **분산원장**(distributed ledger) 기반

비트코인은 암호화폐를 발행하는 신뢰기관을 사용하지 않는다는 측면에서 자체 강화 방식이다. 이것이 가장 획기적인 변화이다. 중앙집중 신뢰기관에 대한 의존 없이 화폐를 발행하고 사용자 간의 직접 거래가 가능하게 된 것이다. 비트코인에서 지불은 다른 사람의 도움 없이 이루어질 수 있지만 실제로는 지불 내용을 전체 비트코인 네트워크에 전달해야 하며, 거래가 즉시 확정되지 않고 일정 시간이 지나야 확정되는 방식을 사용하고 있다. 따라서 정확하게 오프라인 방식이라고 말하기 힘든 측면도 있다. 비트코인은 양도가 가능하며, 여러 비트코인을 결합하여 하나의 비트코인을 만들 수 있고, 거꾸로 하나의 비트코인을 여러 비트코인으로 나눌 수 있다. 이 과정도 한 소유자가 다른 소유자에게 지불하듯이 가지고 있는 코인을 다시 자기 자신에게 지불하여 코인들을 결합하거나 분리한다[4].

비트코인의 소유자를 특정하기 어렵기 때문에 익명 지불이 가능하다고 하며, 비트코인을 이용한 전 세계의 모든 지불은 분산 원장에 기록되어 수정이 가능하지 않게 되어야 거래가 확정되는 방식이다. 이것이 비트코인의 핵심이다. 비트코인 이전 연구에서는 어떤 별도 디지털 값이 금전적 가치를 가지게 되는 형태이었으며, 방식이 온라인이든 오프라인이든 상관없이 기존 금융 모델(은행과 같은 신뢰 기관에 의한 화폐의 발행)을 가정하고 있다. 하지만 비트코인은 특정 신뢰 기관을 전혀 사용하지 않으며, 별도 값이 금전적 가치를 가지기보다는 공개 원장에 거래가 기록되어 금전적 효력을 가지게 되는 방식이다.

[3]법정 화폐의 반대 개념으로 발권력의 독점과 법률상 강제 통용력이 주어져 있지 않은 제도권에서 인정하지 않는 화폐를 말한다.
[4]보유한 비트코인을 결합하거나 나누는 경우에도 트랜잭션을 생성하여 블록체인에 기록되어야 하므로 수수료가 발생한다.

T_1	H(header||in||out)
헤더(header)	종류: 생성, in의 개수: 1, out의 개수: 1, 이 외에 필요한 정보
입력(in)	이전거래: 없음
출력(out)	금액: 100원, 수취인: $H(+K_S)$
서명	Sig.–$K_S(T_1)$

<그림 15.2> 한기코인: 생성

T_2	H(header||in||out)
헤더(header)	종류: 지불, in의 개수: 1, out의 개수: 1, ...
입력(in)	이전거래: $T_1 : 0$
출력(out)	금액: 100원, 수취인: $H(+K_A)$
서명	Sig.–$K_S(T_2)$

<그림 15.3> 한기코인: 지불 S에서 A

2.1 한기코인

비트코인을 이해하기 위한 가상의 암호화폐 한기코인을 만들어보자. 한기코인의 규칙은 다음과 같다.

- 총장(S)만 코인을 만들 수 있다.
- 코인의 소유자는 다른 사람에게 코인을 양도할 수 있다.
- 모든 거래는 전체 공개된다.

모든 참여자는 공개키 쌍을 가지고 있으며, 거래를 진행하기 위해서는 상대방의 공개키를 확보해야 한다. 익명성 때문에 인증서를 사용하지는 않는다. 하지만 총장만 코인을 만들 수 있으므로 총장은 인증서를 사용한다고 가정한다. 일반 사용자는 인증서를 사용하지 않지만 한 사용자가 다른 사용자에게 코인을 양도하기 위해서는 해당 사용자의 공개키를 정확하게 알아야 한다. 이 측면에서 보면 한기코인에서 프라이버시는 거래 당사자 간의 프라이버시를 제공하는 것이 아니라 제3자에게 지불자의 프라이버시만 보장된다고 볼 수 있다. 실세계에서 고객이 특정 상점에 들어가 현금으로 물건을 살 때와 유사한 측면이 있다.

한기코인에서 거래는 헤더, 입력, 출력, 서명 4가지 요소로 그림 15.2와 같이 구성된다. 이 거래를 코인이라는 하는 것은 오해의 소지가 많다. 실제 이것은 이전 절에서 살펴본 익명 서명을 이용한 암호화폐와 차이가 많다. 이전 절에서는 전자서명된 값 자체가 통용되는 화폐이지만 그림 15.2에 제시된 것은 통용되는 화폐라고 보기 어렵고 거래 명세에 해당한다. 즉, 은행이 은행 자신에게 100원을 지급한 거래 명세이다. 오해의 소지가 있지만 앞으로 거래 명세의 각 출력을 코인이라 하고, 한기코인을 설명한다.

한기코인을 이용한 모든 거래 명세는 누구든지 볼 수 있도록 공개되며, 공개된 정보는 수정이 불가능하다고 가정하자. 그림 15.2에 제시된 내용에 의하면 S는 100원을 보유하고 있다. 이 금액을 A에게 양도하고 싶으면 그림 15.3와 같은 거래를 만들어 공개하고 해당 정보를 A에게 전달한다. 실제 이 정보를 A에게 직접 전달할 필요는 없다. 거래 정보는 공개되는 것이므로 공개된 정보를 통해 A가 양도받았다는 사실을 알게 할 수 있다. 거래 명세에 의해 보유하게 된 코인을 다른 사람에게 양도하기 위해서는 해당 거래 명세 출력 정보에 있는 수취인의 공개키에 대응되는 개인키가 있어야만 가능하다. T_1의 유일한 출력에 있는 100원의 소유자는 S이므로 S만 이 금액을 사용할 수 있다. 이처럼 한 사용자가 소유한 코인은 해당 사용자만 사용할 수 있도록 제한하고 있다.

A도 같은 방법으로 다른 사용자에게 자신이 받은 코인을 양도할 수 있다. 수신한 코인은 이전 거래를 찾아가면서 각 거래 내역의 유효성을 검증해야 한다. 지불의 역사가 오래되면 연결된 지불이 매우 많을 수 있다. 따라서 연결을 따라 너무 오래된 것까지 다시 검증할 필요가 없어야 한다. 공개된 것은 모두 유효하고 수정이 불가능하다면 바로 전

T_3	H(header||in||out)
헤더(header)	종류: 지불, in의 개수: 1, out의 개수: 2, ...
입력(in)	이전거래: $T_2 : 0$
출력(out)	금액: 70원, 수취인: $H(+K_B)$
	금액: 30원, 수취인: $H(+K_A)$
서명	Sig.$-K_A(T_3)$

<그림 15.4> 한기코인: 지불 A에서 B

지불이 공개되어 있는지만 확인하면 된다. 여기서 중요한 것은 공개되는 것은 모두 유효해야 한다는 것이다. 이것을 보장하는 방법이 필요하다. 이중사용 방지도 현재 지불과 동일한 입력의 거래가 있는지 검색해 보면 된다. 따라서 이와 같은 검색을 효과적으로 할 수 있는 방법도 필요하다.

분할과 통합도 유사한 방법으로 제공할 수 있다. 예를 들어 그림 15.3의 100원 가격의 코인을 70원, 30원으로 분할하고 싶으면 그림 15.4처럼 거래를 만들어 등록하면 된다. 이 거래에 따라 A는 자신이 소유한 100원 코인을 70원, 30원으로 분할하여 70원은 B에게 양도하고 30원은 다시 자신이 가지게 된다. 여기서 기존 명목 화폐와 중요한 차이점 하나를 발견할 수 있다. 이와 같은 전자화폐에서 각 소유자가 소유한 총금액은 소유자가 아직 지불에 사용하지 않은 거래 출력(**UTXO**, Unspent Transaction Output)의 합이 되며, 명목 화폐처럼 거래들은 서로 섞이지 않는다. 또 사용자 지갑/장치에 코인이 유지되는 것이 아니라 공개되는 여러 거래 명세에 흩어져 존재하게 된다.

한기코인이 안전하게 유통되기 위해서는 한기코인을 위조할 수 없어야 하며, 유효한 거래만 공개되어야 하고, 공개된 거래는 수정할 수 없어야 한다. 현재 한기코인은 총장만 발행할 수 있도록 하였기 때문에 총장의 개인키가 있어야 화폐를 발행할 수 있다. 총장이 거래가 공개되기 전에 거래의 유효성을 확인하고 전자서명하여 공개하도록 하면 나머지 두 가지 요구사항도 제공할 수 있다. 예를 들어 A가 같은 코인을 이용하여 두 개의 거래를 만들어 동시에 공개하는 것을 시도할 수 있다. 또는 이전 사용된 거래를 삭제하여 이중 사용을 시도할 수 있다. 하지만 모든 거래는 총장의 승인이 필요하기 때문에 이와 같은 시도는 가능하지 않다. 따라서 신뢰할 수 있는 기관을 가정하면 한기코인과 같은 형태의 안전한 암호화폐를 만드는 것은 어렵지 않다. 다만, 이와 같은 형태이면 이 암호화폐는 중앙집중식 온라인 암호화폐가 된다.

비트코인은 이와 같은 신뢰 기관을 사용하지 않고 이 문제들을 해결하였다. 이를 위해 비트코인은 **분산 합의**(distributed consensus) 기술을 이용하고 있다. 분산 합의란 분산된 다수의 개체가 같은 값을 가지도록 하는 프로토콜을 말한다. 이때 개체들은 서로 신뢰하지 않으며, 일부 개체들은 동작하지 않을 수 있다. 이와 같은 조건에서도 분산 합의는 다수가 동일한 결론을 도출할 수 있도록 해준다. 앞서 살펴본 한기코인에서 A의 이중사용의 경우, 두 개의 거래가 각 분산된 개체에 도착하는 순서가 서로 다를 수 있다. 이처럼 분산 합의는 쉬운 문제가 아니며, 비트코인의 참여 노드들은 고정 ID를 사용하지 않기 때문에 더욱더 어렵다. 하지만 비트코인은 매력적인 장려책(incentive)과 즉시 결론을 내려도 되지 않게 하여 이 문제를 해결하였다. 제4차 산업 혁명의 중요한 보안 기술이라고 하는 **블록체인**이 바로 이것을 가능하게 해주는 기술이다.

블록체인은 불가역성을 제공하는 분산 원장을 말하며, 불가역성과 모든 노드가 같은 데이터를 유지하기 위해 내부적으로 분산 합의 기술을 사용하고 있다. 앞으로 설명할 비트코인이 사용하는 분산 합의 기술을 다른 말로 **나카모토 합의**라 하며, 합의 기술에는 그 기술에서 합의가 보장되기 위해 사용하는 규칙과 규칙이 준수되도록 하는 보상체계나 규칙을 준수하지 않을 경우의 불이익 체계도 포함된다.

2.2 비트코인의 세부 동작원리

비트코인은 **사토시 나카모토**(Satoshi Nakamoto)라는 익명의 사람 또는 그룹이 2008년에 처음 소개하였으며[2], 2009년부터 유통되어 실제 사용되고 있는 암호화폐이다. 사이퍼펑크(cypherpunk) 움직임의 일환으로 보는 사람들도 있고, 당시 전 세계적인 금융 위기에 대한 해결책으로 고안된 것이라고 주장하는 사람들도 있다. 비트코인의

통화는 BTC, XBT 등의 용어를 사용하며, 가장 작은 단위의 BTC를 1 satoshi[5]라 한다. 2017년 5월 31일, 2018년 5월 21일, 2019년 5월 7일, 2020년 5월 11일, 2021년 5월 14일, 2022년 5월 6일 기준으로 1 BTC의 거래 가격은 각각 2,451달러, 8,505달러, 5,732달러, 8,760달러, 50,438달러, 36,398달러이며 우리나라 거래소 중 한 곳의 거래 가격은 각각 3,129,000원, 9,384,000원, 6,654,000원, 10,676,000원, 61,906,000원, 47,101,000원이었다. 가격이 매우 가파르게 상승하다 최근에 조금씩 내려가고 있다. 2022년 5월 6일 기준으로 지금까지 생성된 비트코인의 수는 19,031,962.5개이다. 비트코인은 기존 비트코인을 가지고 있는 사람으로부터 양도를 받을 수 있고, 공식 거래소에서 살 수 있다. 이처럼 비트코인은 변동성이 매우 높기 때문에 암호화폐의 원래 목적인 유통보다는 오래전 금처럼 투기를 위한 소유의 목적으로 지금은 주로 활용되고 있다.

비트코인의 일반 참여자들은 공개키 쌍을 가지고 있어야 하지만 인증서 기반을 사용하지 않고 있다. 한 참여자는 여러 개의 공개키 쌍을 사용할 수 있다. 동일 공개키만 계속 사용하면 불연결성이 제공되지 않기 때문에 강한 프라이버시를 제공할 수 없다. 각 참여자의 공개키는 비트코인의 주소(지갑의 주소) 역할을 한다. 특정 다른 참여자에게 비트코인을 양도하고 싶으면 한기코인처럼 해당 참여자의 공개키(지갑의 주소)를 알아야 한다. 따라서 거래 과정에서 지불자는 자신이 생각하는 상대방의 올바른 주소를 알아야 한다. 이렇게 양도된 코인은 해당 참여자의 개인키가 있어야 사용할 수 있다. 이 방식의 가장 큰 문제점은 참여자가 자신의 개인키를 분실하게 되면 가지고 있던 해당 키와 연결된 모든 코인을 더는 사용할 수 없게 된다는 것이다. 따라서 개인키의 안전한 백업이 매우 중요하다. 현재 비트코인 지갑은 비트코인 노드 운영을 위한 소프트웨어와 달리 다양한 업체가 다양한 형태로 만들어 제공하고 있다. 인터넷에 연결되어 있는 지갑을 핫지갑이라 하고, 연결되어 있지 않은 지갑을 콜드지갑이라 한다. 인터넷에 계속 연결되어 있으면 해킹 위험에 노출될 수 있다.

비트코인의 기본적 생각은 앞서 설명한 한기코인과 같다. 각 참여자는 전자서명하여 지불 의사를 표현하고, 이 거래 명세는 네트워크에 있는 모든 참여자에게 전달된다. 이처럼 비트코인을 이용한 모든 지불은 공개된다. 각 참여자는 자신이 받은 거래의 서명값과 같은 기본적인 유효성을 확인하며, 유효하지 않은 것은 중계하지 않는 것이 원칙이다. 모든 거래는 전체 참여자에게 전파되지만, 그 즉시 거래가 확정되는 방식이 아니다. 비트코인의 참여자 중 일부는 아직 확정되지 않은 거래를 수집하며, 현재 수집된 미확정된 거래를 모아 블록[6]이라는 것을 만든다.

비트코인은 P2P 네트워크를 사용한다. P2P 네트워크에서 한 사용자가 전체 네트워크에 있는 모든 사용자에게 메시지를 전파할 때 가장 널리 사용하는 프로토콜은 **가십**(gossip) 프로토콜이다. 이 프로토콜에서 한 참여자가 전체 네트워크에 메시지를 보내고 싶으면 일정한 횟수만큼 주기적으로 $k(\geq 2)$명의 다른 참여자를 랜덤하게 선택하여 메시지를 전송한다. 이 메시지를 수신한 노드들은 같은 과정을 반복하여 전체 네트워크로 메시지를 전파한다. 한 주기에 선택하는 수신자의 수가 1명이어도 n 주기가 지나면 총 2^n명에게 도달한다.

비트코인에서 각 사용자는 완전 노드(full node)를 운영할 수 있고, 부분 노드(lightweight, partial node)를 운영할 수 있다. 완전 노드는 최초 블록(genesis block)부터 지금까지의 모든 블록에 포함된 트랜잭션 정보를 유지해야 하며, 수신된 모든 거래의 유효성을 확인할 의무가 있다. 이 때문에 비트코인의 블록체인을 다른 말로 분산 원장이라 한다. 반면에 부분 노드만 운영하면 본인의 거래를 위해 필요한 최소의 정보만 유지하면 된다. 하지만 P2P라는 원리 측면에서 보았을 때 모든 참여자가 대칭적 역할을 하는 것이 공정하다고 볼 수 있다. 또 완전 노드들이 모두 블록이라는 것을 생성하여 확정하지는 않는다. 채굴자들이 블록을 생성하고 확정하며, 채굴자는 반드시 완전 노드를 운영해야 한다.

완전 노드가 비트코인의 P2P 네트워크의 실질적 노드이며, 충분한 수의 완전 노드가 동작하고 있어야 비트코인이 정상적으로 동작하게 된다. 비트코인 참여자들이 완전 노드를 운영할 동인은 어디에 있는가? 첫째, 채굴자, 거래소 등은 완전 노드를 운영할 수밖에 없다. 둘째, 다른 완전 노드에 의존하지 않고 안전하게 비트코인을 거래하고자 하면 완전 노드를 운영해야 한다. 더욱이 완전 노드를 운영하는 것이 프라이버시 측면에서도 효과적이다. 셋째, 완전 노드를 운영하면 비트코인 운영 관련 투표권을 얻게 된다.

비트코인은 한기코인처럼 기본 거래 단위가 있으며 이를 트랜잭션이라 한다. 한 트랜잭션은 입력, 출력으로 구성

[5] 1 satoshi는 0.00000001 BTC이므로 오늘날 시세(3천만원)를 고려하면 약 0.3원이다.
[6] 블록체인에서 블록은 같은 시점에 블록체인에 포함된 거래들의 집합을 말한다.

되며, 다중 입력과 다중 출력이 가능하다. 각 입력마다 별도 서명이 트랜잭션에 포함되어야 한다. 심지어 같은 지갑 소유의 두 개의 UTXO를 이용하여 입력을 구성하더라도 두 개의 서명이 필요하다. 비트코인 거래에서 입력 금액의 합은 출력 금액의 합보다 같거나 커야 한다. 같지 않을 경우 그 차액은 수수료가 되며, 거래를 확정시킨 채굴자가 이 수수료를 가지게 된다. 비트코인은 지불자가 가지고 있는 코인이 바로 수취인에게 전달되는 형태이기 때문에 push 지불 방식에 해당한다. 반면에 신용카드처럼 중재자가 지불자의 계정에서 금액을 인출하여 수취인에게 전달하는 형태의 지불 방식은 pull 지불 방식에 해당한다.

2.2.1 탈중앙 암호화폐, 실제 가능한 것인가?

거래 정보를 공개하는 방법으로 탈중앙 암호화폐를 실현하기 위해서는 화폐 발행 문제, 거래 위조 문제, 이중 사용 문제 등이 해결되어야 한다. 특히, 화폐 발행은 탈중앙 기법을 통해 발행되어야 하며, 지불은 신뢰 기관 없이 승인될 수 있어야 탈중앙 암호화폐라 할 수 있다.

한기코인과 마찬가지로 특정 비트코인을 사용하기 위해서는 그 비트코인을 유지하고 있는 지갑의 개인키가 필요하기 때문에 다른 사용자의 개인키를 확보하지 못하면 거래를 위조할 수 없다. 거래의 유효성이 확인된 거래만 공개되며, 공개된 거래를 수정할 수 없어서 이중사용은 가능하지 않다. 이것을 제공하기 위해 사토시 나카모토가 사용한 기술이 블록체인이다[3]. 블록체인은 그것이 필요한 기능을 제공하기 위해 분산 합의 기술을 사용하며, 분산 합의 기술에는 해당 응용에서 필요한 규칙과 그 규칙의 준수를 위한 보상책 또는 규칙을 어길 때 발생하는 불이익이 포함된다. 블록체인은 사토시 나카모토가 최초로 제안한 기술은 아니지만, 분산 암호화폐를 실현한 것은 사토시 나카모토가 처음이다.

2.2.2 블록체인을 이용한 조작불가능성

공개된 트랜잭션에 대한 조작(수정, 삭제)이 가능하지 않아야(tamper-proof) 이중 사용을 방지할 수 있다. 앞서 설명한 바와 같이 각 사용자는 전자서명하여 트랜잭션을 생성하며, 생성된 트랜잭션은 분산 원장에 기록된다. 이것이 어떻게 기록되는지는 나중에 다루고, 여기서는 공개된 원장의 **불가역성**(immutability)을 보장하는 기술을 살펴보자. 원장에 기록된 트랜잭션은 기본적으로 전자서명되어 있으므로 지불자를 제외한 다른 사용자들은 이 트랜잭션을 수정할 수 없다. 따라서 비트코인에서 요구하는 것은 서명자를 포함하여 누구도 원장에 공개된 트랜잭션을 수정, 삭제할 수 없어야 한다. 즉, 원장에는 데이터를 추가만 할 수 있고 수정, 삭제할 수 없어야 한다. 더욱이 비트코인은 신뢰하는 기관을 이용하지 않기 때문에 이것을 보장하는 것이 간단한 문제가 아니다.

블록체인에 사용된 기술을 이해하기 위해 먼저 무결성을 보장하는 기법들을 간단히 살펴볼 필요가 있다. 보통 무결성을 보장하기 위해 많이 사용하는 암호기술은 해시함수, MAC, 전자서명이다. 해시함수는 누구나 쉽게 데이터를 바꾸고 그것의 해시값을 바꾸어 무결성을 보장하고자 하는 데이터를 조작할 수 있다. MAC은 MAC키를 가지고 있지 않으면 수정이 가능하지 않기 때문에 MAC을 사용하는 것을 고려해 볼 수 있으나 키가 없으면 확인도 할 수 없으므로 공개된 자료의 무결성을 보장하기 위해 사용할 수 있는 기술은 아니다.

전자서명은 MAC과 달리 서명키를 소유한 사용자만 생성할 수 있고, 이 키가 없으면 데이터를 바꾸는 것이 가능하지 않다. 더욱이 공개키만 공개하면 누구나 데이터의 무결성을 확인할 수 있다. 중앙집중 신뢰 기관을 사용한다고 생각하고, 이 기관은 일정한 수의 유효한 트랜잭션들을 모아 전자서명하여 공개한다고 하자. 이 경우에는 이 신뢰 기관을 제외하고는 누구도 공개된 자료를 수정 및 삭제하는 것이 어렵다. 하지만 이와 같은 방식은 탈중앙 암호화폐에 맞는 기술은 아니다. 더욱이 이 신뢰 기관은 막강한 권한을 가지게 된다. 특히, 이 기관은 기존에 포함된 트랜잭션을 삭제할 수 있고, 일부 트랜잭션을 포함하는 것을 거부할 수 있으며, 새로운 것을 이전 공개한 자료에 포함할 수 있다. 물론 이와 같은 문제 때문에 실제 신뢰할 수 있는 기관이 이 역할을 해야 하지만 비트코인은 이와 같은 기관을 사용하지 않고 블록체인이라는 기술을 사용하여 탈중앙 방식으로 원장의 불가역성을 제공하고 있다.

비트코인에서는 해시함수 기반 암호 퍼즐을 사용하는 기술을 사용하여 불가역성을 보장하고 있다. 암호 퍼즐은

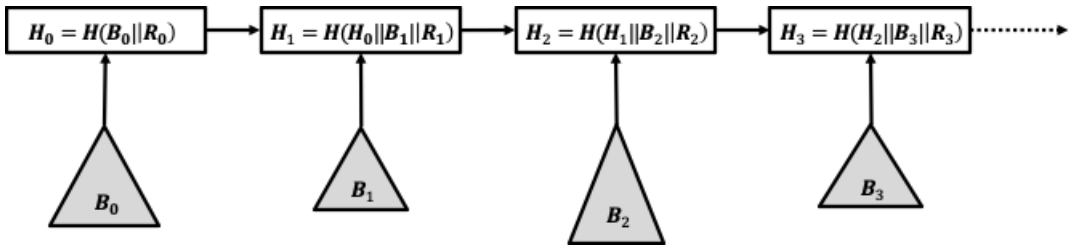
해결하기 어렵지만, 답을 확인하기는 매우 쉽다는 비대칭적 특성이 있으며, 해결하는 방법은 모든 경우를 다 해보는 방법(brute-force)밖에 없어야 한다. 비트코인에서 각 트랜잭션은 지불자의 서명키로 전자서명하여 공개되며, 전자서명된 트랜잭션들을 모아 블록을 만들고, 이 블록의 해시값을 계산하여 공개한다. 즉, 비트코인은 라운드라는 개념을 사용한다. 특정 기간에 이루어진 모든 전자서명된 트랜잭션들을 블록이라는 문서로 통합하여 공개하게 된다.

해시함수만 사용하면 앞서 언급한 것처럼 누구나 블록에 있는 트랜잭션의 내용을 수정하거나 삭제한 후에 해시값을 생성하여 블록을 수정할 수 있다고 생각할 수 있다. 하지만 개별 거래는 전자서명되어 있어서 블록체인 기술과 상관없이 지불자의 개인키가 없으면 수정할 수 없다. 반면 삭제나 추가는 블록에 대한 단순 해시값만 공개한다면 누구나 쉽게 할 수 있다. 이 때문에 블록체인에서는 해시값을 계산할 때 블록값만 포함하여 해시하지 않고 랜덤값을 포함하여 해시하여야 하며, 이 해시값이 유효한 해시값이 되기 위해서는 해시값의 첫 몇 개의 비트 값들이 모두 0이 되어야 한다[7]. 이를 위해 이 값을 얻을 때까지 블록에 포함될 거래 내용을 고정한 상태에서 랜덤값을 바꾸어 가면서 계속 시도하게 된다. 이 때문에 이를 암호 퍼즐이라 한다.

0이 되어야 하는 비트값의 개수를 조절하여 이 해시값을 계산하는 데 필요한 시간을 조절할 수 있다. 현재 2,016 블록마다(약 2주마다) 난이도를 조절하고 있다. 예를 들어 첫 비트만 0이 되어야 하면 보통 2번의 해시값 계산만으로 찾을 수 있고, 첫 n개의 비트가 모두 0이 되어야 하면 보통 2^n번의 해시값을 계산하면 찾을 수 있다. 암호 퍼즐을 해결하는 데 필요한 시간이 10분 정도 소요되도록 현재 비트코인에서는 첫 76bit가 0이 되어야 한다. 다음은 2022년 5월 7일에 확정된 735,277번째 블록의 해시값이다.

00000000000000000000890f722fab7e37c783b82da48529affc18fc7974d956c

이처럼 특정한 노력을 해야 값을 얻을 수 있어서 이를 **작업 증명**(PoW, Proof-of-Work)이라 한다. 작업 증명은 Adam Back이 스팸 메일을 제한하기 위해 처음 사용하였으며, 용어는 Jakobsson과 Juels가 처음 사용하였다[4].



<그림 15.5> 비트코인 블록체인

비트코인에서 특정 라운드에서 해결해야 하는 암호 퍼즐을 성공적으로 계산한 사용자는 새 비트코인을 얻을 수 있다. 이 때문에 이 퍼즐을 해결하는 것을 **채굴**(mining)이라 한다. 그러면 누구나 채굴기를 구입하여 10분 정도를 투자하면 블록 값을 수정할 수 있다고 생각할 수 있다. 하지만 블록을 독립적으로 계산하지 않고 이전 블록의 해시값을 포함하여 계산한다. 따라서 그림 15.5와 같이 최초 블록부터 지금의 블록까지 순차적으로 연결된 형태가 되며, 이 때문에 이것을 블록체인이라 한다.

체인 형태로 엮여 있으므로 중간 블록에 있는 값을 수정하면 그 이후 모든 블록을 다시 계산해야 한다. 또한 비트코인의 특성 때문에 블록의 생성은 중단없이 계속 생성된다. 따라서 특정 블록을 수정하고 그 이후 모든 블록을 수정하고자 하더라도 현재 블록보다 더 긴 길이의 체인을 만드는 것은 가능하지 않다. 이 때문에 블록체인은 불가역적이고 첨삭만 가능(append-only)하다고 하는 것이다.

참고로 블록에 포함될 모든 거래를 연속적으로 결합하여 해시하는 것은 아니고 모든 거래를 머클 해시 트리로 구성하여 이 트리의 루트값만 블록의 해시값을 계산할 때 사용한다. 즉, 기본적으로 블록값은 이전 블록값, 거래를 구성한 해시트리의 루트값, 그리고 랜덤값 3가지 값을 이용하여 계산한다. 또 해시트리를 구성할 때 채굴자는 자신에게 규칙에서 정한 금액값의 새 코인(coinbase transaction)과 거래들에 있는 수수료를 자신에게 지불하는 거래를

[7]실제는 해시값을 정수로 생각하고 시스템에서 정한 특정 수 이하의 값이 나오면 유효한 해시값이 된다.

포함한다. 이를 통해 비트코인에서 새 화폐들이 발행된다. 이와 같은 보상을 받기 위해 채굴자는 정직하게 행동하게 된다.

비트코인 안전성에 중요한 요소 중 하나는 유효한 트랜잭션만 블록에 저장되어야 한다는 것이다. 채굴에 성공한 채굴자는 그 사실을 전체 네트워크에 알리게 된다. 완전 노드를 포함한 다른 채굴자는 채굴자가 전송한 블록의 내용을 확인하여 블록이 유효한 경우에만 해당 블록을 다음 블록으로 인정한다. 다음 블록으로 인정되어야 보상을 받을 수 있기 때문에 유효하지 않은 트랜잭션을 포함하여 블록을 만들 이유가 없다.

블록체인과 관련하여 한 가지 더 고려해야 하는 점은 암호 퍼즐은 확률적 알고리즘[8]으로 해결하는 것이기 때문에 우연히 두 명의 채굴자가 거의 동시에 채굴에 성공할 수 있다. 이처럼 체인이 2개 이상의 갈래로 나누어지면 일시적 **포크**(fork)가 발생하였다고 한다. 하지만 이것이 계속해서 발생하는 것은 확률적으로 매우 어렵다. 암호퍼즐에 해결하는데 소요되는 시간을 10분으로 조정한 이유도 이와 관련되어 있다. 난이도가 낮을수록 우연히 동시에 해결할 확률은 높아진다.

비트코인에서는 일시적 포크 문제를 해결하기 위해 **가장 긴 체인을 우선하는 규칙**을 사용하고 있다. 채굴자가 암호퍼즐을 해결하였어도 해결한 블록이 현재 가장 긴 체인에 포함되지 않으면 해당 채굴자는 어떤 보상도 받을 수 없다. 따라서 채굴자는 보상을 받기 위해 이 규칙에 따라 현재 가장 긴 체인에 있는 마지막 블록을 이용하여 다음 블록을 만들게 된다. 이와 같은 이유로 비트코인의 작업 증명 프로토콜은 일시적으로 합의가 깨질 수 있으나 가장 긴 체인 우선 원칙에 의해 다시 하나의 블록체인으로 쉽게 합의하게 된다.

가장 긴 체인 우선 원칙에 따라 자신의 거래가 포함된 블록의 깊이가 6 이상이 되면 안전하게 확정되었다고 간주하며, 채굴된 새 코인의 경우에는 깊이가 10 이상이 되어야 사용할 수 있도록 하고 있다. 비트코인에서는 전파속도를 고려하여 블록 크기를 1MB로 제한하고 있다. 따라서 한 블록에 최대 포함할 수 있는 트랜잭션 수가 제한되어 있다. 그러므로 현재 거래량이 많으면 자신의 거래가 이번 라운드에 포함되지 않을 수 있고, 거래를 블록에 포함할지는 채굴자가 결정하는 것이기 때문에 언제 포함될지 특정하기 어렵다. 긴 기간 동안 포함되지 않으면 노드들은 이 거래를 삭제하며, 코인의 소유자는 거래를 다시 생성하여 해당 코인을 다시 사용할 수 있게 된다.

더 많은 비용을 투자하여 채굴 장비를 구축하여 채굴하면 채굴에 성공할 확률이 높아지며, 실제로 전 세계에 채굴에 사용되는 컴퓨팅 파워의 51% 이상을 특정 채굴자가 제어할 수 있다면 이 채굴자는 블록체인을 마음대로 조작할 수 있다. 하지만 아직 비트코인에서는 이와 같은 문제가 발생하지 않고 있으며, 이 때문에 현 블록체인 채굴 생태계가 건전하다고 말한다. 물론 현재는 소위 말하는 큰 손들이 전체 채굴 파워의 많은 부분을 점유하고 있다. 비트코인 외에 다른 암호화폐의 경우에는 51% 공격이 실제 발생한 사례가 있다[5, 6]. 모나코인의 경우 57% 해시 파워를 획득한 채굴자가 블록의 암호 퍼즐을 해결하고도 공개하지 않고 계속 채굴하다가 어느 시점에 이것을 공개하여 이중 사용하는 공격(block withholding attack, selfish mining attack)이 있었다.

2.2.3 채굴

누가 채굴하나? 비트코인에서는 누구든지 원하면 채굴할 수 있다. 또 아무도 채굴하지 않는다면 비트코인은 더는 동작하지 않는다. 그러면 왜 사람들은 채굴자가 될까? 이것은 보상이 있기 때문이고, 채굴자가 채굴 시스템을 구축하는 데 든 비용과 이 시스템을 운영하는데 드는 비용보다 이 보상이 커야 한다. 채굴 시스템을 운영하는 비용에는 전기세, 시설 운영비, 인건비 등이 포함된다. 특히, 많은 계산량 때문에 장비 냉각에 많은 비용이 소요되기 때문에 추운 지방에 채굴 시설을 구축하거나 전기세가 저렴한 국가에 채굴 시설을 구축하는 경우가 많다. 비트코인에서 채굴자가 채굴에 성공하면 수수료[9]와 새 비트코인을 받을 수 있다. 지금까지는 이것이 충분한 보상이 되기 때문에 건전한 채굴 생태계가 형성되었다고 볼 수 있으며, 이와 같은 이유로 비트코인 가격이 현재의 수준을 유지(채굴자들이 기대하는 수준이 되어야 함)하고 있다고 볼 수 있다.

[8] 채굴자가 난스를 모두 0부터 차례로 검사하는 것은 아니며, 앞에 요구하는 수의 0이 나오는 난스가 하나만 존재하는 것이 아니다.

[9] 현재 적정 수준의 트랜잭션 수수료는 트랜잭션 크기에 비례하며, 1 byte 당 108 satoshi이다. 이론적으로 한 블록이 1 MB이면 수수료는 최대 1 BTC가 될 수 있다.

사토시 나카모토는 비트코인의 수가 무한정 계속 증가하면 그 가치를 유지하기 어렵다고 판단하여 일정 시점이 되면 새 비트코인을 생성하지 않도록 하였으며, 이를 위해 일정 주기(약 4년)마다 암호 퍼즐을 해결하였을 때 새롭게 발행하는 코인의 수를 반으로 줄이고 있다. 최근 2020년 5월 12일에 보상으로 주어지는 비트코인 수가 6.25 BTC로 줄었다. 현재 시세를 고려하여 1BTC가 약 5,000만원이라고 가정하면 10분에 누군가 약 삼억천이백오십만원 정도의 수입을 얻게 되는 것이다. 총 발행될 비트코인의 수는 21,000,000개이며, 2022년 5월 기준으로 이미 전체 발행될 코인수의 약 90%이상이 발행된 상태이다. 2032년이 되면 발행될 비트코인의 99%가 발행되게 되며, 2140년이 되면 발행이 완전히 종료될 것으로 예측되고 있다. 2032년 이후가 되면 블록마다 발행되는 코인의 수가 1BTC 이하가 될 것이며, 이 경우에는 채굴자들의 보상 수익이 채굴자의 기대에 못 미칠 수 있다[10]. 더욱이 수수료는 강제화되어 있는 것이 아니기 때문에 어떤 현상이 나타날지는 예측하기가 어렵다. 그럼에도 불구하고 사토시 나카모토의 천재성을 부인하기는 어렵다. 사토시는 비트코인이 만약 성공한다면 어떤 과정으로 성공할 것인지를 확실히 예측하고 비트코인을 설계하였다고 볼 수 있다.

사토시 나카모토는 원래 사람들이 자신의 개인 컴퓨팅 파워를 이용하여 채굴할 것으로 생각하였다. 실제 초창기에는 사토시와 그의 몇 친구들만 그들의 가용 컴퓨터를 이용하여 비트코인을 채굴하였다. 하지만 비트코인에 대한 가치가 점점 높아짐에 따라 채굴자들도 점점 늘어났다. 그리고 이들은 더욱 효과적으로 채굴할 수 있는 방법을 찾게 되었다. 이때 등장한 것이 GPU 채굴 방법이다. 이 방법도 FPGA(Field-Programmable Gate Arrays)를 이용한 채굴 방법이 등장하면서 뒤로 밀렸으며, 지금은 ASIC(Application Specific Integrated Circuit)을 이용하는 방법이 가장 많이 사용되고 있다. ASIC 관련 하드웨어 업체들 입장에서 보면 생각하지 못한 매우 큰 새로운 시장이 등장한 것이 된다. 또 초기에는 한 집단이 자체 시설(이를 채굴 농장(mining farm))을 만들어 채굴하였지만 지금은 여러 집단이 채굴 풀(mining pool)을 형성하여 함께 채굴하고, 채굴에 성공하면 보상을 나누어 가지는 방식을 사용하고 있다. 또 채굴을 할 수 있는 장비를 구축하고 이를 대여하여 주는 채굴 클라우드 서비스도 등장하였다.

비트코인에서 사용하는 작업 증명 방식은 블록체인 안전성에 매우 중요한 요소이지만 전기 소비로 인한 환경 파괴가 심각하다는 지적에 따라 최근에는 작업 증명 외에 다른 방법을 찾고 있으며, 이 중 하나가 **지분 증명**(PoS, Proof-of-Share) 방식이다. 이에 대해서는 16장에서 자세히 설명한다. 비트코인에서 사용하는 작업 증명의 또 다른 문제는 확정 속도이다.

2.2.4 하드 포크, 소프트 포크

비트코인은 P2P 시스템이기 때문에 모든 노드가 같은 버전의 소프트웨어를 사용하도록 강제화하기가 쉽지 않다. 따라서 노드들이 다른 버전의 SW를 사용하여도 시스템은 문제없이 동작해야 한다. 비트코인에서는 소프트웨어 업그레이드는 다른 소프트웨어처럼 소프트웨어 결함을 해소하기 위한 이유도 있지만, 규칙을 바꾸기 위해 소프트웨어가 업그레이드되는 경우가 더 많다. 특히, 트랜잭션 검증 규칙, 블록 구성 규칙 등의 일관성은 반드시 유지되어야 한다.

규칙 변경 측면에서 이 문제를 살펴보자. 규칙 변경은 크게 다음 2가지로 나누어 볼 수 있다.

- 경우 1. 과거와 호환되지 않는 규칙의 도입
- 경우 2. 과거와 호환되는 규칙의 도입

경우 1를 하드 포크라 하고, 경우 2를 소프트 포크라 하며, 둘 다 블록체인이 두 갈래로 나누어질 수 있으며, 각 갈래가 계속 유지될 수 있는 문제점이 있다. 이 2가지 경우 어떤 문제가 발생하는지 살펴보기 위해 두 개의 노드 A와 B 입장에서 살펴보자. 여기서 A는 이전 규칙을 사용하는 노드이고, B는 새 규칙을 사용하는 노드라 하고, 블록 구성에 관한 규칙이 변경되었다고 하자.

[10] 지금도 이미 채굴 보상이 투자 대비 작다고 한다. 하지만 채굴을 중단하면 비트코인의 가치하락으로 더 큰 손해를 볼 수 있어, 채굴을 쉽게 중단하기도 어렵다.

먼저 경우 1을 생각하여 보자. 간단하게 블록 크기를 1MB에서 2MB로 높였다고 하자. A는 B가 생성한 새 블록을 인정할 수 없다. 이때 A와 같은 입장의 노드들과 B와 같은 입장의 노드들이 계속 독자적으로 블록들을 만들었다고 하면 블록체인이 2가지 갈래로 나누어지게 된다. 이 갈래를 다시 하나로 합치기는 쉽지 않다. A와 같은 입장의 노드들이 새 규칙을 인정하고 포크된 이후 그들의 갈래를 통해 발생한 모든 이익을 포기해야 한다. B와 같은 입장의 노드들은 새 규칙이 필요하다고 생각하는 집단이므로 이들이 A 갈래로 합치기도 쉽지 않다. 이 때문에 두 갈래가 계속 유지되는 현상을 하드 포크라 한다.

경우 2는 경우 1과 반대로 블록 크기를 축소하는 것을 예로 생각해 볼 수 있다. A와 같은 입장의 노드들은 자신들이 생성한 블록은 물론 B가 생성한 블록들도 인정할 수 있다. 반면에 B와 같은 입장의 노드들은 A가 생성한 블록들을 인정할 수 없다. 즉, 소프트웨어를 업그레이드하지 않은 노드들도 규칙 변경이 적용된 블록을 인정할 수 있다. 이와 같은 이유로 두 갈래가 유지되는 것을 소프트 포크라 한다. 하지만 소프트 포크는 하드 포크와 비교하여 A와 같은 입장의 노드들이 B 쪽으로 합쳐지는 것이 상대적으로 쉬울 수 있다. 물론 이와 같은 통일이 일어나기 위해서는 B와 같은 입장의 노드들이 다수이어야 한다.

하드 포크이던 소프트웨어포크이던 블록체인은 그것의 기술과 상관없이 언제든 불가역성이 보장되지 않을 수 있다는 것을 의미한다. 다수의 참여자들이 동의하면 하지 못할 것은 아무것도 없다.

2.3 비트코인의 개선

비트코인도 최초 사토시 나카모토가 제안한 형식 그대로 지금까지 유지되는 것은 아니다. 조금씩 기술적 발전을 하고 있다.

2.3.1 세그윗

세그윗(segwit)은 비트코인의 블록 크기 제한 문제를 극복하기 위해 도입된 기술이다. 비트코인은 전파속도를 고려하여 블록의 크기를 1MB로 제한하였다. 이 블록을 구성하는 데이터는 트랜잭션이며, 트랜잭션의 내용 중 가장 많은 부피를 차지하는 것이 전자서명 값이다. 세그윗은 트랜잭션의 내부 내용 중 전자서명 값을 블록에서 분리하여 별도 유지한다. 이렇게 하면 1MB의 블록 크기에 더 많은 트랜잭션을 포함할 수 있다. 서명값들은 별도 머클 해시 트리로 구성하여 코인베이스 트랜잭션에 포함하는 방법을 사용하고 있다. 세그윗은 2015년에 처음 제안되었고, 소프트 포크를 통해 2017년 8월에 도입되었다. 이 이후 블록 크기를 2MB로 확장하는 Segwit2x를 2017년 11월에 하드 포크로 도입하기로 하였다가 여러 반대로 도입을 포기하였다.

2.3.2 2계층 기술

비트코인에서 사용하는 블록체인 자체를 수정하지 않고 블록체인의 성능을 개선하는 방법도 있다. 이와 같은 기술을 2계층(layer 2) 블록체인 기술이라 한다. 현재 다양한 2계층 기술이 개발되고 있다. 이 절에서는 이와 같은 기술 중 **지불 채널**(payment channel)에 대해 살펴본다. 지불 채널은 두 사용자 간에 연속된 거래가 진행될 경우 모든 거래 내용을 블록체인에 꼭 저장할 필요가 없다는 점을 이용하는 기술이다. 예를 들어 A가 B에게 0.01BTC를 다섯 번 지불한 경우 A가 B에게 0.05BTC를 지불한 트랜잭션 하나만 기록하면 된다. 채널을 사용하여 거래를 하게 되면 수수료를 절약할 수 있으며, 트랜잭션 처리 속도를 향상할 수 있다. 특히, 비트코인은 수수료 때문에 보통의 수수료보다 적은 금액을 거래하는 것이 힘들다. 하지만 지불 채널을 이용하면 소액 지불이 가능하다. 지불 채널을 이해하기 위해서는 비트코인 관련 지금까지 설명하지 않은 몇 가지 내용을 먼저 이해해야 한다.

첫째, 비트코인 지갑은 **다중 서명 지갑**을 지원한다. 보통 비트코인 지갑은 하나의 공개키 쌍과 연결되어 있지만 다중 서명 지갑은 여러 개의 공개키를 임계 기반 형태로 지갑과 연결하여 사용할 수 있다. 2-2 다중 서명 지갑을 만들어 서로 다른 두 개의 개인키를 이용하여 트랜잭션에 서명해야 지갑이 보유한 비트코인을 양도할 수 있도록

<표 15.1> 비트코인 잠금의 종류

	절대	상대
트랜잭션 수준	nLockTime	nSequence
UTXO 수준	CLTV(Check LockTime Verify)	CSV(Check Sequence Verify)

만들 수 있다. 또 2-3 다중 서명 지갑을 만들고, 3개의 개인키 중 하나는 백업키로 설정할 수 있다. 이 경우 3개의 키 중 어떤 2개의 조합만 있으면 지갑의 비트코인을 사용할 수 있게 된다.

둘째, 비트코인은 시간 잠금 기능이 있다. 일정 시간이 지나야 트랜잭션 또는 트랜잭션의 출력을 사용할 수 있도록 제한할 수 있다. 여기서 시간은 실제 시간일 수 있고, 블록 높이일 수 있다. 또 절대적, 상대적 개념이 모두 가능하다. 예를 들어 T_1, T_2 두 개의 트랜잭션이 있고, T_2 트랜잭션은 T_1 트랜잭션의 출력을 사용하는 트랜잭션이라 하자. T_2 트랜잭션 입력의 nSequence 값을 10으로 설정하면 T_2 트랜잭션은 T_1 트랜잭션이 등록된 이후 10개 블록이 지나야 블록체인에 등록이 될 수 있다. 잠금이 된 트랜잭션은 잠금이 해제되기 전에 같은 입력을 이용한 트랜잭션이 등록되면 잠겨있던 트랜잭션은 잠김이 해제되어도 이중 사용으로 사용할 수 없게 된다.

비트코인에는 현재 표 15.1처럼 총 4종류의 시간 잠금 기능이 있다. nLockTime과 nSequence는 트랜잭션 수준에 해당하며, 트랜잭션의 블록 등록을 지연해주는 역할을 한다. 따라서 이와 같은 잠금이 설정된 트랜잭션은 잠금이 해제될 때까지 채굴 블록에 포함할 수 없다. CLTV와 CSV는 UTXO 수준이며, 특정 UTXO의 사용을 지연해주는 역할을 한다. 즉, 이 UTXO를 사용하는 트랜잭션의 채굴을 지연하여 준다.

셋째, 해시 시간 잠금(HTLC, Hash TIme Locked Contracts) 기능도 있다. 이 잠금은 트랜잭션에 포함된 해시값의 입력을 함께 제시해야 트랜잭션을 블록에 저장할 수 있다. 이 잠금은 만료 시간이 있어 만료 시간 전에 해시값의 입력이 제시되어야 하며, 그 후에는 이 트랜잭션은 무조건 무효화되어 입력의 원 소유자는 그것을 다른 지불에 사용할 수 있다.

지불 채널은 다중 서명 지갑과 시간 잠금을 이용하는 2자간 오프 체인 지불 방법이다. 오프 체인이란 2자간 비트코인 트랜잭션을 교환하여 거래를 진행하지만 이 트랜잭션들을 블록체인에 등록하지 않는다. 채널을 개설할 때와 종료할 때 두 번만 블록체인에 저장하고, 그 사이에 진행된 거래는 블록체인에 등록하지 않는다. 채널의 개설은 2-2 다중 서명 지갑을 만드는 것이고, 이 지갑에 두 사용자 모두 또는 두 사용자 중 한 명만 비트코인을 예치하게 된다. 채널이 개설되면 이 지갑에 있는 비트코인은 두 사용자 모두가 동의해야 사용할 수 있다. 따라서 개설할 때 여러 가지 추가 조치가 없으면 예치된 돈을 부당하게 잃어버릴 수 있는 가능성이 있다. 예를 들어 A와 B가 0.5BTC를 각각 예치하여 채널을 개설하고자 하면, 이 채널에서 초기 예치금 0.5BTC를 회수할 수 있도록 해주는 트랜잭션에 서명하여 서로 교환한 후에 채널 개설을 완료해야 한다. 이 트랜잭션을 보통 패널티 트랜잭션이라 하며, 패널티 트랜잭션은 시간 잠금이 되어 있어, 서로 불법적 회수를 시도할 수 없다. 정상적으로 채널을 닫으면 패널티 트랜잭션은 이중사용이 되기 때문에 사용할 수 없게 된다.

패널티 트랜잭션의 시간 잠금은 nLockTime을 이용할 수 있고, CLTV를 이용할 수 있다. nLockTime은 패널티 트랜잭션 자체를 잠금하는 것이고, CLTV는 패널티 트랜잭션 자체가 아니라 패널티 트랜잭션 출력을 잠금하는 것이다. 둘 다 가능하지만 nLockTime은 트랜잭션 가단성(malleability) 공격에 취약할 수 있어 CLTV를 이용하는 것을 더 선호한다. 트랜잭션 가단성 공격이란 내용이 같은 해시값이 다른 두 개의 트랜잭션을 만들어 공격하는 것을 말한다.

채널 개설이 완료되면 A와 B는 유효한 블록체인 트랜잭션을 만들어 서로 교환하게 된다. 예를 들어 0.01BTC를 여러 차례 A와 B간에 교환할 수 있다. 0.01BTC가 교환될 때마다 채널의 상태는 바뀌며, 채널의 상태를 나타내는 트랜잭션이 만들어진다. 따라서 두 사용자는 다양한 상태를 나타내는 트랜잭션을 얻게 된다. 원칙적으로 최종 상태로 채널을 닫아야 하지만 본인에게 좀 더 유리한 상태로 채널을 닫는 시도를 할 수 있다. 이와 같은 시도도 초기에 교환된 패널티 트랜잭션이나 중간에 추가로 교환한 패널티 트랜잭션을 통해 어느 한 사용자가 부당한 이득을 취할

수 없도록 만들 수 있다.

사용자 A가 여러 사용자와 소액 거래를 하고 싶을 때 각 사용자마다 지불 채널을 만드는 것은 번거로울 수 있다. A가 B와 지불 채널이 개설되어 있고, B와 C가 지불 채널이 개설되어 있다면 A는 C와 지불 채널을 개설하지 않고 B를 이용하여 C에게 지불할 수 있다. 이것을 **지불 채널 네트워크**(PCN, Payment Channel Network)라 한다. 대표적인 지불 채널 네트워크가 라이트닝 네트워크이다. 이 네트워크는 A가 특정 사용자에게 비트코인 거래를 하고 싶을 때 지불 채널들을 이용하여 지불 채널 네트워크를 구축해 준다. 지불 채널 네트워크에서 가장 큰 문제는 중간 사용자가 중계를 멈추고 채널을 닫아 부당한 이득을 취하고자 할 수 있다. 이 문제는 HTLC를 이용하여 해결한다. A는 최종 수신자로부터 해시값을 받아 트랜잭션에 포함하여 지불 채널 네트워크를 이용하게 된다. 중간 노드들은 해시 잠금 때문에 포함된 해시값의 입력값이 없으면 받은 비트코인을 얻을 수 없게 된다. 최종 수신자는 입력 값을 알기 때문에 입력 값을 공개하여 트랜잭션을 마무리하면 중간에 있는 노드들도 차례로 마무리할 수 있게 된다.

2.4 비트코인 블록체인의 특성

비트코인 블록체인의 특성은 다음과 같다.

- 특정 1. 지속해서 끊임없이 계속 생성되어야 한다.

  비트코인에서는 10분마다 하나의 블록이 생성된다. 누구나 블록 생성에 참여할 수 있으며, 블록의 생성은 영원히 끊임없이 계속되어야 한다. 사토시 나카모토가 고안한 보상체계 때문에 아직까지는 문제없이 계속 생성되고 있다.

- 특징 2. 기록된 것은 변경할 수 없으며, 첨삭만 가능하다.

  전자서명 기술 때문에 입력 소유자 외에는 기존 트랜잭션 내용을 수정할 수 없지만, 트랜잭션의 삭제나 추가는 블록에 포함되는 머클 해시 트리를 재구성하여 누구나 시도할 수 있다. 특정 블록을 수정하기 위해 암호 퍼즐을 성공적으로 계산하여도 해당 블록 이후 모든 블록의 암호퍼즐을 새롭게 계산하여야 하며, 가장 긴 체인 우선 원칙 때문에 계속 생성되고 있는 기존 체인보다 더 긴 체인을 만드는 것은 가능하지 않다.

- 특징 3. 분산 저장되어 있다.

  완전 노드를 운영하는 모든 참여자는 최초 블록부터 최신 블록까지 모든 블록의 정보를 유지하고 있다. 보통 같은 데이터가 여러 곳에 분산 저장되어 있다면 분산 저장된 모든 데이터를 다 바꾸기 힘들기 때문에 이 자체가 수정을 어렵게 하는 요소이다.

- 특징 4. 누구나 접근할 수 있다. 이 때문에 비트코인을 공개형 블록체인이라 한다.

- 특징 5. 블록에 기록을 포함하는 권한은 블록을 생성하는 주체가 결정한다.

  채굴자가 원칙적으로 지금까지 블록에 포함되어 있지 않은 트랜잭션들의 해시 트리를 구성하여 현재 블록을 계산하여야 하지만 모든 트랜잭션을 포함할 의무는 없으며, 더욱더 빠르게 암호 퍼즐을 해결하기 위해 트랜잭션을 하나도 포함하지 않을 수 있다. 하지만 규칙에 따라 비트코인이 잘 동작해야 그것의 가치가 유지 또는 상승되기 때문에 채굴자가 비트코인 가치에 나쁜 영향을 줄 수 있는 행동을 할 동인이 없다.

- 특징 6. 체인 순서에 의해 각 블록이 생성된 시점에 대한 상대적 시간을 알 수 있다.

  특징 5에서 설명한 바와 같이 블록에 특정 트랜잭션의 포함 여부는 채굴자가 결정한다. 따라서 블록에 포함된 순서가 실제 거래가 이루어진 순서라고 단정할 수는 없다.

- 특징 7. 오픈 소스로 운영된다. (신뢰성이 높음)

  비트코인처럼 안전성과 신뢰가 중요한 경우에는 소프트웨어 소스 자체를 공개하여 소프트웨어가 정해진 규칙에 따라 정확하게 동작하고 트랩도어와 같은 문제가 있는 요소가 없다는 것을 누구나 확인할 수 있도록 하는 것이 필요하다. 오픈 소스이므로 이것을 활용하여 알트코인을 개발하는 것도 용이하다.

참고로 블록체인의 변경불가능성 특징은 블록체인을 어떤 응용에 활용하는지에 따라 단점이 될 수도 있다. 한번 기록된 정보는 영구히 삭제할 수 없기 때문에 오류가 포함되더라도 이를 수정, 삭제할 수 없고, 프라이버시, 잊힐 권리(right to be forgotten)라는 측면에서도 위험한 요소가 될 수 있다. 또 UTXO 방식을 사용하고 있기 때문에 비트코인의 블록체인 데이터는 계속 쌓이기만 하는 구조이다. 일반적인 데이터와 달리 aging 기능이 없다.

2.5 비트코인의 안전성

새 비트코인은 채굴을 통해서만 생성할 수 있다. 따라서 항상 특정 참여자가 채굴에 성공할 수 있다면 혼자 부를 독식할 수 있는 문제점이 있다. 하지만 확률적이며 일정 시간이 소요되도록 하는 채굴 방식과 비트코인 생태계의 건전성 때문에 이와 같은 문제는 발생하기 어렵다. 또한 채굴이 아닌 방법으로 비트코인을 만들어 분산 원장에 포함할 수는 없다. 물론 앞서 설명한 바와 같이 지금은 상위 4 5개 채굴 풀이 전체의 50% 이상의 해시파워를 가지고 있어, 실제 생태계가 건전하다고 말하기 어려운 측면이 있다.

기존 거래 명세를 수정하거나 이중 사용하여 부당한 이득을 취하고자 할 수 있다. 거래 명세를 수정하기 위해서는 해당 거래 명세가 공개된 블록을 새롭게 채굴한 다음 그 이후 모든 블록도 다시 채굴해야 한다. 하지만 가장 긴 체인을 우선하는 비트코인의 규칙 때문에 오래된 거래 명세를 수정하기는 계산적으로 거의 불가능하다. 참고로 블록들은 10분마다 계속 채굴되고 있다. 매우 강력한 채굴자가 등장하면 기존 공개된 거래 명세를 무시하고 생태계를 교란할 수 있지만 앞서 언급한 바와 같이 현재의 생태계 상황을 고려하였을 때 아직은 현실성이 없다.

다른 사용자의 코인을 가로채어 사용하는 문제의 경우에는 그 코인을 사용하기 위한 개인키가 필요하다. 비트코인은 타원곡선 기반 전자서명 알고리즘을 사용하고 있기 때문에 서명의 위조나 암호해독을 통한 타인의 개인키 확보는 이 알고리즘에 의존한다. 대부분에 보고되는 거래소에 대한 해킹 사례는 비트코인 자체의 보안 문제보다는 운영 사이트와 서버가 가지고 있는 취약점을 이용하는 공격들이다. 실제로 일부 거래소의 경우에는 고객의 개인키까지 보유하고 있어, 거래소 해킹을 통해 비트코인이 탈취된 사례가 있다.

2.6 비트코인의 문제점

비트코인은 애초에는 화폐 기능을 하기 위해 고안된 것이다. 하지만 비트코인은 가격 변동이 크고, 거래가 확정되는데 소요되는 시간이 길기 때문에 실제 화폐 기능을 하기 어렵다. 현재는 화폐보다는 투자 자산 기능만 하고 있다. 또 암호화폐는 익명 거래가 가능하여, 불법 거래에 많이 사용되었기 때문에 부정적으로 보는 시각이 있고, 현재 사용하고 있는 다양한 지불 방식에 대해 큰 불편함을 느끼지 못하고 있어 암호화폐가 가까운 미래에 실제 화폐 역할을 할지는 미지수이다. 물론 16장에서 설명하는 CBDC가 가까운 미래에 통용될 가능성은 충분히 있다.

암호화폐가 대중에 관심을 받게 되고, 그것을 투자 대상으로 여김에 따라 암호화폐를 기존 상품과 유사하게 쉽게 거래하기 위해 코인 거래소가 등장하였다. 코인 거래소는 일종의 중재자이다. 이 측면에서 P2P 탈중앙 암호화폐의 원래 취지에 맞는 참여자는 아니다. 기존 은행 서비스와 달리 개인의 부주의로 보유 암호화폐를 모두 잃을 수 있기 때문에 개인은 자신의 모든 거래에 대해 전적으로 책임지기보다는 코인 거래소라는 중재자를 활용하는 것이 더 안전하고 편리하다고 생각할 수 있다.

채굴은 비트코인에서 매우 중요한 핵심 요소이다. 또 이 채굴은 중단 없이 계속 되어야 비트코인이 정상 동작할 수 있다. 비트코인의 채굴이 독점되면 부가 집중되는 문제도 있지만 51% 공격 등 안전성에도 위협이 된다. 현재는 ASIC을 이용한 채굴로 소위 큰 손들에 의한 채굴이 집중되고 있다. 현재 상위 4곳의 채굴 풀이 차지하는 비율은 50%을 초과하고 있다. 물론 이 풀에 속한 각 개인이 차지하는 비중은 걱정될 수준은 아니다. 하지만 채굴의 중앙 집중화 역시 애초 P2P 탈중앙 암호화폐의 취지에도 맞지 않으며, ASIC을 이용한 채굴 경쟁은 많은 양의 전기 소비로 환경에도 매우 나쁜 영향을 주게 된다.

비트코인이 사용하는 작업 증명은 이와 같은 문제를 근본적으로 해결하기 어렵다. 따라서 작업 증명 대신에 지분

증명 등 다른 분산 합의 기술을 사용하여 블록체인을 구현하는 방법들도 제안되고 있다. 이에 대해서는 16장에서 자세히 살펴본다.

비트코인이 화폐의 역할을 하고 있지 않지만 투자의 대상이 되고 있어 비트코인의 거래는 계속 발생하고 있다. 비트코인의 기능적 측면에서 가장 큰 문제점은 확장성이다. 현재 비트코인은 10분만마다 새 블록이 생성되며, 이 블록의 크기는 1MB로 제한되어 있다. 트랜잭션의 크기가 가변적이지만 블록마다 약 3,000건 정도의 거래만 수용할 수 있으며, 이 거래가 확정되는데 여섯 블록이 지나야 하므로 거래 확정 속도가 느리다는 단점도 가지고 있다.

한 블록에 포함할 수 있는 거래량과 이로 인한 속도 문제는 보통 신용카드 거래량과 비교된다. Visa는 하루에 약 1억5천 개의 트랜잭션을 처리하고 있다. 즉, 1초에 약 1,700개를 처리하고 있다. 더욱이 실제 처리 가능한 속도는 1초에 약 24,000개의 트랜잭션이다. 반면에 비트코인은 1초에 7개의 트랜잭션만 처리가 가능하다. 비트코인의 확장 속도와 처리량 향상을 위해 세그윗, 지불 채널, 샤딩(sharding) 등 여러 방안들이 도입되거나 검토되고 있다.

비트코인의 확장 문제에 대한 의견 때문에 비트코인이 두 개로 갈리진 경우도 있다. 비트코인에서 처음으로 하드 포크된 암호화폐는 비트코인 캐시(www.bitcoincash.org)이다. 이처럼 특정 암호화폐 커뮤니티 내에 의견 충돌이 발생하면 기술적인 특성과 상관없이 암호화폐가 두 개로 갈라질 수 있다. 실제 비트코인에서 하드 포크된 암호화폐는 비트코인 캐시 외에 비트코인 골드(www.bitcoingold.org), 비트코인 SV(bitcoinsv.io)가 있다.

비트코인 캐시는 비트코인에서 직접 파생된 새로운 암호화폐이지만 비트코인의 성공으로 비트코인과 유사한 수많은 종류의 암호화폐가 개발되었다. 이들을 모두 통틀어 알트 코인(ALTernative coin)이라 한다. 중요 알트코인에 대해서는 16장에서 다룬다. 이 측면에서 비트코인의 역사성과 의미가 인정되고 있다는 것을 방증하는 용어로도 해석될 수 있다.

참고문헌

[1] Narayana R. Kocherlakota, "Money is Memory," J. of Economic Theory, Vol. 81, No. 2, pp. 232–251, Aug. 1998.

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[3] Stuart Haber, W. Scott Stornetta, "How to Time-stamp a Digital Document," Advances in Cryptology, CRYPTO '90. LNCS 537, pp. 437–455, Springer, 1991.

[4] Markus Jakobsson, Ari Juels, "Proofs of Work and Bread Pudding Protocols," Secure Information Networks, pp. 258–272, 1999.

[5] "Bitcoin Gold Hit by Double Spend Attack, Exchanges Lose Millions," https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions/, 2018.

[6] "Japanese Cryptocurrency Monacoin Hit by Selfish Mining Attack," https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack/, 2018.

퀴즈

1. 비트코인의 블록체인은 해시 퍼즐을 이용한 작업 증명을 이용한다. 다음 중 비트코인에서 사용하는 해시 퍼즐의 특징이 아닌 것은?

   ① 해결하는데 소요되는 시간을 조절할 수 있다.
   ② 해결하는 과정에 확률적 요소가 포함되므로 우연히 동시에 해결할 수 있다.
   ③ 해결하는데 걸리는 시간은 길 수 있지만 확인은 매우 빠르게 할 수 있는 비대칭적 특징을 가지고 있다.
   ④ 해결하는데 걸리는 시간은 사용하는 장비의 성능에 영향을 받지 않는다.

2. 다음 중 비트코인 거래의 특징이 아닌 것은?

① 금전 이동에 해당하는 트랜잭션이 블록체인에 기록되어 지불이 이루어지는 형태이다.

② 비트코인 트랜잭션은 다중 입력, 다중 출력을 지원하며, 입력의 합이 출력의 합과 같아야 한다.

③ 한 지갑이 보유한 총액은 블록체인에 기록된 출력 중 대상이 해당 지갑이고, 아직 지불에 사용하지 않은 출력의 합이다.

④ 이미 지불에 사용한 금액을 이중사용할 수 없도록 새 트랜잭션이 제출되면 그것이 입력이 이미 사용된 적이 있는지 블록체인에서 검사해야 한다.

3. 비트코인 채굴과 관련된 다음 설명 중 틀린 것은?

① 채굴에 성공하면 일정한 수의 새 비트코인과 블록에 포함한 트랜잭션의 수수료를 보상으로 받는다.

② 장비 싸움(더 좋은, 더 많은 장비를 가지고 있을수록 채굴에 성공할 확률이 높음)이지만 확률적 요소가 포함되어 있다.

③ 아무도 채굴하지 않아 블록체인에 블록이 추가되는 것이 멈추더라도 기존 데이터의 불가역성은 보장된다.

④ 채굴하기 위한 투자 대비 수익이 기대에 미치지 못하더라도 채굴을 멈추면 비트코인 생태계에 영향을 줄 수 있고, 그 영향으로 비트코인 가격이 하락할 수 있기 때문에 보유한 비트코인의 가치를 유지하기 위해서는 계속 채굴할 수밖에 없는 특성도 있다.

4. 비트코인은 블록체인을 사용하여 비트코인이 제공해야 하는 여러 가지 요구사항을 충족하고 있다. 다음 중 블록체인을 통해 충족하는 요구사항이 아닌 것은?

① 유효한 트랜잭션만 블록체인에 저장되도록 하고, 저장된 트랜잭션은 수정 및 삭제가 가능하지 않도록 하여 이중사용을 방지하고 있다.

② 블록이 확정될 때마다 일정한 수의 화폐가 발행되도록 하여 화폐의 발행을 통제하고 있다.

③ 다른 사람이 보유한 비트코인을 사용할 수 없도록 하기 위해 블록체인을 사용하고 있다.

④ 비트코인 노드(완전노드)들이 모두 같은 데이터를 유지하도록 해준다.

5. 명목화폐와 비트코인을 비교한 다음 설명 중 틀린 것은?

① 둘 다 금전적 가치가 지불자에서 수취인으로 바로 이동하기 때문에 push 방식의 지불이다.

② 둘 다 지불이 이루어지는 순간 금전적 가치의 이동이 확정된다.

③ 명목화폐는 화폐가 수취인에게 전달되지만 비트코인은 지불 의사가 수취인뿐만 아니라 전 세계의 모든 비트코인 노드로 전달되어야 한다.

④ 명목화폐는 발행기관이 중앙집중적으로 발행하지만 비트코인은 참여 노드들이 규칙에 따라 주기적으로 자발적으로 발행한다.

연습문제

1. 비트코인 이전 암호화폐에서 온라인, 오프라인 방식의 차이를 설명하고, 각 방식에서 이중사용을 어떻게 처리하는지 설명하시오.

2. 은닉서명을 이용한 암호화폐에서는 해당 암호화폐를 발급받은 고객뿐만 아니라 누구든지 암호화폐에 해당하는 전자서명 값을 가지고 있으면 사용이 가능하다. 이와 관련하여 다음에 대해 각각 답변하시오.

① 은닉서명을 받을 때 단순한 일련번호 대신에 랜덤 공개키를 이용한다고 하자. 즉, $-K_D$가 특정 액면가에 대한 서명키이고, $+K$가 랜덤 공개키라 할 때 암호화폐가 Sig.$-K_D(H(+K))$ 형태가 된다. 이 경우 해당 화폐를 사용하기 위해서는 일련번호 역할을 하는 $+K$에 대응되는 개인키가 필요하도록 지불 프로토콜을 설계할 수 있다. 이것의 장점을 기존 방식과 비교하여 설명하시오.

② 위의 랜덤 공개키 대신에 해시체인의 루트 값을 포함하였다고 하자. 이 경우 루트체인의 각 값이 액면가 동전으로 활용할 수 있다. 이 방식과 관련하여 인출과 지불 과정에서의 문제점을 설명하시오.

3. 3장에서 소개된 중재방식의 전자서명에서 서명이 유효하기 위해서는 서명자뿐만 아니라 중재자의 서명까지 필요하다. 이와 관련하여 블록체인 기술을 어떻게 사용할 수 있는지 설명하시오.

4. 블록체인에서 하드 포크와 소프트 포크의 차이를 설명하고 하드 포크 측면에서 블록체인의 변경불가능성을 논하시오.

5. 비트코인에서 특정 공격자가 거래 내역을 수정하고자 한다. 특정 트랜잭션의 내용을 수정하기 위해서는 다음 세 가지를 할 수 있어야 한다. 첫째, 트랜잭션 내용 자체를 수정해야 한다. 둘째, 수정된 트랜잭션이 포함되는 새 블록을 채굴해야 한다. 셋째, 채굴된 블록이 유효 블록체인에 포함되도록 해야 한다. 각 세 가지에 대해 어려운 정도를 간단히 설명하시오.

6. 작업증명을 이용하는 블록체인에서 채굴에 참여하는 전체 해시파워의 51%을 특정 사용자가 확보하면 51% 공격을 시도할 수 있다고 한다. 이 사용자가 실제 할 수 있는 공격이 무엇인지 설명하시오.