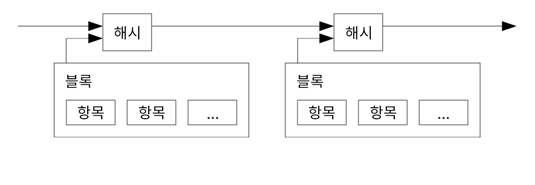
**블록체인 시스템**: 제 거래를 보장해주는 3자가 없는 거래 시스템에서 거래 내역을 보장하기 위해 만들어진 시스템.

**거래**: 거래는 디지털 서명으로 이루어짐. “이전 거래 내역” (이전 거래 내역에는 코인과 주인이 있음)을 받는 사람의 공개키로 해시 후 코인에 붙여서 거래가 이루어지는 방식

=> 이중 지불 거래를 막기위해 모든 거래 내역을 공개하며 거래 발생시 참가자들은 거래 내역을 공유하는 하나의 history에 있는지 확인하여 이중 지불이 일어났는지 판단할 수 있음

**타임스탬프 서버**: 시간 순으로 기록된 블록에 해시를 하며 해시를 발행하는 역할. 각각의 타임스탬프는 이전의 타임 스탬프를 해시 형태로 포함하는 구조



**작업증명(proof of work)**: 작업 증명 방식은 SHA-256과 같은 알고리즘을 통해 해시 되었을 때 특정 숫자보다 작은 값을 찾는 과정을 말함. 숫자가 작을수록 난이도가 증가함. 타임스탬프 네트워크는 블록 해시를 수행한 결과 만족하는 0비트를 가질 때 까지 임의의 값인 논스(nonce)를 증가시키는 방식으로 작업증명을 구현. CPU가 노력한 결과가 작업증명 조건을 충족하게 되면, 이 블록은 수행한 작업증명과 같은 노력의 일을 반복하지 않는 한 변경할 수 없다. 하나의 블록을 변경하기 위해서는 그 블록만이 아니라 해당 블록에 연결된 모든 블록에 작업증명을 다시 진행해야 함

작업증명의 난이도는 시간당 생성되는 블록의 평균을 통해 계산됨. 시간당 생성되는 블록의 평균이 작아질수록 난이도가 감소하고 많아질수록 난이도가 증가함.

**네트워크 동작 방식**

1. 새로운 거래들이 전체 노드에 전파된다.

2. 각 노드들은 신규 거래들을 블록에 취합한다.

3. 각 노드들은 블록에 가장 어려운 난이도로 행해진 작업증명을 찾는다.

4. 노드가 새로운 작업증명을 발견하면 해당 블록을 전체 노드에 전파한다.

5. 노드들은 모든 거래가 유효하고, 이전에 사용되지 않은 경우에만 블록을 받아들인다.

6. 노드들은 체인 위의 다음 블록에 이전 블록을 해시 형태로 추가하는 것으로 해당 블록을 받아들였다는 의사를 표시한다.

노드들은 항상 가장 긴 체인을 옳은 것으로 간주하고 인증된 체인을 이어간다. 만일 두 개의 노드가 각기 다른 버전의 다음 블록을 동시에 전파하는 경우, 다른 버전의 블록을 전달받는 노드들이 발생한다. 이 경우, 먼저 전달 받은 블록을 기준으로 작업을 수행하지만, 다른 갈래의 블록도 저장하여 해당 블록이 더 길어질 것에 대비한다. 다음 작업증명이 완료되어 둘 중 하나가 더 긴 체인이 되는 경우, 더 이상 두 블록을 대등하게 취급하지 않고 긴 체인을 형성한 블록을 기준으로 작업

**보상**

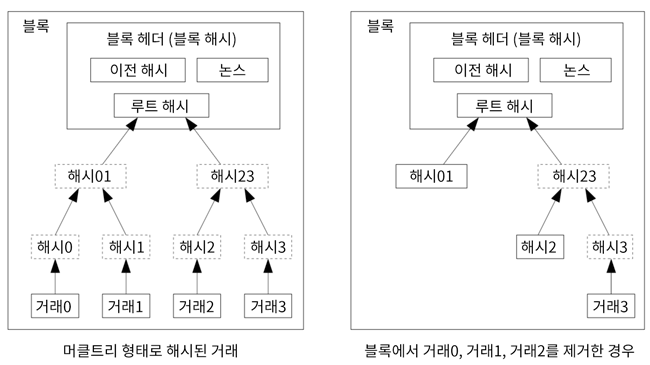
블록의 첫 거래는 블록의 생성자에게 새로운 코인을 보내는 특별한 거래. 네트워크 구조를 유지하는 노드에게 보상을 줌으로써, 중앙관리기구 없이 분산된 형태로 유통되는 구조를 유지할 수 있음.

거래 수수료도 보상 중 하나. 거래에서 출력되는 돈보다 입력되는 금액이 작다면 그 차이는 거래 수수료의 형태로 블록을 생성하는 보상으로 제공

이러한 보상 체계는 노드들이 선의의 행동을 하도록 독려한다. 만약 이기적인 공격자가 선의의 노드보다 많은 연산능력을 끌어 모을 수 있다면, 다른 이의 지불을 갈취하거나, 새로운 코인을 생성하여 사적인 이익을 취하려 할 것이다. 하지만 이러한 방법보다 정해진 규칙에 순응하는 것이 더 많은 코인을 가져다 주기 때문에 공격자가 굳이 공격을 해야 할 이유는 없음

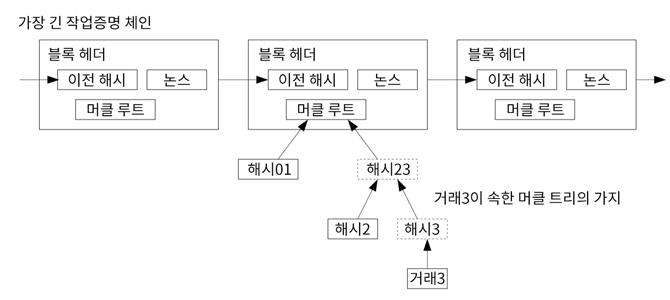
**저장 공간의 재사용**

코인을 기준으로 충분히 많은 블록이 이어지게 되면 지난 거래 내역은 저장 공간의 확보를 위해 폐기해도 된다. 블록 해시를 깨지않고 이를 가능하게 하려면 모든 거래가 머클 트리(Merkle Tree)안에 해시됨



**지불 검증의 간소화(Simplified Payment Verification)**

풀 노드(full network node)를 운용하지 않더라도 지불을 검증하는 것은 가능하다. 사용자가 자신이 가장 긴 체인임을 확인할 수 있을 때까지 네트워크 노드들에게 요청하여 가장 긴 작업증명 체인의 블록 헤더의 사본(copy)을 가지고 있으면 해당 거래가 포함된 블록의 머클트리의 가지(branch)를 얻어올 수 있다. 사용자 스스로 거래의 유효성을 체크할 수는 없으나, 체인에 연결된 것을 확인할 수 있음

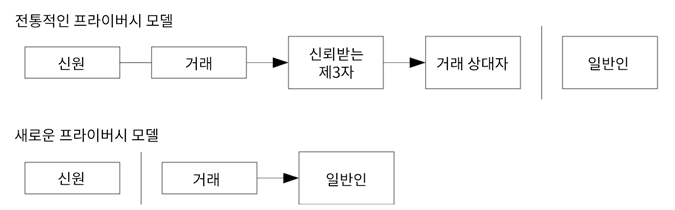


**가치의 병합과 분할(Combining and Splitting Value)**

코인을 중심으로 개별적 관리하는 것도 가능하지만, 이 경우 작은 단위의 거래를 하기는 여러모로 불편하다. 가치가 나누어지거나 합쳐질 수 있도록 하기 위해 다수의 입력과 다수의 출력을 허용

**프라이버시(Privacy)**

기존의 은행 구조는 담당하는 그룹과 신뢰받는 제3자의 정보 접근 권한을 제한하는 방식으로 프라이버시를 보호한다. 모든 거래를 공개하는 방식에서 은행 형태의 모델을 차용할 수는 없지만, 프라이버시를 유지하면서 모든 거래를 공유하는 것이 불가능한 것은 아니다: 공개 키들을 익명으로 사용하면 된다. 참여자 모두는 어떤 이가 다른 이에게 얼마를 보냈는지 확인할 수는 있지만, 정작 거래가 누구에 귀속되는지에 대한 정보는 공개하지 않기 때문에 확인할 수 없음



**결론(Conclusion)**

전자 서명으로 이뤄진 기존의 보편적인 형태는 소유권에 대한 강한 통제권을 제공하지만 이중지불을 막지 못하면 불완전할 수 밖에 없다. 이를 해결하기 위해 작업증명을 이용하여 공개적으로 거래를 기록하는 P2P 네트워크를 제안하였다. 이 방식은 정직한 노드들이 다수의 연산능력을 확보하고 있다면 공격자가 쉽게 조작하는 것이 불가능