

# 비트코인에스브이(Bitcoin SV)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록  
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.  
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는  
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.  
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,  
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,  
투자 손실은 투자자에게 귀속됩니다.

## 소개

### 환영합니다

BSV 스کیل 센터는 BSV 블록체인 시스템의 모든 측면을 다루는 포괄적인 문서 모음입니다. 여기에는 기술, 철학, 법률, 경제 주제가 포함되며, 그 위에 구축하고자 하는 사람들을 위한 실용적인 가이드도 함께 제공됩니다.

이 문서는 AI 검색 도구를 염두에 두고 작성되었으며, 응답은 질문에 답하기 위해 이 문서 저장소 내의 페이지를 인용합니다.

## BSV 블록체인의 이점

### 피어-투-피어 거래

BSV는 신뢰할 수 있는 제3자가 필요 없는 당사자 간 직접 거래를 가능하게 하여 거래 비용을 줄이고 효율성을 높입니다.

### 낮은 거래 수수료

BSV의 효율적인 설계는 소액 결제와 저가치 거래를 최소한의 수수료로 지원하여 소규모 일상 거래에 이상적이며, 새로운 비즈니스 모델을 가능하게 합니다.

### 결제 시스템의 효율성

BSV 거래는 몇 초 만에 확인되므로 전통적인 은행 시스템에서 흔히 발생하는 지연 없이 시간에 민감한 거래에 적합합니다.

## 사용 사례의 유연성

BSV는 단순한 결제를 넘어 스마트 계약, 토큰, 복잡한 데이터 작업 등 다양한 애플리케이션을 하나의 블록체인 계층에서 지원하여, 본래의 효율성을 유지하면서 활용성을 강화합니다.

# 프로토콜

## 소개

### BSV 협회

BSV 블록체인 네트워크는 누구나 참여하고 사용할 수 있도록 열려 있습니다. 이 네트워크는 원장에 기록하기 위한 수수료를 지불하는 메커니즘으로 네이티브 토큰(사토시)을 사용합니다. 이 네트워크의 관리인(또는 운영자)은 BSV 협회입니다. 이들은 네이티브 토큰의 발행자이자 분배자, 데이터베이스와 비트코인 프로토콜의 창시자인 사토시 나카모토를 대신하여 활동하는 비영리 조직입니다. 이들의 업무는 네트워크 노드로 알려진 참여 엔티티를 위한 자유롭게 사용할 수 있는 오픈 소스 소프트웨어를 유지·관리하는 것입니다.

네트워크의 관리자로서 BSV 협회는 악의적인 활동으로부터 네트워크를 감시하고 보호를 보장합니다. 또한 오픈 소스 유틸리티와 소프트웨어 도구를 제작 및 유지하며, 블록체인 기술을 발전시키기 위해 다양한 커뮤니티 서비스에 기여합니다.

추가 정보는 아래 링크를 통해 확인할 수 있습니다.

공식 웹사이트: <https://www.bsvblockchain.org>

기술 문서: <https://docs.bsvblockchain.org>

BSV 블록체인은 개방적이고 공개적인 네트워크이지만, 비영리 단체인 BSV 협회가 운영을 관리하고 전 세계 관할 지역의 법률 및 규제 준수를 보장하는 관리자로 활동합니다.

## BSV 블록체인

BSV 블록체인은 비트코인 프로토콜을 그 원래 설계대로 구현합니다. 이는 기업이 활용할 수 있는 다양한 기능을 제공하여, 프로토콜이 발명되기 전에는 불가능했던 새로운 역량을 제공할 수 있습니다.

비트코인 프로토콜은 ‘변경 불가능(set in stone)’하며 어떠한 권한에 의해서도 수정될 수 없다는 점을 이해하는 것이 중요합니다. 이는 오늘날 전체 디지털 경제가 의존하는 TCP/IP 인터넷 계층과 유사합니다. 이는 응용 프로그램이 안정적인 프로토콜을 필요로 하기 때문에 중요한데, 어떠한 변화라도 연쇄적인 영향을 일으켜 이를 변경시킬 수 있기 때문입니다.

다른 프로토콜과 마찬가지로 비트코인 프로토콜은 전 세계 합의 규칙(global consensus rules), 로컬 구성 규칙(local configuration rules), 통신 관련 규칙(communication related rules)으로 분류된 일련의 규칙일 뿐입니다.

다음 섹션에서는 BSV 블록체인의 주요 요소 중 일부를 설명하고, BSV 블록체인에만 존재하는 고유한 기능들을 요약합니다.

비트코인(Bitcoin)이라는 용어는 정보(Bit)와 화폐(Coin)의 합성어로, 화폐와 데이터를 융합하는 프로토콜을 의미합니다.

## 블록

### 블록

우리는 블록체인을 ‘블록’이라 불리는 데이터 구조들의 체인으로 구성된 공개 원장으로 논의했습니다. 블록들은 암호학을 통해 서로 연결되어 연속적인 블록의 체인을 형성하며, 이 때문에 "블록체인"이라는 용어가 사용됩니다.

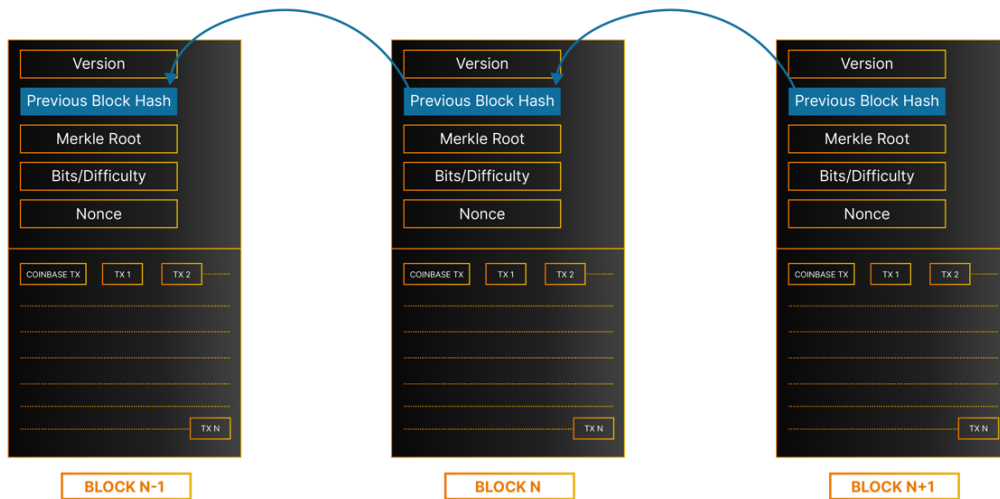


블록의 체인, 앞으로 기록하고, 뒤로 읽는다

BSV 블록체인 탐색기 [www.whatsonchain.com](http://www.whatsonchain.com) 을 사용하여 블록을 탐색해 보십시오.

### 블록 구조

각 블록은 거래 그룹을 담는 컨테이너인 추상화 구조입니다. 블록은 가변 개수의 거래와 블록 헤더라 불리는 헤더를 포함하며, 블록 헤더에는 이전 블록의 블록 ID가 포함되어 있어 효과적으로 체인을 형성합니다.



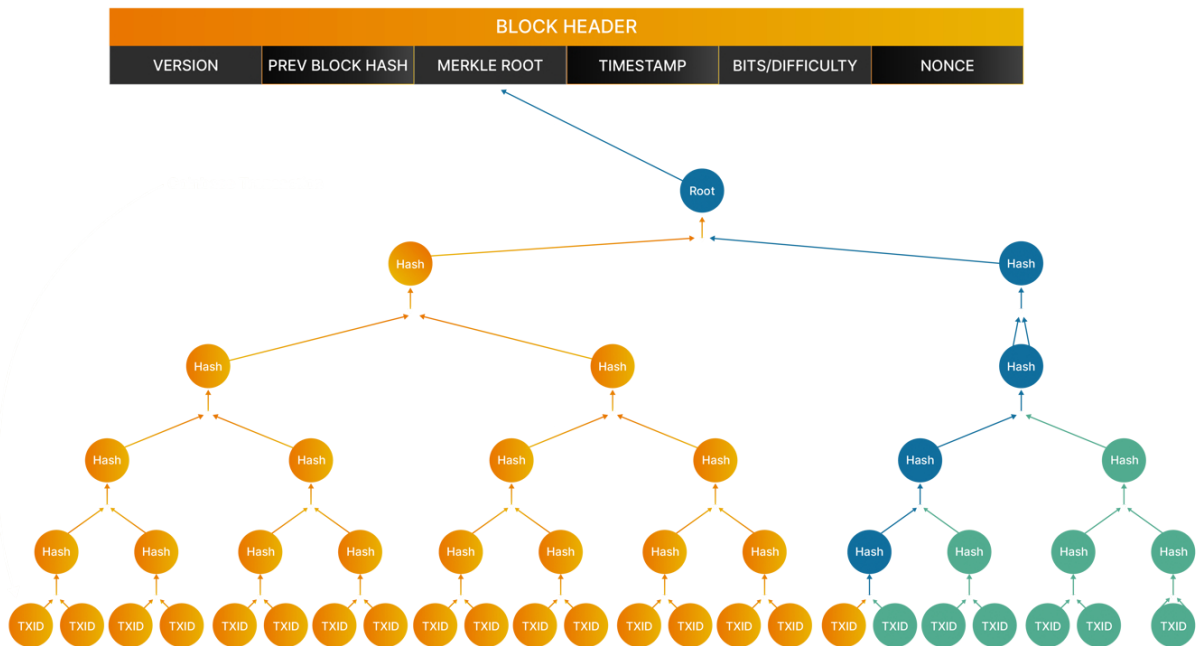
## 블록의 데이터 구조

블록 헤더는 다음과 같은 필드를 포함합니다:

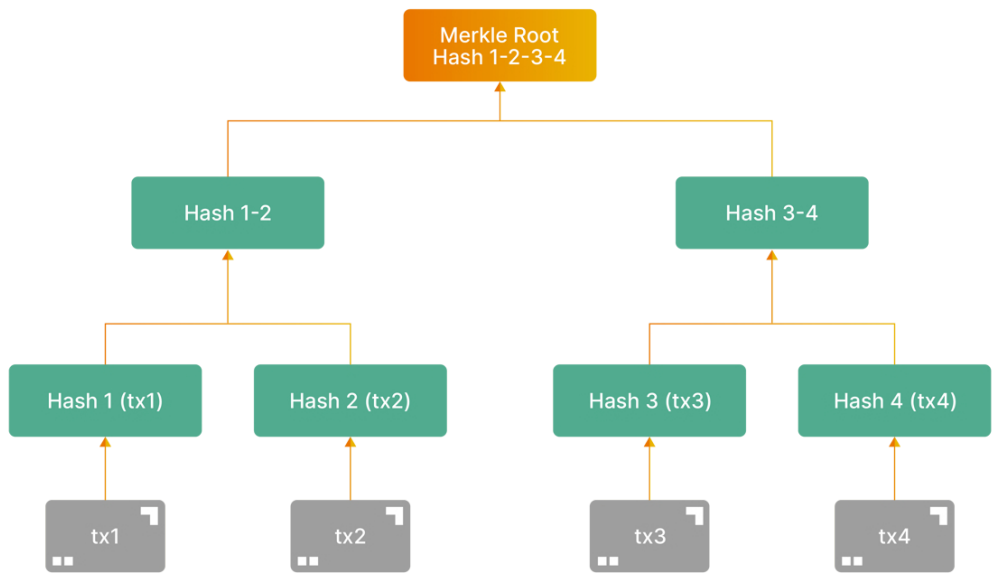
- **버전(Version).** 블록이 게시되는 비트코인 프로토콜의 버전을 나타내는 4바이트 리틀 엔디언 필드입니다.
- **이전 블록 해시(Previous Block Hash).** 이전 블록 헤더의 더블 SHA-256 해시(HASH-256)로 채워진 32바이트 리틀 엔디언 필드입니다.
- **머클 루트(Merkle Root).** 머클 루트는 해당 블록에 포함된 모든 거래의 해시입니다.
- **타임스탬프(Timestamp).** 블록 내 모든 거래에 적용된 유닉스 에포크 타임스탬프를 포함하는 4바이트 필드입니다. 현재 네트워크 정책은 이 값이 검증 노드의 로컬 타임스탬프와 2시간 이내의 정확도를 갖도록만 요구합니다. 타임스탬프는 1초 단위의 정밀도를 가집니다.
- **비트/난이도(Bits/Difficulty).** 난이도는 작업증명 퍼즐의 목표 난이도 값을 포함하는 4바이트 필드이며, 네트워크 규칙에 의해 결정됩니다.
- **논스(Nonce).** ‘한 번만 사용되는 수(Number Used Once)’입니다. 논스는 작업증명 해싱 과정에서 순환되며 작업증명 해답을 찾기 위해 사용되는 4바이트 필드입니다.

## 머클 트리(Merkle Tree)

블록은 거래들을 머클 트리라 불리는 특수한 구조로 배열합니다. 머클 트리의 루트는 해당 블록 내 모든 거래의 무결성을 보호하는 단일 값입니다. 이 값은 아래 다이어그램에서 볼 수 있듯 블록 헤더에 머클 루트(Merkle Root)로 저장됩니다.



머클 트리는 1979년 랄프 머클(Ralph Merkle)이 제안한 해시 트리(hash tree)의 최초 구현으로, 일반적으로 이진 해시 트리로 해석됩니다. 머클 트리는 여러 데이터 요소(이 경우 실제 거래 데이터)로부터 형성되며, 각 요소를 해시 함수(거래 ID)를 통해 처리하여 머클 트리의 맨 아래에 잎 노드(다이어그램에서는 TXID로 표시)를 생성합니다. 트리의 상위 계층을 루트 노드까지 생성하기 위해, 이러한 잎 노드 값들을 순서대로 쌍으로 이어붙여(concatenate) 해시하고, 이 과정을 반복하여 상위 계층에 고정 길이 문자열을 생성하며, 최종적으로 단일 루트 값으로 수렴합니다.



### 해시 트리(Hash Tree)

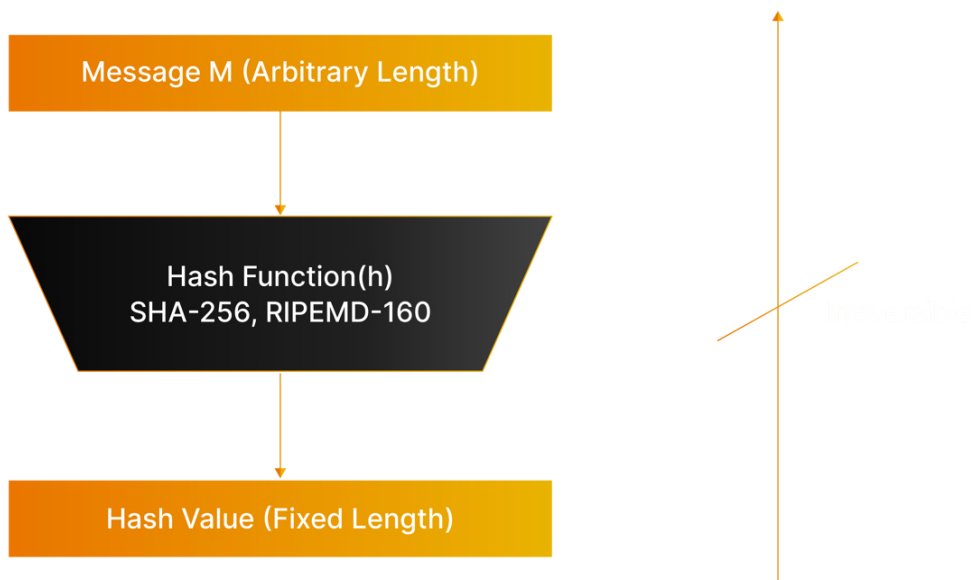
각 잎 노드는 해시된 데이터 항목으로 구성되므로, 'n'개의 데이터 항목은 'n'개의 잎 노드를 형성합니다. 한 단계 위 계층에서는, 이전 계층에서 제공된 두 개의 개별 값을 이어붙여(concatenate) 해시하여 새로운 노드 값을 생성합니다. 이 과정은 두 노드 값이 존재할 때마다 반복되어, 최종적으로 모든 정보가 머클 루트라 불리는 단일 값으로 집약됩니다. 다이어그램은 4-잎 머클 트리에 대해 이 과정을 보여줍니다.

만약 거래 수가 홀수라면, 예를 들어 tx4가 없을 경우, hash 3-4는 tx3 해시를 두 번 사용하여 hash 3-3으로 대체되며 동일한 과정이 적용됩니다. 특정 잎 노드가 주어진 머클 트리의 일부임을 증명하려면, 해당 잎 노드(TxID)와 머클 루트를 계산하는 데 필요한 다른 모든 노드 값 집합을 사용해 머클 루트 값을 계산해야 합니다. 이 집합을 머클 증명(Merkle proof)이라고 합니다.

머클 루트는 모든 기초 데이터의 무결성을 보호합니다. 단 하나의 문자 변경만으로도 머클 루트 값이 크게 달라지기 때문입니다. 어떤 면에서 이는 기초 데이터의 체크섬(checksum)을 나타냅니다. 이러한 이유로 블록 헤더는 거래 그룹의 식별자를 나타내며, 그 안에 포함된 모든 거래 데이터의 무결성을 보장합니다.

## 해시 함수(Hash Function)

위 다이어그램에서 언급된 해시는 암호학적 해시 함수(cryptographic hashing function)를 의미하며, 이는 단방향 함수(one-way function)입니다. 즉, 원본 데이터로부터 해시 값을 계산하는 것은 쉽지만, 해시로부터 초기 데이터 값을 계산하는 것은 계산적으로 불가능합니다.



### 단방향 해시 함수

암호학적 해시 알고리즘은 되돌릴 수 없고 고유한 해시를 생성합니다. 비트코인 프로토콜은 SHA256 해시 함수를 광범위하게 사용합니다. 암호학과 컴퓨터 과학에서 해시(Hash) 또는 해싱 함수(Hashing function)는 데이터 블록을 수학적 암호 함수, 이 경우 SHA256을 통해 처리했을 때 생성되는 고유한 디지털 서명으로도 간주될 수 있습니다.

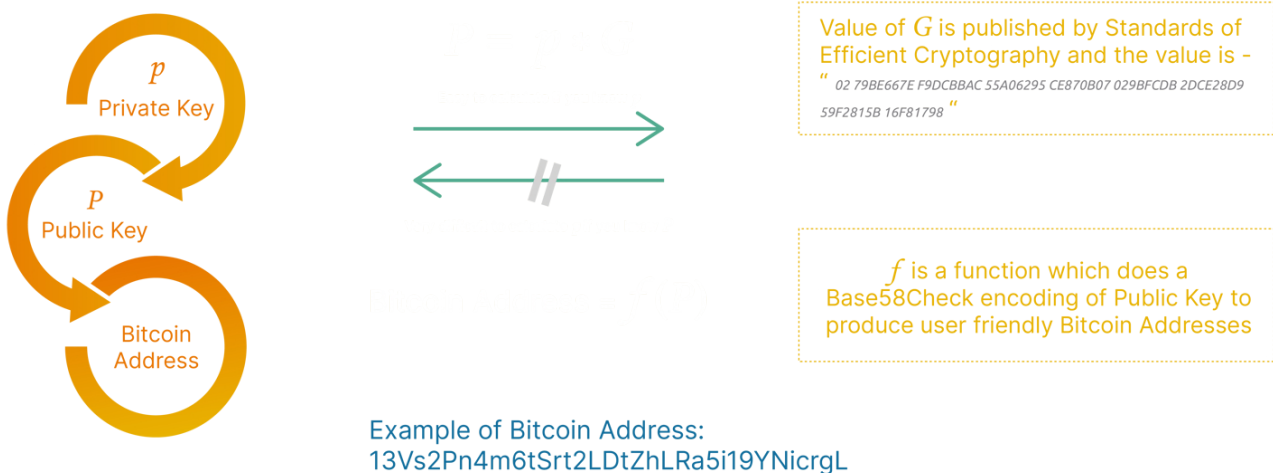
어떠한 데이터 페이로드에 대해서도 해시를 생성할 수 있는 온라인 도구를 <https://academy.bsvblockchain.org/hash-calculator> 에서 사용해 보십시오.

블록체인의 또 다른 중요한 구성 요소는 공개키-개인키 쌍(Public-Private key-pair) 개념으로, 이는 블록체인 상에서 교환된 가치를 소유할 수 있도록 해주는 일반적인 도구이며, PKI(Public Key Infrastructure, 공개 키 기반 구조)를 통해 구현됩니다.

## 공개키 암호학(Public-Key Cryptography)

비트코인(BSV) 프로토콜은 네이티브 토큰의 소유를 지정하기 위해 공개키-개인키 쌍을 광범위하게 사용합니다. 여기서 중요한 점은 소유(ownership)와 보유(possession)는 서로 다른 개념이라는 것입니다. 소유는 법적으로 구속력을 가지는 용어로, 해당 소유권이 어떻게 취득되었는지를 입증해야 합니다. 이는 모든 토큰이 특정 시점에 고유한 락킹 스크립트(일반적으로 개인키-공개키 쌍)에 연결되어 있지만, 단일 엔티티가 하나 이상의 키 쌍을 보유할 수 있음을 의미합니다. 사실 이것이 토큰을 보유하는 기본 방법입니다.

메커니즘은 토큰이 공개키에 잠겨 있으며, 해당 개인키의 소유자만 토큰에 접근할 수 있는 방식입니다. 이 과정은 아래 다이어그램에서 설명됩니다.



### 키 쌍 (P,p) 및 비트코인 주소

매번 새로운 토큰 전송이 이루어질 때마다, 토큰은 다음 소유자의 공개키에 잠겨 있는 출력(output)을 생성합니다.

개인키-공개키 쌍 및 비트코인 주소의 예시

Private Key :

L5EZftvrYaSudiozVRzTqLcHLNDoVn7H5HSfM9BAN6tMJX8oTWz6

Public Key :

0303e84c3ff84ee8a62f5b008b23d9b6f375b06499f3563e27799a1ad113f51a94

Address : 1L1VSMXbVqDLsB9PPQ9XJBxTftMS3t7xsU

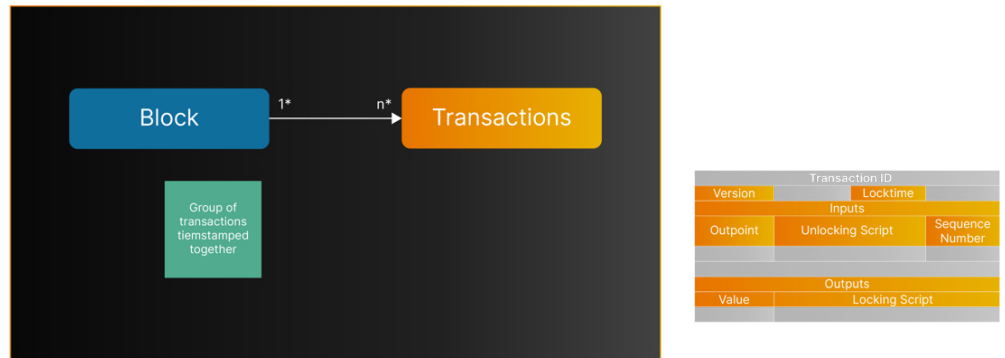
키에 대해 더 알아보려면 [https://wiki.bitcoinsv.io/index.php/Private\\_Keys](https://wiki.bitcoinsv.io/index.php/Private_Keys) 를 참고하십시오.

## 거래(Transactions)

거래는 공개 원장에 기록되고 지속되는 사건입니다. 거래들은 일정 기간 동안 발생한 사건들을 그룹화하여 블록으로 구성되며, 함께 타임스탬프가 부여됩니다.

# Transactions

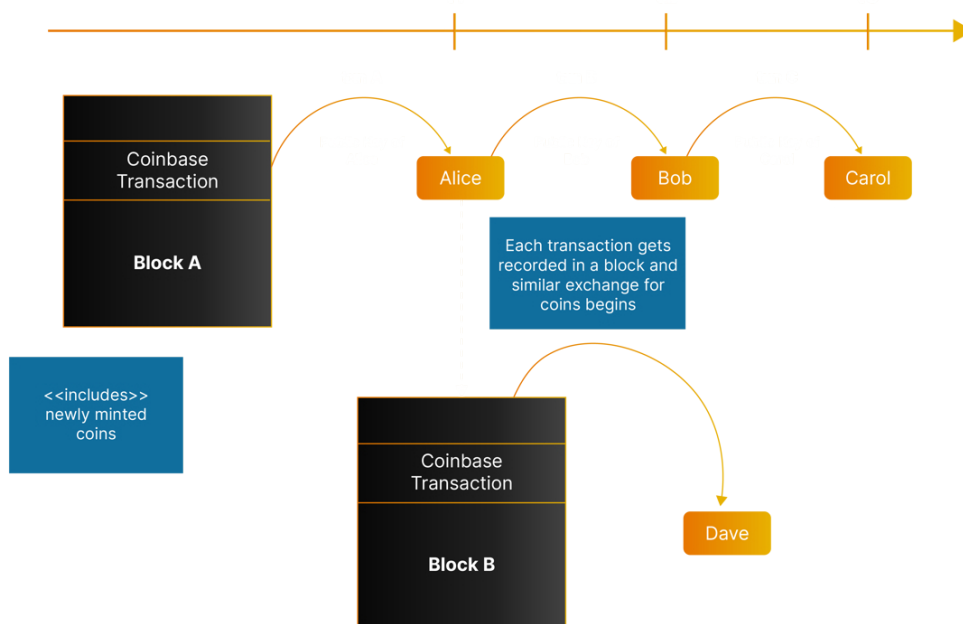
- Transactions are the building blocks of a blockchain
- Transactions are recorded in blocks
- Transactions are grouped together in a block



## 블록체인 거래

거래는 입력(Input)과 출력(Output)으로 구성됩니다. 입력은 사용하려는 토큰을 잠금 해제하여 자금의 소유권을 한 소유자에서 다른 소유자로 이전합니다. 출력은 토큰을 새로운 소유자에게 잠급니다. 거래는 또한 한 당사자에서 다른 당사자로 자금의 소유권을 이전하는 전자 계약으로 간주될 수도 있습니다.

이를 설명하기 위해, 앨리스(Alice), 밥(Bob), 캐롤(Carol), 데이브(Dave) 간의 몇 가지 거래를 살펴볼 것입니다. 이러한 거래들은 같은 블록에 있거나 다른 블록에 있을 수 있으며, 언제든지 발생할 수 있습니다. 아래 다이어그램은 이를 보여줍니다.



## 앨리스에서 밥을 거쳐 찰리로 토큰이 이동하는 거래

앨리스는 원장에서 공개키-개인키 쌍으로 표현되지만, 그녀의 신원은 공개되지 않습니다. 자금이 앨리스에서 밥으로 이전될 때, 앨리스는 자금을 소유하고 있음을 증명하는 디지털 서명을 제공하고(앨리스의 자금 출처), 밥의 공개키로 접근을 잠금으로써 소유권을 밥에게 이전하는 거래가 생성됩니다.

거래 자체에는 앨리스나 밥과 관련된 어떠한 신원 정보도 포함되지 않습니다. 다이어그램은 앨리스로부터 자금을 받은 밥이 이제 해당 자금을 사용할 수 있는 개인키를 소유하게 되었음을 보여줍니다. 그는 거래 T2를 사용해 자금을 캐롤에게 이전합니다. 캐롤은 이후 거래 T3에서 자금을 데이브에게 이전합니다.

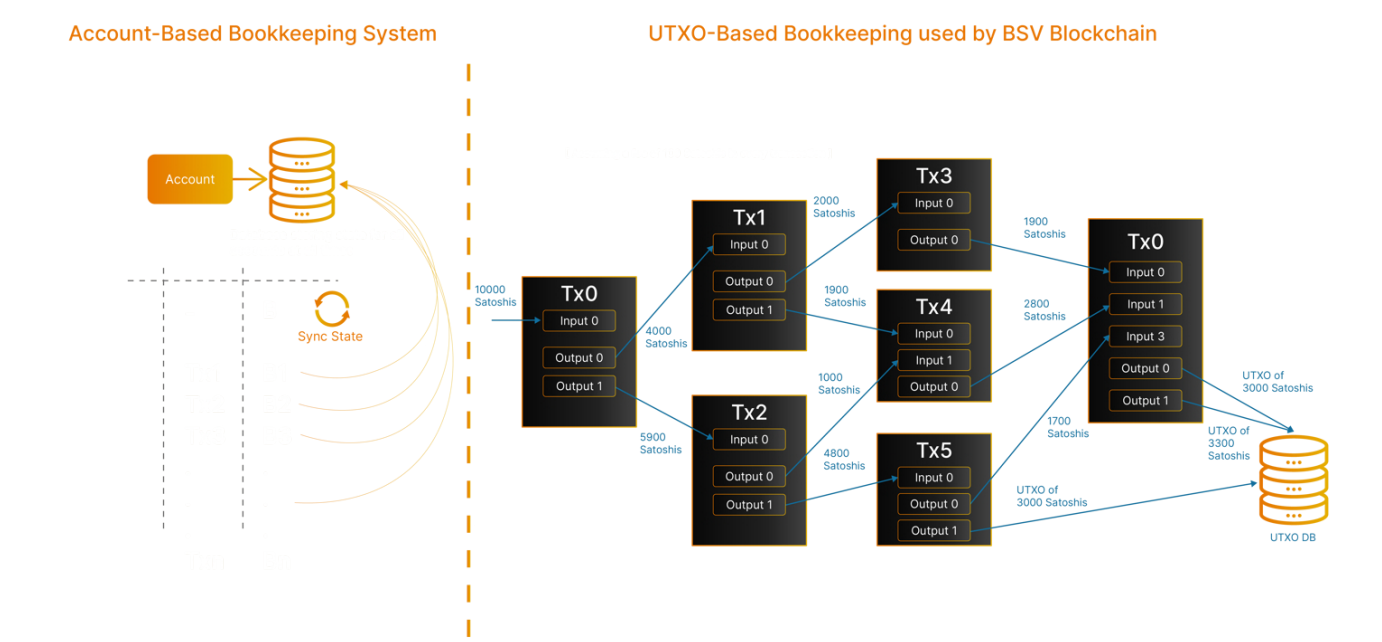


모든 블록의 첫 번째 거래는 "코인베이스 거래(Coinbase transaction)"라고 불립니다. 이 거래는 입력이 없으며 단일 출력을 가지는데, 이는 작업증명(Proof of Work)이라 불리는 과정에서 관련 블록을 블록 체인에 추가할 권리를 획득한 노드에 대한 보상으로 새로운 코인을 유통에 도입하는 역할을 합니다. 이 보상은 블록 보조금(block subsidy)과 거래 수수료(transaction fees)라는 두 가지 구성 요소로 이루어져 있습니다. 자세한 내용은 [network-policies](#) 및 [transaction-lifecycle](#)를 참조하십시오.

블록체인은 두 가지 뚜렷한 체인을 가지고 있습니다. 블록의 체인과 다수의 코인 체인입니다. 블록의 체인은 이미 설명했으므로, 여기서는 (다수의) 코인 체인을 살펴봅니다. 백서에 따르면 "코인은 디지털 서명의 체인으로 정의된다"고 되어 있습니다. 어느 시점에서든, 코인 또는 UTXO 자금은 해당 토큰이 최초로 유통에 들어오게 한 코인베이스 거래까지의 전체 거래 이력을 추적할 수 있습니다. 이 두 체인은 함께 시간 속에서 불변의 사건 체인, 즉 타임체인(time-chain)을 형성합니다.

아직 입력으로 사용되지 않은 거래 출력, 즉 소비되지 않은 출력은 UTXO(Unspent Transaction Output)라고 불립니다. 은행에서 모든 계좌의 총 계좌 잔액이 은행에 존재하는 총 자금을 나타내는 것처럼, 블록체인에서는 이 UTXO들이 집합적으로 특정 시점에 시스템 내에서 후속 거래에 사용할 수 있는 모든 토큰을 나타냅니다.

아래 다이어그램은 이러한 비교를 설명하면서 동시에 UTXO의 생성과 소멸 과정을 보여줍니다. 블록체인은 언제든지 존재하는 모든 UTXO의 현재 상태를 저장하는 UTXO 데이터베이스를 유지합니다.



### 비트코인 프로토콜에 의해 정의된 회계의 UTXO 모델

계정(Account)과 UTXO를 처리하는 방식에는 상당한 차이가 있습니다. 단일 소유자는 하나의 키에 대해 여러 개의 UTXO를 가질 수 있으며, 심지어 각 UTXO마다 하나의 키 쌍을 가질 수도 있습니다. 계정과 달리, 소유자의 신원은 UTXO에 연결되지 않으며 계정 잔액을 유지할 필요도 없습니다(이는 계정 기반 시스템에서는 매우 일반적입니다).

UTXO 모델은 블록체인이 거래 처리를 병렬화할 수 있도록 하며, 이는 블록체인을 확장하는 데 있어 중요한 요소입니다.

비유하자면, UTXO는 지폐와 같습니다. \$100 지폐를 가지고 있을 때 \$50 물건을 사면 원래의 지폐는 건네지고 더 이상 당신의 소유가 아닙니다. 대신 \$50 거스름돈을 새 지폐로 받게 되며, 원래의 \$100 지폐는 당신의 소유에서 사라집니다.

같은 방식으로, 100 사토시의 UTXO를 소비하면 그 중 50 사토시의 소유권은 새로운 소유자에게 이전되고, 10 사토시를 수수료로 지불할 수 있으며, 40 사토시의 새로운 UTXO가 생성됩니다. 이 새로운 UTXO는 원래 소비된 동일한 공개키에 할당될 수도 있지만, UTXO의 속성(새로운 거래 내 UTXO의 위치)이 바뀌었기 때문에 새로운 UTXO가 됩니다.

**안전 금고 비유로 이해하는 UTXO**  
계정 시스템과 달리, 개별 사토시 토큰은 각각 별개의 항목이며 비트코인은 일련의 토큰들로 구성됩니다. 이러한 토큰들은 UTXO라 불리는 봉투에 함께 담기게 됩니다. 봉투는 이후 수많은 안전 금고가 있는 가상 방 안의 안전 금고에 잠기게 됩니다. 안전 금고 번호는 대부분의 락킹 스크립트와 연관된 공개 주소나 공개키의 식별자와 동일한 개념입니다. 이 식별자는 여러 봉투를 보관할 수 있으며, 앞서 언급한 것처럼 각 봉투가 토큰들의 집합을 보관하는 여러 UTXO를 가질 수도 있습니다.

따라서, 안전금고는 여러 번 사용할 수 있습니다. 안전금고를 재사용한다는 것은 사람들이 당신이 그것을 사용하는 것을 볼 수 있다는 의미이며, 그 결과 프라이버시를 잃게 됩니다. 그러나 실제적으로는 방 안에서 필요한 만큼의 새로운 안전금고를 생성할 수 있습니다.

사토시 토큰은 절대 사라지지 않습니다. 따라서 시스템은 처음 생성되었을 때와 항상 동일한 수의 토큰을 보유합니다. 토큰은 대체될 수 있습니다. 이는 원장이 갱신됨에 따라 다양한 방법으로 수행될 수 있습니다. 만약 키를 잃어버린다면, 이는 안전금고의 키를 잃어버린 것과 같습니다. 안전금고에 접근할 수는 있지만, 그것은 비용과 시간, 그리고 노력이 필요합니다. 예를 들어, 안전금고에 \$5가 들어있는데 키를 다시 찾는 데 드는 비용이 \$5,000이라면, 그 금고에 다시 접근하려고 하지 않을 가능성이 큼니다. 하지만 금고에 \$5,000,000이 들어있다면, 반드시 비용과 노력을 들여 접근하려 할 것입니다.

분실된 토큰은 시스템을 깨뜨리지 않습니다. 대신 사람들이 더 큰 금액/가치의 토큰에 대해 구매 기록을 유지해야 하도록 만듭니다. 소액에 대해 복구 과정을 사용하는 것은 비현실적이며, 이러한 방법은 큰 금액의 UTXO를 복구하는 경우에만 사용됩니다. 이는 비트코인이 현금으로 설계되었기 때문이며, 현금은 수십억 달러를 안전금고에 보관하는 시스템으로 설계되지 않았기 때문입니다.

## 거래 입력과 출력(Transaction Inputs and Outputs)

전통적인 결제 시스템에서는 계정 기반 원장(차변, 대변)을 사용하기 때문에 거래는 단일 입력과 단일 출력을 가집니다. 반면, 비트코인의 UTXO 기반 원장은 거래가 여러 입력과 여러 출력을 가질 수 있도록 합니다.

각 출력은 술어(predicate, 참 또는 거짓으로 평가됨)인 락킹 스크립트를 포함하며, 이는 새로운 거래에서 입력으로 포함될 때 참으로 평가되기 위해 필요한 누락된 정보를 올바르게 제공받아야 합니다. 이러한 특성으로 인해 거래는 공개 원장과 결합될 때 전자 계약으로 기능하게 됩니다. 락킹 스크립트는 Script(일반적으로 비트코인 스크립트라 불림)라는 네이티브 프로그래밍 언어를 사용하여 다양한 전자 계약을 네이티브하게 지원할 수 있습니다.

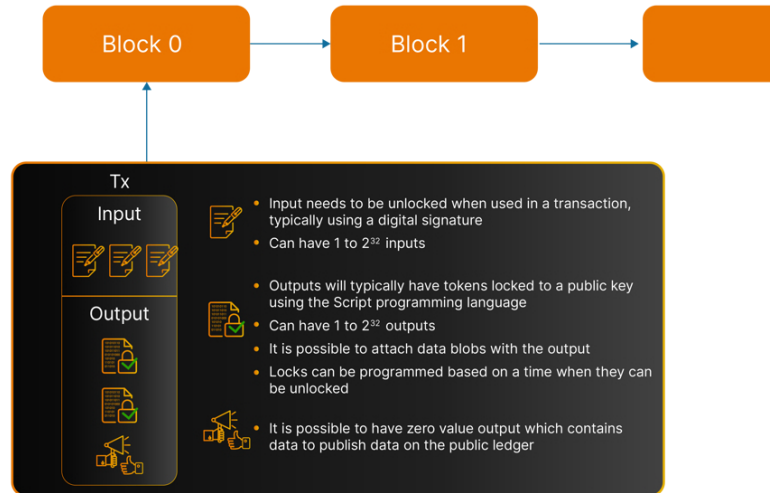
- Bitcoin은 익명성(Anonymous)과 사생활(Private)을 보장하지 않는다
- 비트코인 거래는 익명성(Anonymous)과 사생활(Private)을 보장하지 않는다
- 비트코인 거래는 익명성(Anonymous)과 사생활(Private)을 보장하지 않는다
- 비트코인 거래는 익명성(Anonymous)과 사생활(Private)을 보장하지 않는다



Anonymous



Private



## 거래 입력과 출력

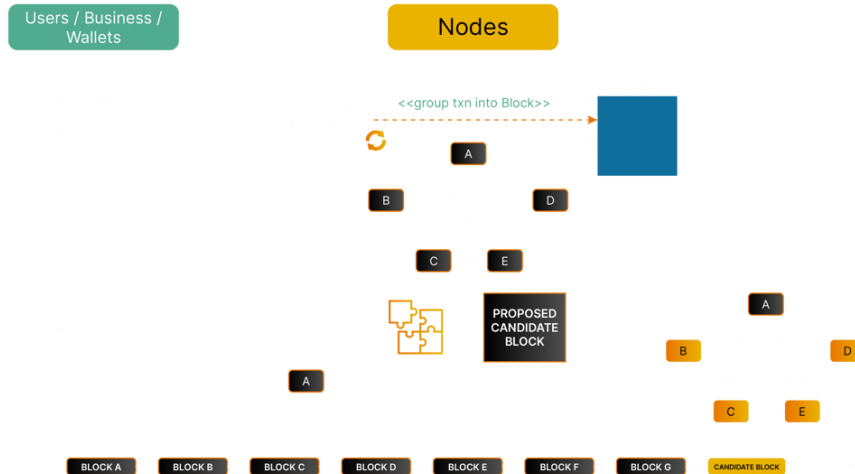
이러한 거래들은 사실상 하나의 체인을 형성합니다. 코인은 유통에 처음 등장하는 시점(모든 블록의 첫 번째 거래)부터 현재 특정 소유자의 공개키에 할당된 지점까지 여정을 이어갑니다. 이러한 구조는 코인을 디지털 서명의 체인으로 기능하게 만드는 핵심입니다.

## 작업증명(Proof of Work)

작업증명(Proof of Work, PoW)은 서로 신뢰하지 않는 많은 노드들이 블록체에서 “다음” 블록을 추가하기 위해 경쟁하는 네트워크 합의 과정입니다. 각 노드는 자신이 수신한 거래들을 기반으로 블록을 생성하고, 이를 네트워크에 제안하여 합의를 요청합니다. 노드의 다수가 해당 제안에 동의하면, 그 블록은 블록체인에 유효한 블록으로 추가됩니다. 네트워크의 모든 노드는 언제든지 블록을 제안할 수 있으며(이를 후보 블록(candidate block)이라 부름), 채굴 퍼즐의 해답을 찾았을 때에만 네트워크에 해당 블록의 세부 정보를 알립니다. 모든 노드는 이 채굴 퍼즐의 해답을 찾기 위해 경쟁하지만, 네트워크 합의 과정에서는 제안된 블록의 유효성을 보장하기 위해 서로 협력합니다.

이 과정을 관찰해보면, 노드가 정직하게 검증을 수행하는 것이 스스로의 이익에 부합함을 알 수 있습니다. 왜냐하면 그들은 자신들의 블록 제안을 구축하기 위해 고비용의 자원을 투입하기 때문입니다.

아래 다이어그램은 이를 보여줍니다.



## 작업증명(Proof of Work)

이 다이어그램은 블록체인 네트워크를 클라이언트-서버 아키텍처에 비유하여 설명합니다. 클라이언트는 거래를 생성하는 네트워크 사용자이며, 서버는 새로운 블록을 생성하고 블록체인의 운영을 유지하기 위해 작업 증명 과정에 참여하는 노드들의 네트워크를 나타냅니다. '클라이언트'는 거래를 '서버'에 제출합니다. 서버인 노드 네트워크는 각 노드가 수신한 모든 거래를 네트워크 내의 다른 모든 노드와 공유하며 협력하는 동시에, 거래 블록을 제안하여 다음 블록이 될 수 있도록 경쟁합니다. 이 경쟁은 고성능 장비를 사용해 풀어야 하는 퍼즐이며, 해답이 발견되면 노드들은 다시 협력하여 제안된 블록을 검증합니다. 모든 노드가 단일 해답에 동의하면, 새로운 블록은 블록체인에 추가됩니다.

노드 네트워크는 네트워크 사용자로부터 거래를 처리하는 노드들로 구성됩니다. 이 노드들은 비트코인 프로토콜을 구현하는 특수화된 소프트웨어를 실행하며, 엄격한 규칙 집합에 따라 작동하고 네트워크 내에서 그 규칙을 집행하는 역할을 합니다. 좋은 비유로, 노드는 국가에서 사법부와 의회가 만든 법률을 집행하는 경찰과 같습니다.

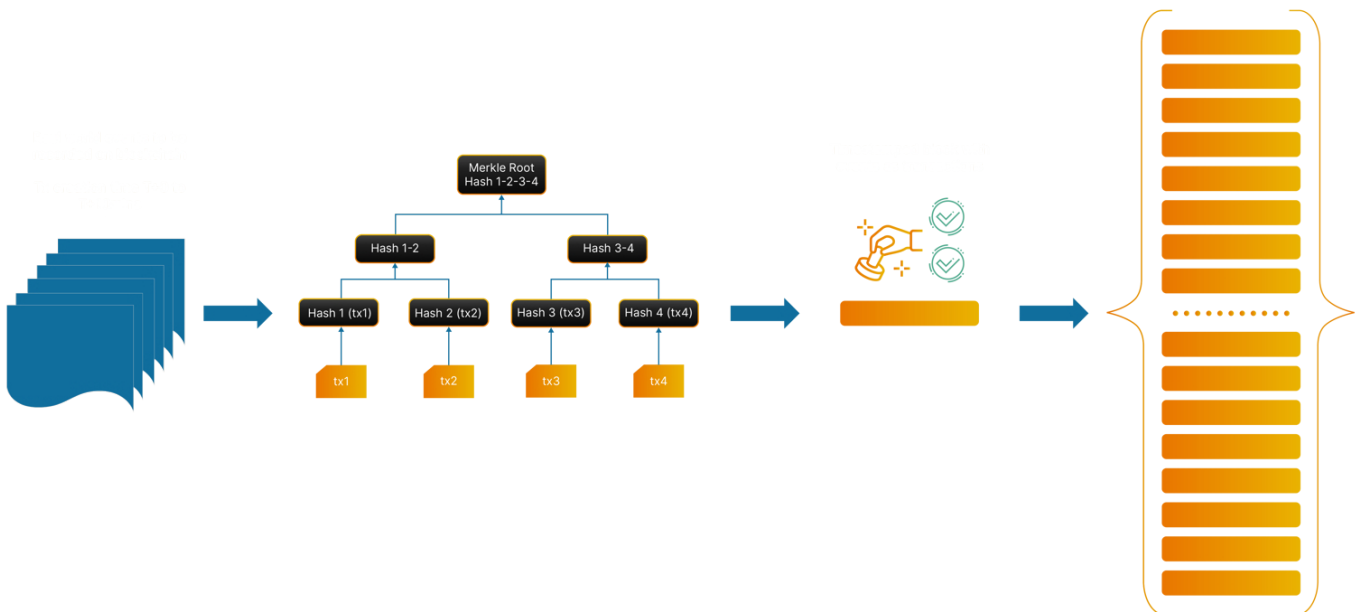
이 과정은 *network-policies*에서 더 자세히 설명됩니다.

## 기능(Capabilities)

BSV 블록체인을 혁신적으로 만드는 두드러진 속성은 다음과 같습니다:

- **불변성(Immutability)** - BSV 블록체인은 거래와 데이터의 불변 원장으로, 각 블록에는 타임스탬프가 부여됩니다. 수학적 관점에서 블록체인은 사건 'e'가 시간 't'에 발생했다는 영구적 증거를 기록합니다. 블록체인은 불변성을 달성하기 위해 두 가지 개념에 의존합니다: 분산 타임스탬프 서버(distributed timestamp server)와 작업증명(proof of work)입니다. 분산 타임스탬프 서버는 블록의 거래들을 해시하고, 블록 생성 시점의 유닉스 시간 값과 함께 블록 헤더에 연결합니다. 이 해시는 블록에 고유하며, 블록의 내용으로부터 생성되기 때문에, 내용을 변경하면 블록 생성 당시 블록 헤더에 저장된 해시가 무효화됩니다. 이 해시를 생성하기 위해 채굴자는 자본 지출(cap-ex)에 투자하고, 반복되는 전기 요금이라는 상당한 운영 비용(op-ex)을 지불해야 합니다. 채굴자가 자신이 해당 블록을 채굴했음을 증명하기 위해서는 작업증명을 제시해야 하며, 이는 네트워크 내 다른 채굴자들

에 의해 쉽게 검증될 수 있습니다. 작업증명은 암호학적 도전 또는 퍼즐의 일종으로, 이를 해결하기 위해서는 매우 높은 해시 파워(계산 자원)가 필요하지만, 일단 해답이 있으면 검증은 매우 쉽습니다. 이름에서 알 수 있듯, 이는 채굴자가 상당한 양의 계산 자원을 투입했음을 네트워크에 입증합니다.



- 분산성(Distributed)** - 소비자와 기업에게 노드 네트워크는 분산 네트워크입니다. 프로토콜은 각 노드가 블록체인에 대해 동의하고 동일한 복사본을 보유할 것을 요구합니다. 각 노드는 동일한 불변 규칙 집합을 실행하며, 이는 노드 소프트웨어의 일부로 프로그래밍되어 있습니다. 이는 네트워크에 회복력을 제공하여, 최종 사용자에게 단일 장애 지점(single point of failure)이 발생하지 않도록 합니다. 또한 네트워크에 신뢰 불필요성(trustlessness) 요소를 추가하여, 최종 사용자가 거래의 무결성을 검증하기 위해 단일 노드를 신뢰할 필요가 없게 만듭니다. 마지막으로, 이는 특히 기업을 포함한 최종 사용자에게 시스템을 경제적으로 만듭니다. 각 거래마다 수수료가 부과되는데, 채굴자들이 더 많은 거래를 처리하기 위해 서로 경쟁함에 따라 이 수수료는 협상될 수 있습니다. 노드들은 서로 초연결(hyper-connected) 상태에 있으며, 네트워크가 성숙해짐에 따라 노드 간 네트워크 토폴로지는 소규모 세계(small-world) 또는 만다라(mandala) 네트워크로 발전하게 됩니다.



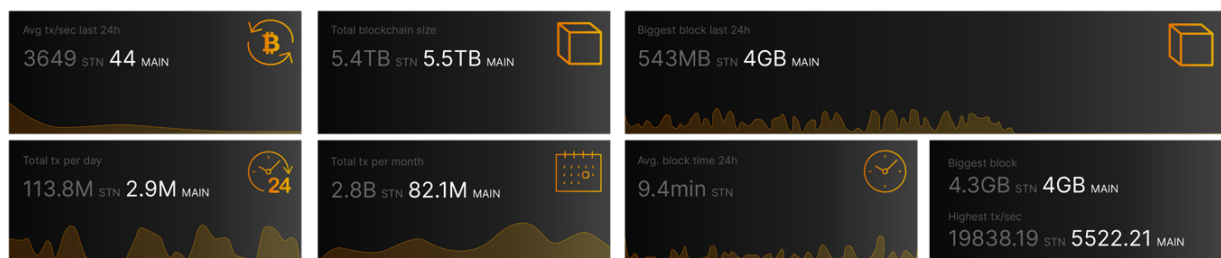
- 프라이버시와 책임성(Privacy and Accountability)** - 비트코인 프로토콜은 거래 당사자의 신원을 분리함으로써 프라이버시를 처리합니다. 자금을 이전하기 위해 송신자는 개인키를 사용하여 코인의 소유권에 서명해야 하며(개인키 자체는 공개되지 않음), 동일한 거래에서 수신자의 공개키가 이전된 코인과 연결됩니다. 이는 원장이 투명하고 감사 가능한 상태를 유지하면서도 사용자에게 가명성(pseudonymity)을 제공합니다. 추가적으로, 원장의 불변성은 책임성을 의미합니다. 블록 내의 거래는 삭제되거나 변경될 수 없기 때문에, 개인과 기업의 디지털 흔적이 영구히 저장되어 책임성을 강화합니다. 비트코인을 이용한 불법 또는 범죄 행위는 불변의 증거 경로를 통해 쉽게 추적될 수 있으며, 따라서 법 집행 시스템에 의해 제재를 받게 됩니다.
- 보안(Security)** - 기존의 많은 시스템과 마찬가지로, 보안은 사용자와 프로토콜 모두의 책임입니다. 개인과 기업에게는 이 주제의 범위를 벗어난 권장 보안 모범 사례가 있으며, 프로토콜의 관점에서는 경제적 보안(economic security)의 철학을 구현합니다. 이에 대한 여러 측면은 다음과 같습니다:
  - 원장 데이터베이스에 접근할 수 있는 키는 블록체인 자체에 저장되지 않고 다양한 시스템에 분산되어 있어, 공격자가 시스템을 공격하는 것이 경제적으로 비합리적입니다. 이는 신용카드 정보와 같은 민감한 데이터가 단일 데이터베이스에 저장되어 해킹에 취약한 기존 시스템과는 다릅니다.
  - 거래 무결성, 특히 이중지불(double spend)에 대한 책임은 채굴자에게 있으며, 프로토콜은 블록을 채굴한 채굴자뿐만 아니라 대다수의 노드가 동일한 검증을 수행해야 블록이 유효하다고 인정되도록 요구합니다.
  - 마지막으로, 경제적 측면은 작업증명에 연결된 인센티브입니다. 노드가 블록을 채굴하고 비즈니스를 수익성 있게 운영하기 위해서는 해시 파워 측면에서 막대한 투자가 필요합니다. 프로토콜은 노드가 동일한 불변 규칙 집합을 준수하여 합의의 형성할 것을 요구합니다. 만약 어떤 노드가 유효하지 않은 거래를 블록에 포함시키기 위해 해시 파워를 낭비한다면, 다른 노드가 그 블록을 수용하지 않기 때문에 수익 창출 능력이 제한됩니다. 또한 어떤 노드가 블록체인 내 거래를 덮어쓰려 한다면, 프로토콜은 그 노드가 새로운 작업증명 체인을 구축하고 끊임없이 길어지는 블록체인 체인 팁(chain-tip)을 따라잡아야 유효한 것으로 인정하도록 요구합니다. 이는 블록에 기록된 거래를 변경하거나 삭제하는 것을 계산적으로 불가능하게 만듭니다.
- 연합 네트워크 합의(Federated Network Consensus)** - 비잔틴 장군 문제(Byzantine Generals Problem)는 분산 컴퓨팅에서 노드 간 합의를 확립하여 시스템의 신뢰성을 유지하는 문제를 다룹니다. 프로토콜에서 사용되는 합의 메커니즘은 “하나의 CPU, 하나의 투표(one CPU, one vote)”이며, 이는 네트워크 내에서 채굴자가 보유하고 지속적으로 사용하는 CPU의 수에 따라 투표 비율이 결정됨을 의미합니다. 비잔틴 장군 문제의 관점에서 각 노드 또는 채굴자는 장군에 해당하며, 투표 비율은 군대의 규모, 즉 퍼즐을 풀기 위해 채굴자가 투자하고 사용하는 CPU 수에 비례합니다. 이러한 투자는 일반적으로 “게임에 피부를 걸었다(having skin in the game)”라고 불리며, 이는 채굴자가 네트워크에 대해 정직하게 행동하도록 보장하고, 인센티브를 유지하려는 동기를 부여하여 비잔틴 장군 문제에 대한 경제적 해결책을 제공합니다.
- 확장성(Scalability)** - 블록체인의 확장성과 관련하여, 엔터프라이즈 제품 설계는 블록 크기와 개별 거래 크기의 두 가지 측면을 고려해야 합니다:
  - 블록 크기(Block size)** - 2020년, BSV 블록체인의 메인 네트워크는 100만 건 이상의 거래가 포함된 340MB 블록을 처리했으며, 곧 이어 130만 건의 거래가 포함된 369MB 블록을 처리했습니다. 2023년까지 네트워크가 처리한 가장 큰 블록은 4GB에 달했으며, 일부 날에는 단일 일자에 5천만 건 이상의 거래가 처리되었습니다. 메인 네트워크는 초당 2,800건의 거래를

안정적으로 처리하며, 확장성 테스트 네트워크는 초당 최대 6,000건의 거래를 처리한 기록이 있습니다. 현재 노드 소프트웨어를 모놀리식(monolithic) 구조에서 모듈형/마이크로서비스 아키텍처로 재설계하여 추가 확장을 준비하고 있습니다. 목표는 초당 100만 건의 거래를 처리하는 것으로, 이는 BSV를 현재 가장 확장 가능한 블록체인으로 만듭니다. 큰 블록을 허용하는 중요한 결과 중 하나는 채굴자의 거래 수수료를 낮추는 것이며, 이는 BSV를 소액 결제를 지원하는 유일한 블록체인으로 만듭니다.

2. **개별 거래 크기(Individual Transaction size)** - 프로토콜은 또한 거래 수준에서 확장성을 제공하며, 거래에서 가치를 교환하는 엔터티 간 다양한 계약 유형을 지원하기 위해 Script라는 네이티브 언어를 사용합니다. 거래 내에 존재하는 이러한 스크립트는 단순한 결제 정보(디지털 서명, 가치 등)뿐 아니라 데이터를 포함할 수도 있습니다. 프로토콜은 입력 또는 출력의 수에 제한을 두지 않으며, 각 스크립트는 최대 4.2GB의 데이터 항목을 가질 수 있습니다. 이를 통해 비트코인 거래는 결제 및 데이터 거래로 모두 기능할 수 있으며, 비트코인 원장은 실제 데이터 원장으로 발전할 수 있습니다.

- **피어-투-피어 교환(Peer-to-peer exchange)** - 프로토콜에는 신뢰하지 않는 당사자 간의 피어-투-피어 거래를 가능하게 하는 두 가지 중요한 기능이 있습니다. 하나는 단순화된 결제 검증(Simplified Payment Verification, SPV)이고, 다른 하나는 거래 입력을 위한 결제 채널(Payment channel)입니다. 주목할 점은 이 두 기능 모두 비트코인 프로토콜을 사용하는 기업에 확장성과 비용 효율성을 향상시킨다는 것입니다. SPV는 블록체인 사용자가 자신이 생성한 거래에 초점을 맞춘 최소한의 인프라만을 실행할 수 있도록 하여, 블록체인을 운영하는 데 드는 비용을 거의 무시할 수준으로 만듭니다. 결제 채널은 블록체인에 단일 거래만 기록하면서도 일련의 상호 연결된 거래(마치 하위 원장(sub-ledger)과 유사함)를 구축할 수 있는 메커니즘입니다. 이러한 상호 연결된 거래는 비즈니스 사용 사례에 따라 언제든지 단일 거래로 전환될 수 있습니다. 처리량 제공뿐 아니라 블록체인은 거래를 최소한의 수수료로 처리하는데, 이는 일관되게 미화 1센트의 100분의 1보다 적습니다.

안정적인 기본 프로토콜과 기술적 기반이 마련되면서, 이 혁신은 의료, e스포츠, 공급망 관리, 사물인터넷, 빅데이터 애플리케이션, 송금, 분산 네트워크 인텔리전스, 개인화된 신원 시스템 등 다양한 산업에서 새로운 데이터 비즈니스 모델의 등장을 가능하게 할 잠재력을 가지고 있습니다.



확장성, 안정성, 보안성, 그리고 즉시 거래를 기반으로 구축된 BSV 블록체인은 기업들에게 올바른 선택이 될 것을 약속합니다. 이는 소액결제 기능을 제공하여 기존 비즈니스 모델을 혁신합니다. 또한 데이터 무결성과 사기 탐지 기능을 제공함으로써 기업을 보호합니다. 공개 원장으로서, 회계와 장부 기록에 투명성을 도입합니다. 소액결제 플랫폼(핵심 기능 중 하나)을 제공함으로써, 현재 광고 기반 인터넷 모델을 넘어 데이터 경제가 진화할 수 있는 대안을 마련합니다. 이 기술은 아직 초기 단계에 있으며, 블록체인이 제공하는 고유한 기능을 활용한 혁신이 활발히 진행되고 있습니다.

# 거버넌스의 경제 모델(Economic Model of Governance)

비트코인 프로토콜이 가져온 혁신은 추적 가능한 가명 거래 시리즈에 연결된 경제 시스템이었습니다. 작업증명(Proof of Work) 기반 암호화폐, 타임스탬프 서버 개념, 분산형 암호화폐는 수십 년 전부터 존재했습니다. 심지어 블록체인 개념(정보 블록을 해시하여 다음 블록에 연결하는 방식)도 25년 전에 처음 발표되었습니다.

작업증명 과정은 "**경제적 매체**": **게임 이론적 신호 시스템**으로서의 본질이 더 잘 이해되어야 합니다. 게임 이론에서, 예를 들어 공작새를 살펴볼 수 있습니다. 공작새는 꼬리의 크기를 통해 자신의 건강과 체력을 신호합니다. 꼬리가 너무 길면 포식자로부터 도망칠 만큼 강하지 못해 결국 죽게 되고 번식할 수 없습니다. 반대로, 긴 꼬리를 가지고도 살아남는 공작새는 그 크기의 꼬리를 가진 채 생존할 수 있는 강인함을 암컷에게 증명합니다. 공작새의 꼬리는 실제 가치가 없기 때문에 신호로서 가치를 갖습니다.

PoW에 대한 투자는 경제적 신호의 한 형태입니다. 중요한 것은 그 신호가 비용이 많이 든다는 점입니다. 작업증명(공작새의 꼬리와 같이)은 거래를 검증하고 블록으로 정렬하여 네트워크를 보호하기 위해 인프라에 막대한 자금을 투자할 의지가 있음을 입증하는 수단이며, 다른 채굴자들도 이를 수익성 있게 검증할 수 있습니다. 블록 보상 보조금이 사라짐에 따라 거래 수수료의 중요성은 점점 커집니다. 시간이 지나면, 거래 정렬 이외의 다른 것에 주력하는 채굴자는 거의 보상을 얻지 못하게 됩니다. 작업증명 해싱 자체에는 다른 가치가 없으며, 이는 공작새의 꼬리와 같습니다.

채굴 노드들은 작업증명(PoW)을 통해 네트워크를 안전하게 유지하기 위해 손실을 감수하고 위험을 떠안겠다는 의지를 신호합니다. 그들은 네트워크에 투자하기 위해 막대한 금액을 지불할 의사가 있으며, 이를 통해 장기적인 헌신을 보여줍니다. 가장 중요한 점은, 채굴자들이 법 밖에서 행동하려 한다면 거대한 고정 자본 기반이 위험에 노출된다는 것입니다. PoW 채굴에서 가장 큰 통제 수단은 **기존의 법률 시스템**입니다. 만약 어떤 채굴자가 충분한 해시 파워를 가지고 정직한 노드들을 압도하면서 법 밖에서 행동하려 한다면, 이는 쉽게 탐지됩니다. 더 중요한 것은, 이들은 법정에서 증거로 인정될 수 있는 서명된 데이터를 제공하며, 형사 기소를 가능하게 합니다. 추가적으로, 다른 채굴자들도 법적으로 조치를 취할 수 있습니다. 이러한 조치에는 반경쟁 행위와 카르텔 기반 행동과 관련된 기타 보호 장치가 포함됩니다.

이러한 특성으로 인해, 비트코인 프로토콜에 의해 정의된 블록체인 시스템은 암호학적 시스템이 아니라 암호학을 사용하는 경제 시스템입니다. 이제 채굴 과정에 관련된 다양한 개념을 이해함으로써 이것이 어떻게 발생 하는지 더 깊이 살펴보겠습니다.

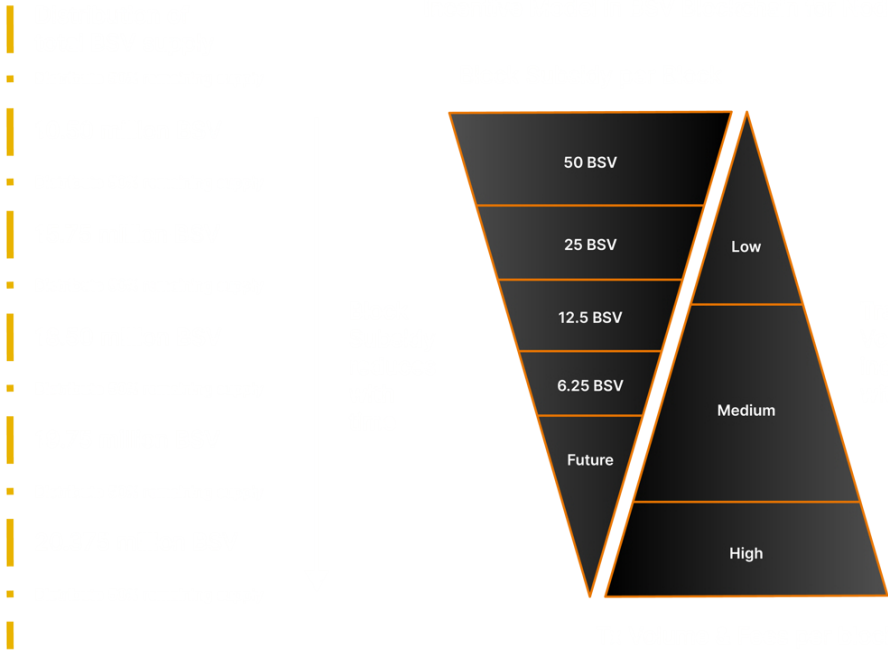
## 토큰과 그 분배(Token and its distribution)

블록체인 네트워크는 인센티브 구조 측면에서 독특하며, 이는 공공 네트워크의 보안에 필수적인 네트워크 내장 화폐를 포함합니다. BSV 블록체인의 경우, 네이티브 토큰은 비트코인(SV) 또는 간단히 BSV입니다. 이는 네트워크 내부에서 사토시(Satoshi)라 불리는 기본적인 불가분의 가치 단위를 나타내는 추상화입니다. 하나의 BSV 코인은 단지  $10^8$  사토시를 나타내는 액면 단위일 뿐입니다.

2009년 1월 네트워크가 시작될 때, 이 시스템에서 생성될 수 있는 모든 네이티브 토큰이 발행되었습니다(규칙 집합과 코드베이스에 명시됨). 시스템에는 2,100만 BSV 또는 2.1 경( $21,000,000 * 100,000,000$ )의 사토시 토큰이 있습니다. 이러한 토큰들이 생성되거나 발행될 당시, 전체 2.1경 토큰의 가치는 0이었습니다. 이 토큰들은 블록체인 네트워크에서 거래를 가능하게 하는 효용성에 따라 가치를 얻게 됩니다. 거래의 수가 많을수록 블록체인 네트워크의 효용성이 높아지며, 이는 토큰에 가치를 부여합니다. 요약하면, 토큰의 가치는 공개 시장에서의 거래와 상업 활동에서의 거래 효용성에 의해 결정됩니다.

이 토큰들은 블록 보조금(Block subsidy)이라 불리는 과정을 통해 네트워크 참여자들에게 분배됩니다. 이 메커니즘은 노드들이 거래를 처리하고 블록을 생성하는 기능을 수행하도록 재정적 인센티브 역할을 합니다. 블록 보조금은 4년마다 50%씩 줄어드는 감가(deprecating) 모델을 따릅니다. 2009년에는 블록당 50 BSV에서 시작했으며, 현재는 블록당 6.25 BSV이고, 2024년에는 블록당 3.125 BSV로 반감될 예정입니다.

앞으로 네트워크는 보조금이 최소화되며, 노드들의 수익 대부분은 거래 수수료에 의존하게 될 것입니다. 이는 아래 다이어그램에 설명되어 있습니다.



이는 네트워크가 거래 처리자로서 노드가 서비스를 제공하는 데 필요한 비용을 충당하기 위해 가능한 한 많은 거래량을 확보해야 함을 의미합니다. 이러한 거래량을 지원하기 위해서는 네트워크가 소액결제, 중앙은행 디지털 화폐(CBDC), 데이터 거래 및 디지털 계약 등 블록체인이 제공하는 다양한 사용 사례를 활용할 수 있어야 합니다.

네트워크에 네이티브 토큰이 존재하고 이를 거래 수수료로 사용하는 것의 부정적인 측면은 토큰 가격의 변동성으로, 이는 기업의 수익 예측 및 계획을 방해할 잠재력이 있다는 점입니다. 이는 토큰 가격이 네트워크 참여의 동력이자 투기적 투자 자산으로 작동하는 블록체인에서 흔히 나타나는 문제입니다. 그러나 BSV 블록체인의 경우(거래 수수료가 일반적으로 매우 낮게 설정되어 있음), 이는 우려할 필요가 없습니다. 현재 거래 수수료는 바이트당 0.05 사토시로, 300바이트 거래의 경우 총 수수료는 1센트의 1/1000 수준에 불과합니다. 설령 가격이 크게 변동하더라도 기업의 예산 및 수익 계획에 눈에 띄는 영향을 미칠 가능성은 매우 낮습니다.

토큰 시스템의 마지막 측면은 프로토콜에 의해 고정된 한정된 공급량입니다. 블록체인의 전체 보안은 토큰 교환과 관련됩니다. 예를 들어, 100명이 엔트리를 생성하려고 하지만 토큰이 99개만 있다면, 토큰을 전송하려는 경제적 인센티브(거래 수수료)가 발생합니다. 거래 수수료나 지불용 토큰 또는 그 밖의 무언가가 없다면 인센티브가 존재하지 않습니다. 현재 시장은 의사 100만 개에 플레이어 100명만 있는 의사 뺏기 게임과 같습니다. 그러나 미래에는 수십억 명의 플레이어와 단지 100만 개의 의사만 존재할 것입니다. 만약 거래가 토큰 이외의 다른 것으로 교환되며, 엔트리를 생성하기 위해 토큰을 교환하지 않는다면, 이는 무한한 수의 의자를 만들게 되어 게임의 본질을 바꾸는 것입니다.

## 네트워크 합의(Network Consensus)

블록체인은 새로운 블록을 누가 추가할 수 있는지를 결정하기 위해 비트코인 프로토콜에 정의된 네트워크 합의 방법론을 사용합니다. 이 방법론은 (채굴) 노드가 공인된 공개 엔터티가 되도록 특별히 설계되었습니다. 노드가 되려면 분산 원장을 저장하기 위한 데이터 센터(현재 수 테라바이트 규모)를 구축해야 하며, 강력한 계산 능력을 가진 기계가 필요한 작업증명(Proof-of-Work)이라는 계산 집약적 과정에 참여해야 합니다. 이러한 인프라는 예를 들어 법적 조치가 그들에게 취해질 경우, 해당 노드에게 경제적 비용이 발생함을 의미합니다.

이러한 시스템 설계에는 또 다른 이유가 있습니다:

작업증명 시스템에서는, 당신이 어제 무엇을 했는지 또는 오늘 무엇을 하는지가 내일 무엇을 할 것인지, 그리고 내일 무엇을 벌거나 통제할지를 결정하지 않습니다. 지속적인 투자의 요구가 작업증명 시스템의 본질을 바꿉니다.

비트코인 프로토콜은 가치 교환 시스템에서 신뢰할 수 있는 중개자를 신뢰할 수 없는 중개자로 대체하려고 했으며, 이를 위해 이러한 신뢰할 수 없는 엔터티가 정직하게 기능할 것을 요구했습니다. 이는 그들이 결코 "안주하지 못한다"는 것을 의미합니다. 위에서 설명한 PoW 시스템은 어떤 엔터티도(조기 참여, 영향력 등으로) 얻을 수 있는 모든 이점을 제거합니다. 그들은 "작업"을 수행하고 계산을 해결해야만 보상을 얻습니다. 이 방법론의 구현은 거래를 처리하기 위해 노드가 해야 하는 모든 것과는 상당히 독립적이며, 이는 노드 아키텍처 섹션에서 자세히 설명됩니다.

## 에너지 투자(Energy Investment)

PoW 시스템은 이러한 계산을 수행하기 위해 에너지에 대한 투자를 요구합니다. PoW 계산을 해결하는 데 필요한 에너지는 네트워크 난이도의 함수이며, 이는 약 10분에 한 번씩 계산이 해결되도록 난이도를 조정하는 수학적 알고리즘을 기반으로 합니다. PoW를 수행하기 위한 계산 자원이 크게 증가하면 난이도가 상승하고, 반대로 줄어들면 난이도가 하락합니다.

기술적으로, PoW 시스템은 네트워크가 각 블록에서 처리하는 거래 수와는 독립적입니다. 그러나 간접적으로는 다음과 같은 경제적 요인과 관련됩니다:

1. 거래 수는 수수료로 얻는 수익에 직접 비례하며, 점차적으로 수수료가 노드에게 주요 인센티브 원천이 될 것입니다.
2. 노드가 수행하는 계산에는 에너지가 필요하며, 블록 내 거래 수가 많을수록 거래당 소비되는 에너지는

줄어듭니다.

3. PoW는 기존 참여자에게 부당한 이점을 제거하므로, 독점의 가능성을 없앱니다.

```
{% hint style="info" %}
```

PoW 시스템에 의해 운영되는 노드, 원장의 공개적 성격, 신원과의 분리라는 세 가지 요소가 블록체인의 가치를 만듭니다. 이러한 특징은 결제 시스템에서 신뢰할 수 없는 중개자를 처음으로 가능하게 합니다.

```
{% endhint %}
```

이제 이러한 배경을 바탕으로, 원래 프로토콜이 블록체인에 반드시 존재하도록 의도했지만 다른 어떤 블록체인도 가지지 못한 가장 독특하고 이례적인 개념 중 하나를 살펴보겠습니다. 그것은 합법적 관할권이 블록체인 상에서 자산을 압류하고 기록에 대한 수정 명령을 내릴 수 있는 방법과 시스템입니다.

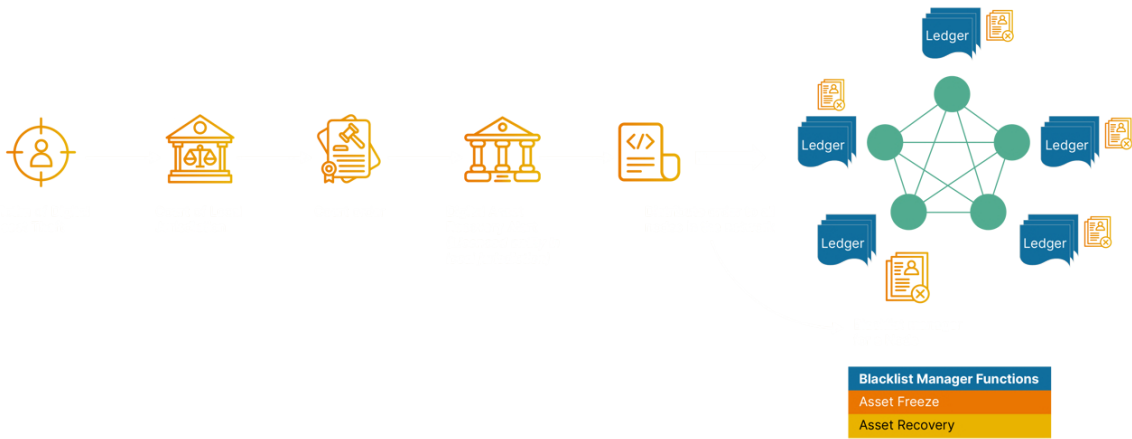
## 디지털 자산 복구(Digital Asset Recovery)

비트코인 프로토콜에 명시된 작업증명(Proof-of-Work) 합의에 기반한 블록체인은 가치 교환 네트워크에서 신뢰할 수 있는 중개자를 거래 활동에 무관한 신뢰할 수 없는 노드들로 대체합니다.

이는 거래 수수료를 지불할 의사가 있는 누구나 네트워크를 개방적이고 허가 없이 사용할 수 있도록 허용합니다. 그러나 동시에 이는 공개 원장에 악성 콘텐츠를 게시하거나 키 도난, 기타 사기 행위 등 다양한 공격 벡터에 시스템이 취약해지게 만듭니다.

비트코인 프로토콜은 이를 경고 시스템(Alert System)이라 불리는 메시징 시스템을 사용하여 해결했습니다. 이를 통해 노드들은 네트워크의 건강을 유지하고 악의적 행위로부터 보호하기 위한 메시지를 교환할 수 있었습니다. 최근 수립된 디지털 자산 복구(Digital Asset Recovery) 프로세스는 경고 시스템의 사용 사례 중 하나를 표준화된 거버넌스 체계와 함께 구현한 것으로, 블록체인 네트워크에 적용되었습니다. 또한 이는 네트워크 내 사법부 및 법률 시스템과의 인터페이스 역할을 하여 불법 행위의 무고한 피해자들에게 구제 메커니즘을 제공합니다.

BSV는 설계상 합법적 권리를 가진 소유자가 분실된 자산(토큰)을 법적으로 복구할 수 있도록 허용하는 유일한 블록체인입니다. 동일한 시스템은 법원의 금지 명령 및 법적 통지에 따라 자산을 동결할 수도 있습니다. 이 과정은 블록체인 시스템이 현재 모든 금융 시스템이 법적으로 적용받는 것과 동일한 법률 체계 하에서 운영되도록 합니다. 또한 이는 공개 원장이 악의적 행위자들에 의해 직면할 수 있는 불법 활동을 억제하는 역할을 합니다.



네트워크의 모든 노드는 법원에서 발행한 자산 동결 및 복구 명령을 포함하는 블랙리스트를 유지합니다. 이러한 명령에는 불법 행위와 관련되어 법원에서 동결을 요청한 UTXO 주소가 포함될 수 있습니다. 또한 자산 복구 명령은 법원 판결을 통해 정당한 소유자로부터 도난당한 자금을 복구하기 위해 UTXO에서 복구 UTXO로 자금을 재할당하는 것을 포함할 수도 있습니다. 이 시스템은 블록체인의 다음과 같은 속성을 설명합니다.

1. 기존 법률 체계가 자금의 소유권을 규정하며, 블록체인 토큰은 동일한 규칙을 따릅니다.
2. 블록체인의 불법 사용은 자금과 주소를 쉽게 동결할 수 있고 복구가 신속히 이루어질 수 있기 때문에 억제됩니다.
3. 노드는 자신이 속한 현지 관할권의 법원 명령을 따라야 하며, 이를 통해 동일한 관할권에 의해 규제됩니다.

## 네트워크 정책(Network Policies)

비트코인 프로토콜은 블록체인의 노드 네트워크와 그 작동 방식을 정의합니다. 그 기본 전제는 다음과 같습니다:

- 노드는 블록체인에 새로운 블록을 추가하는 네트워크 행위자입니다.
- 노드(채굴자라고도 함)는 다음과 같은 능력으로 특징지어집니다:
  - 블록을 생성한다.
  - 블록을 다른 피어(다른 노드)에게 배포하고, 수신한 블록을 검증한다.
  - 발견한 블록을 네트워크 피어들에게 배포한다(이는 전체 블록과 그 내용을 배포한다는 의미는 아님. 다른 노드들은 이미 발견된 블록 내의 거래 대부분, 또는 적어도 대다수를 이미 보유하고 있기 때문임).
  - 거래를 처리(검증)한다.
- 가장 긴 블록 체인이 올바른 체인이며, 새로운 블록을 생성하는 데 사용된다.
- 노드는 네트워크의 규칙을 집행하며, 이 규칙을 만들거나 수정하지 않는다. 좋은 비유로, 노드는 도시에서 법을 집행하는 경찰과 같지만, 법을 만들거나 수정하지는 않는다.

- 새로 발행된 코인은 각 블록의 첫 번째 거래(코인베이스 거래)에서 생성되는 블록 보상 중 블록 보조금에서 유통에 추가된다. 이 과정에서 노드는 발행자가 부당한 일방적 계약에 의해 노드의 기능을 수행할 의무가 있으며, 이를 수행하지 못하면 계약을 위반하게 되고 발행자가 결정한 법적 구제에 책임을 지게 된다.
- 노드는 자신이 보게 되는 모든 거래를 자신이 생성하려는 블록에 포함시켜야 하는 계약적 의무를 가진다. 때로는 수수료가 없는 거래도 있을 수 있으며, 수수료가 있는 거래와 무료 거래 사이에서 우선순위를 정해야 하는 상황에 도달할 때까지는 이러한 거래들도 허용해야 한다. 이 시점에 이르면 무료 거래를 무시할 수 있다.
- 노드는 네트워크 사용자(예: 도난당한 자금을 이동하는 해커나 이중 지불 시도) 또는 네트워크를 공격하는 불성실한 채굴 노드로부터 네트워크를 보호해야 하는 계약적 의무를 가진다.

노드는 항상 블록을 생성하는 엔터티입니다. 단순히 노드 소프트웨어를 실행하지만 새로운 블록을 생성하지 못한 엔터티는 실제로 블록 생성 과정에 참여하지 않으며 네트워크에 어떠한 가치도 더하지 않습니다. 따라서 네트워크는 이들을 노드로 인정하지 않습니다.

프로토콜 사양에 따르면, 네트워크의 블록 생성 난이도는 2주마다 재조정됩니다. 블록당 평균 시간이 10분이라는 기준에 따라, 최대 2주 동안 2016개의 블록이 생성될 수 있습니다. 따라서 2016이라는 값은 네트워크 내에서 어느 시점에서든 가능한 노드 수의 상한이 됩니다(매번 다른 노드가 블록을 생성한다고 가정할 경우). 평균적으로 어느 시점에서든 3~5개의 대형 노드와 몇 개의 소형 노드가 존재하게 됩니다. 이는 네트워크가 가진 탈중앙화 수준을 정의하기도 합니다.

현재 BSV 블록체인의 경우, 동일한 해싱 알고리즘을 사용하는 여러 블록체인 포크가 존재하기 때문에 네트워크 보안상의 고려로 블록 생성 후마다 난이도가 조정됩니다.

이제 노드의 정의를 이해했으므로, 블록체인의 특정 시점에서 현재 상태를 정의하는 가장 긴 체인(longest chain) 개념을 이해하는 것도 중요합니다.

## 가장 긴 체인(Longest Chain)

백서는 프로토콜에서 가장 긴 체인을 다음과 같이 정의합니다:

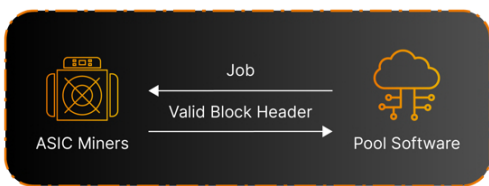
*작업증명은 본질적으로 하나의 CPU가 하나의 투표이다. 다수의 결정은 가장 긴 체인으로 표현되며, 그 체인에는 가장 많은 작업증명 노력이 투입되어 있다. 만약 다수의 CPU 파워가 정직한 노드들에 의해 통제된다면, 정직한 체인이 가장 빠르게 성장하며 모든 경쟁 체인을 앞지르게 된다.*

이 설명은 종종 네트워크의 모든 참여자에게 민주적 권리를 제공하는 시스템으로 이해되어 왔습니다. 그러나 이 다수결 결정은 민주적인 것이 아닙니다. 작업증명의 본질과 시스템의 한계는 사용자에게 다수결 결정을 제공하는 것이 아니라 상업적 노드(블록 생성자)에게 다수결을 제공합니다. 이는 IP 주소나 기계당 하나의 투표가 아니라, 투자 단위당 하나의 투표가 거래의 순서를 결정하는 것입니다.

또 하나의 오류는 완전한 자율성을 가정하는 것입니다. 가장 긴 체인은 다수결 결정을 나타내지만, 각 노드가 반드시 이를 따라야 한다는 가정은 노드 운영자가 유효한 거래의 가장 긴 체인을 무엇으로 보는지에 따라 다를 권리를 무시하는 것입니다. 노드가 어떤 체인이 무효하다고 판단할 경우, 노드 운영자는 시스템을 수동으로 재정의하여 대체 체인을 선택할 수 있습니다. 따라서 노드가 자동으로 가장 긴 체인을 따라야 한다는 주장은 유효하지 않습니다. 노드 운영자는 자신이 정직하다고 믿는 체인을 선택해 구축하며, 이는 단기적으로는 이익을 잃을 위험을 감수하지만 장기적으로는 네트워크의 정직성을 보장하여 수익을 증가시킵니다.

즉, 노드는 항상 자신이 정직하다고 간주하고 그 위에 구축할 체인을 의식적으로 결정합니다.

## 상위 수준 아키텍처(High-Level Architecture)



### 노드 상위 수준 시스템 아키텍처

노드는 세 가지 주요 구성 요소를 가집니다:

- **채굴(Mining)** (풀 소프트웨어와 ASIC 채굴기) – 이 구성 요소는 노드에 대한 작업증명을 제공합니다. 이는 독립적으로 실행되며 보상 획득을 위해 채굴자가 채굴해야 하는 임시 블록인 후보 블록 헤더(candidate block header)를 입력으로 받습니다. 이 과정은 다음 섹션에서 자세히 설명됩니다. 풀 소프트웨어는 작업증명으로 알려진 해시 계산 과정을 다수의 계산 장비에 분산시키는 샤딩 메커니즘입니다.
- **노드 소프트웨어(Node software)** – 이 구성 요소는 거래 검증, 블록 준비 및 검증, 블록체인에 추가될 후보 블록을 생성하기 위한 핵심 처리의 대부분을 수행합니다.
- **네트워크(Network)** – 이는 네트워크 내의 모든 노드와 채굴 풀 간 메시지 교환을 가능하게 합니다.

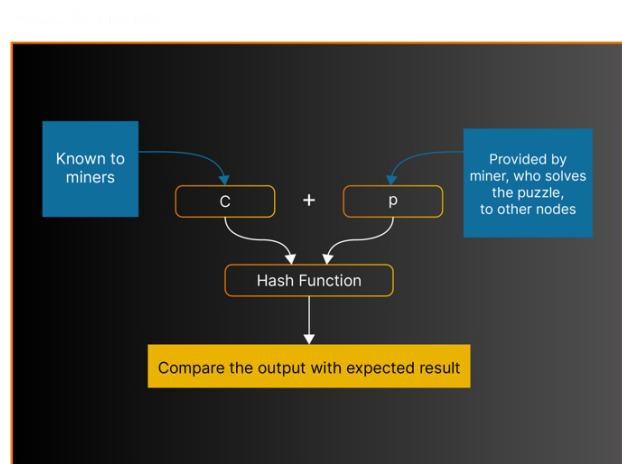
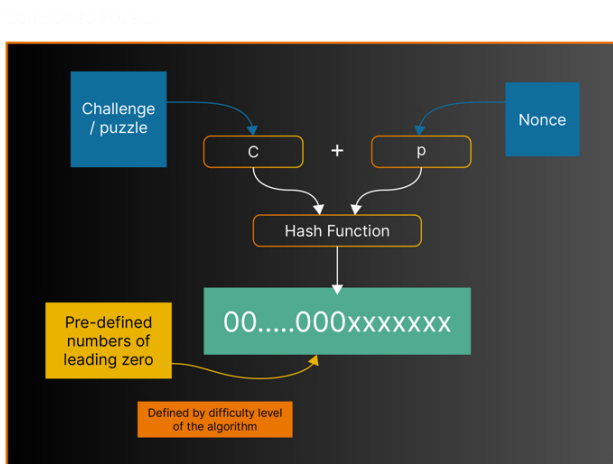
노드 소프트웨어의 세 가지 구성 요소를 분리한 이 관점은 하나의 추상화일 뿐입니다. 다양한 구성으로 노드 소프트웨어를 구축할 수 있으며, 예를 들어 노드 소프트웨어 구성 요소 자체가 여러 하위 구성 요소로 나눌 수 있습니다. 때로는 노드 소프트웨어가 BSN과 노드 소프트웨어를 모두 대표할 수도 있습니다. 위의 구분은 독립적으로 작동하는 다양한 측면을 설명하기 위해서만 제시되었습니다.

## 채굴(Mining)

네트워크의 정책을 이해하기 위해서는 과정에서 채굴 구성 요소를 이해하는 것이 필수적입니다.

- 거래는 사용자로부터 수집되며, 다른 노드에서 누락된 거래도 수집됩니다.
- 이러한 거래는 검증됩니다. 유효한 경우, 입력에 해당하는 UTXO가 업데이트되고 TXID가 저장됩니다. 유효하지 않은 경우, 거래는 거부됩니다.
- 그런 다음 TXID는 블록 후보에 추가됩니다.
- 블록 후보는 블록의 헤더 구성 요소와 후보 머클 루트로 이루어져 있으며, 이는 채굴자에게 전달되어 지정된 목표 값보다 낮은 해시 출력을 찾기 위해 해싱됩니다. 이를 작업증명(Proof-of-Work) 해답이라고 합니다.
- 작업증명 해답이 발견되면, 머클 루트는 다른 정의된 필드와 정의되지 않은 필드들과 결합되어 블록 헤더를 생성합니다. 블록 헤더에는 다음이 포함됩니다:
  - **Version** - 블록이 게시되는 비트코인 프로토콜 버전을 나타내는 4바이트 리틀 엔디언 필드.
  - **hashPrevBlock** - 이전 블록 헤더의 더블 SHA-256 해시(HASH-256)로 채워지는 32바이트 리틀 엔디언 필드.
  - **hashMerkleRoot** - 블록에 타임스탬프가 기록된 모든 정렬된 거래들을 기록하는 머클 트리의 머클 루트를 나타내는 32바이트 리틀 엔디언 필드.
  - **Time** - 블록 내 모든 거래에 적용된 유닉스 에포크 타임스탬프를 포함하는 4바이트 필드. 현재 네트워크 정책은 이 값이 검증 노드의 로컬 타임스탬프 기준 2시간 이내의 정확도를 요구합니다. 타임스탬프는 1초 단위 정밀도를 가집니다.
  - **Bits** - 작업증명 퍼즐의 난이도 목표 값을 포함하는 4바이트 필드로, 네트워크 규칙에 의해 결정됩니다.
  - **Nonce** - "한 번만 사용되는 수(Number Used Once)"입니다. 작업증명 해싱 과정에서 작업증명 해답을 찾기 위해 순환되는 4바이트 필드입니다. nonce 외에도, ASIC 해싱 장치는 전체 43억 값의 nonce 공간을 반복(iterate)할 수 있으므로, 노드들은 블록의 코인베이스 거래 내 데이터 필드의 숫자를 반복하는 방식("익스트라 nonce(extra nonce)"라 불림)과 머클 루트를 재계산하여 추가적인 43억 값의 nonce 공간을 ASIC 해시 장치가 반복할 수 있도록 제공합니다.

Version, hashPrevBlock, hashMerkleRoot, Time, Bits는 nonce(Nonce)의 시작 값과 함께 노드 소프트웨어에 의해 결정됩니다. 이 데이터는 채굴 구성 요소로 전달되며, 채굴 구성 요소는 해답을 찾을 때까지 후보 블록 헤더의 더블 해시 값을 계속 계산하는 브루트포스(brute force)와 유사한 과정을 수행합니다. 이 과정은 아래 다이어그램의 예시 목표 값과 함께 설명됩니다. 그림은 단순화된 표현이며, 실제로 nonce는 후보 블록 또는 도전 과제의 일부입니다. 여기서 도전(Challenge) 또는 퍼즐(Puzzle)은 채굴 해답을 의미합니다.



## 채굴 과정의 상위 수준 흐름

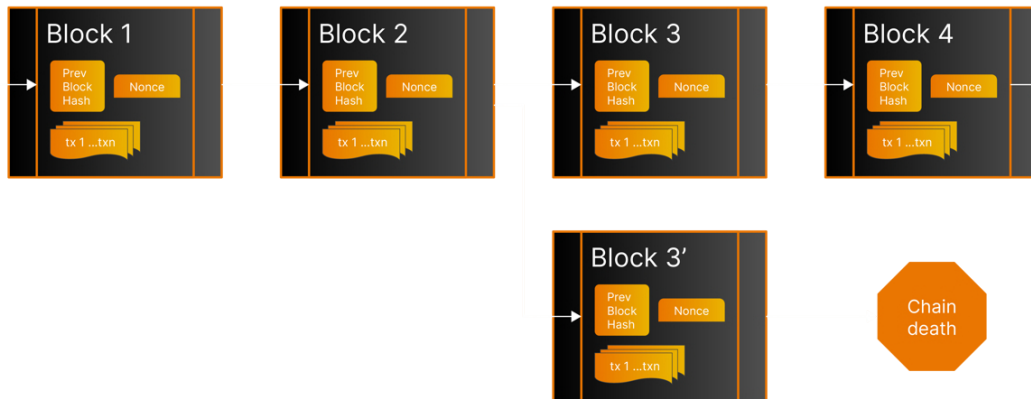
채굴 과정은 작업증명(Proof of Work, PoW)이라고도 불립니다. 채굴 과정의 해답은 노드 소프트웨어로 전달되며, 노드 소프트웨어는 이를 사용해 BSN을 통해 네트워크의 모든 노드에게 제안된 블록에 대한 메시지를 전파합니다. 이후 다른 노드들은 해당 블록의 세부 정보를 요청하며, 이를 수신하면 블록 데이터 및 해당 거래 데이터의 유효성을 검증합니다.

그 다음, 노드들은 해당 블록을 수용할지 여부를 확인하는 메시지를 회신합니다. 이 과정은 나카모토 합의(Nakamoto Consensus)라고 불리며, 어떤 블록이 공통 원장 기록이 될지를 결정합니다. 이는 노드와 원장이 공유하는 역사로 무엇이 기록될지를 결정하는 시스템의 핵심 단계입니다.

합의는 노드들이 제안된 블록을 수용하고, 해당 블록을 이전 블록 ID로 포함하여 다음 블록을 생성함으로써 달성됩니다.

노드들은 해답을 찾기 위해 경쟁하며, 해답을 가장 먼저 찾은 노드만 블록을 게시할 권리를 얻습니다. 다른 노드들의 PoW는 낭비됩니다. 블록이 게시되면 새로운 블록 경쟁이 시작됩니다(즉, 노드들이 새로운 블록 해더를 생성하는 등).

두 개 이상의 노드가 동시에 해답을 찾을 수도 있으며, 이 경우 두 개의 서로 다른 체인 팀이 존재하는 임시 포크가 발생합니다(아래 다이어그램에서 블록 3과 3'로 표시됨).



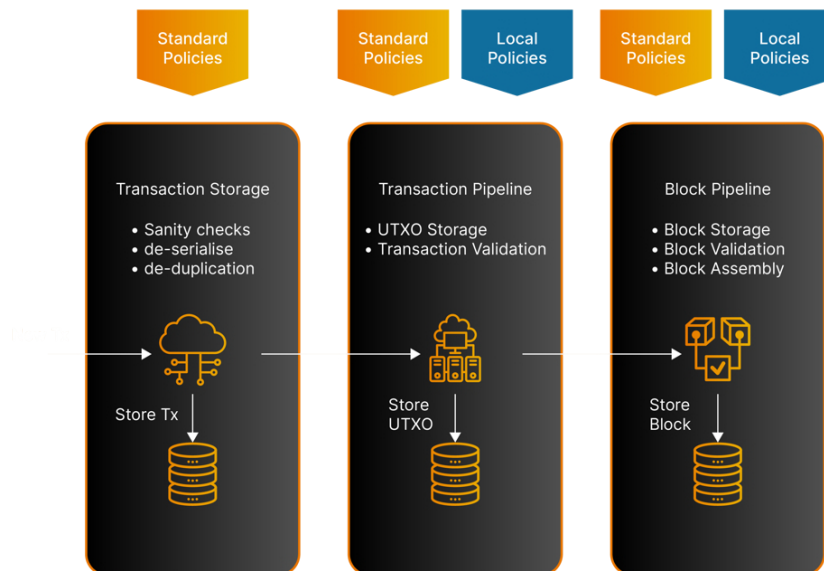
## 경쟁하는 노드들의 작업증명

포크는 이후 블록이 발견되어 제안된 블록 중 하나 위에 구축되면서 해결됩니다(위 다이어그램에서 블록 4). 이 과정에서 앞선 노드는 블록 3을 버리고 블록 4 위에 블록을 쌓게 됩니다.

네트워크 분할이 발생한 후 결코 해결되지 않는 경우, 법률 용어로 이를 분리(demerger)라고 합니다. 이는 실행 중인 블록체인 네트워크가 어느 시점에서 두 갈래로 나뉘었을 때, 원래 프로토콜을 고수하는 쪽은 주체로 남고, 프로토콜을 변경하여 새로운 시스템이 된 쪽은 원래 시스템으로부터 분리된 것으로 간주된다는 의미입니다.

## 표준 정책과 로컬 정책(Standard and Local Policies)

새로운 거래가 노드에 도착하면 일련의 검사와 검증 규칙을 거칩니다. 이는 네트워크 운영을 위해 노드가 반드시 집행해야 하는 합의 규칙입니다. 대부분은 모든 노드에서 표준화되어 있으며 비트코인 프로토콜의 일부입니다(아래 다이어그램에서 표준 정책으로 표시됨). 또한 노드는 자체 인프라와 선호도에 따라 특정한 로컬 정책을 적용할 수도 있습니다.



## 표준 정책과 로컬 정책 - 거래 저장

일반적으로 로컬 정책에 대한 규칙은 거래가 메모리 풀에 수락되거나 블록 후보에 포함되기 전에만 확인됩니다. 반면, 표준 정책 또는 합의 규칙은 항상 확인됩니다.

블록체인으로의 거래는 사용자가 보낸 것일 수도 있고, 또는 노드가 다른 노드가 생성한 블록을 검증하는 과정에서 누락된 거래일 수도 있습니다. 그런 경우, 노드는 해당 블록을 수신한 노드로부터 누락된 거래를 요청합니다. 거래를 수신하면, 이는 마치 새로운 거래인 것처럼 위에 설명된 동일한 검증 과정을 거치게 됩니다.

노드는 처음부터 암호학적 퍼즐을 푸는 것이 아닙니다. 무엇보다 먼저, 노드는 모든 거래를 검증하고 블록을 생성해야 합니다. 퍼즐은 블록 내의 모든 거래, 즉 단 하나의 거래까지도 완전히 검증했을 때만 생성할 수 있습니다. 이를 수행하지 않으면 작업증명 알고리즘을 실행하는 것은 무의미하며, 다른 어떤 노드도 이를 수용하지 않을 것입니다.

## 합의 규칙(Consensus Rules)

네트워크 합의와 그 규칙 집합에는 여러 표준 정책이 설정되어 있습니다. 합의 규칙은 비트코인 노드 클라이언트 소프트웨어 시스템에 코드화되어 있으며, 네트워크 전반에 걸쳐 적용되는 고정적이고 변경 불가능한 규칙을 나타냅니다. 이러한 규칙은 노드가 네트워크 거버넌스 과정에 적극적으로 참여하기 위해 반드시 엄격히 준수해야 합니다.

## 제네시스 블록 규칙(Genesis Block Rule)

블록체인은 2009년 1월 9일에 생성된 최초의 블록에 고정(anchor)되어 있습니다. 이는 블록체인의 시작을 의미하며, 그래서 이름도 "제네시스(Genesis)"입니다.

제네시스 블록은 특별한데, 이는 채굴을 통해서가 아니라 하드코딩된 값으로 생성되었기 때문입니다. 이 블록에는 최초의 50코인 보상이 포함되어 있었습니다. 이 코인들은 사용 불가능하도록 설계되었으며, 이것이 이 블록이 블록체인의 기준(anchor) 역할을 하는 이유입니다.

제네시스 코인베이스 거래의 50코인은 개인키 없이 생성된 공개키로 전송되었으며(ECC, 즉 타원곡선 암호학은 이를 가능하게 함), 이로 인해 해당 공개키는 유효하지 않게 되고 이 코인들은 소비할 수 없게 되었습니다.

타원곡선에서 직접적으로 개인키로부터 도출하지 않고도 점을 생성하는 것이 가능합니다. 이러한 점들은 수학적으로 생성되거나 곡선 상의 미리 정의된 점들에서 선택될 수 있습니다. 그러나 이러한 점들은 암호학적 의미에서 개인키와 연결되지 않기 때문에 서명이나 암호화/복호화 같은 일반적인 암호학적 작업에는 사용할 수 없습니다.

### 타원곡선 상에서 점 생성하기

타원곡선 상에서 점을 생성하려면,  $x$ 좌표를 선택한 다음 타원곡선 방정식을 사용해 대응하는  $y$ 좌표를 계산할 수 있습니다. 곡선이 다음과 같이 정의될 때:

$$y^2 = x^3 + ax + b$$

하나의  $x$ 좌표를 선택하고  $y$ 를 계산할 수 있습니다. 이 접근 방식은 다음 단계를 포함합니다:

- $x$ 좌표를 선택한다.
- $y^2 = x^3 + ax + b$  를 계산한다.
- $y$ 를 계산한다(우변이 해당 체(field)에서 이차 잉여(quadratic residue)일 경우).

### 설명

1. 곡선 매개변수 선택: secp256k1 곡선을 선택한다.
2. 무작위  $x$ 좌표 선택: 무작위로  $x$ 좌표를 선택한다.
3.  $y^2$  계산: 타원곡선 방정식의 우변을 계산한다.
4.  $y$  계산: 우변이 소수체에서 이차 잉여인지 확인한다. 만약 그렇다면 제곱근을 계산해  $y$ 를 찾는다.

### 참고

- **이차 잉여(Quadratic Residue):** 유효한  $y$ 가 존재하려면  $x^3 + ax + b$  값이 해당 체에서 이차 잉여여야 한다.
- **보안 고려사항(Security Considerations):** 생성된 점은 곡선 위에서 수학적으로는 유효하지만 개인키와 연결되어 있지 않습니다. 따라서 개인-공개키 쌍이 필요한 작업에는 사용할 수 없습니다.

제네시스 블록 규칙은 악의적인 당사자가 새로운 체인을 생성하여 해시 파워나 경제 활동을 악의적으로 전환하는 것을 방지합니다. 이는 단순화된 결제 검증(Simplified Payment Verification)의 핵심 요소로, 사용자가 최소한의 오버헤드로 올바른 블록 체인을 사용하고 있음을 확인할 수 있도록 합니다.

제네시스 블록은 다음의 블록 해시로 식별됩니다 -

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

네트워크 사용자 모두가 이 블록 해시를 알고 있도록 보장함으로써, 어떤 블록 체인이 유효한지에 대한 확실성을 가질 수 있습니다. 만약 사용자나 노드가 제네시스 블록이 아닌 다른 기원점으로 이어지는 블록 체인에 연결된다면, 즉시 잘못된 네트워크에 연결되었음을 알 수 있습니다.

## 블록 크기 규칙(Block Size Rule)

블록의 크기는 블록 헤더와 그 안의 모든 거래를 포함한 블록의 직렬화(serialised)된 형태의 바이트 단위 크기입니다.

프로토콜은 블록의 크기를 마지막 블록이 채굴된 이후 노드가 본 거래의 수에 따라 정의합니다. 프로토콜에는 최대 크기가 정의되어 있지 않습니다. 이는 노드 소프트웨어의 호스팅 능력에 달려 있습니다. 네트워크가 시간이 지남에 따라 성장함에 따라 평균 블록 크기는 제한 없이 증가할 것으로 예상됩니다.

## 가장 긴 체인 규칙(Longest Chain Rule)

mining에서 설명했듯이, 노드는 항상 가장 긴 정직한 체인을 추적하면서 그 체인 위에 블록을 쌓아야 합니다. 이것이 채굴 노드가 소프트웨어를 구성하는 최소한이자 최적의 방법입니다. 채굴 노드가 의도적으로 가장 긴 정직한 체인이 아닌 다른 체인 위에 블록을 구축한다면, 이는 악의적인 것으로 간주되며 프로토콜 위반입니다.

## 블록 보조금 규칙(Block Subsidy Rule)

새로운 블록을 생성할 때 채굴 노드는 블록 보조금으로 보상을 받습니다. 이 보조금은 네트워크에 새로운 코인을 분배하는 기능도 수행합니다. 채굴 노드가 이 활동을 통해 받는 보상은 재정적 수익으로 간주되며, 현지 소득 및 세금 규정을 따릅니다. 채굴 노드가 수행하는 서비스 또한 그들의 현지 관할권 내에서 다른 모든 비즈니스가 적용받는 규제에 구속됩니다.

## 난이도 조정(Difficulty Adjustment)

난이도 조정의 목적은 네트워크 운영의 안정성을 유지하고 블록 생성 속도를 가능한 한 10분에 가깝게 유지하는 것입니다.

이를 위해 새로운 블록이 발견되는 빈도를 검증하여 난이도 수준을 조정해야 합니다. 이 조정은 블록 헤더의 'bits' 값을 사용하여 채굴 과정에서 적용되며, 이는 목표 값 계산(블록 해시 값의 앞부분에 오는 0의 개수로 정의됨)에 영향을 미칩니다. 이는 노드 소프트웨어에 구현되어 있으며 특정 노드에서 수동으로 설정할 수는 없습니다.

비트코인 블록체인 네트워크가 출시된 후 첫 284일 동안 하루에 144개의 블록이 생성되어 총 41,000개의 블록이 채굴되었어야 했습니다. 이는 200만 비트코인에 해당합니다. 그러나 실제로는 그 시점에서 125만 개만 채굴되었습니다.

## 네트워크 합의(Network consensus, 나카모토 합의라고도 함)

작업증명(Proof of Work) 정족수(quorum) 시스템은 합의 방법론 자체에 아무런 고유 가치가 없도록 네트워크 합의를 형성하는 방식에 기반합니다. 이는 평판이나 선택 방법론에 의한 전통적 투표 시스템의 대안입니다.

블록체인에서 합의를 투표로 달성하는 대신, 노드들은 블록 위에 새로운 블록을 쌓음으로써 해당 블록을 수용했음을 보여줍니다. 프로토콜에서는 이를 "노드에 의한 투표"라고 정의합니다. 노드들은 거래를 처리하는 과정에서 블록을 생성하고, 이미 브로드캐스트된 거래가 포함된 이전 블록 위에 새로운 블록을 구축함으로써 "투표"합니다.

블록을 생성한 노드의 수는 공개적으로 확인할 수 있습니다. 최대 2016개의 노드가 운영될 수 있는데(2주간 난이도 조정 기간 동안 1시간에 6블록), 이는 난이도 조정 주기가 이 숫자만 허용하기 때문입니다. 난이도 조정이 발생하면 새로운 2016개의 노드 세트가 블록을 채굴하는 주기로 카운트가 초기화됩니다. 일반적으로 대부분의 블록은 소수의 노드, 보통 5~10개 정도의 노드가 생성합니다. 따라서 어느 시점에서든 네트워크 투표는 최대 2016개의 노드에 고정됩니다. 네트워크에 다른 노드가 존재할 수 있지만, 블록을 생성하지 못하면 네트워크 합의와 투표 메커니즘에 포함되지 않습니다. 이들은 단순히 리스너 클라이언트일 뿐, 노드 네트워크의 일부가 아닙니다.

또 다른 측면으로 살펴볼 것은 코인베이스 출력에 대한 100 블록 규칙입니다. 100 블록은 노드가 코인베이스 거래를 사용하기 전에 기다려야 하는 최소 블록 수입니다. 따라서 노드가 유효한 블록을 찾은 후에는 100 블록 동안 네트워크를 보호할 경제적 인센티브를 갖게 됩니다. 이는 동시에 운영될 수 있는 노드의 창(window)이 100개임을 의미합니다. 어느 시점에서든 최대 100개의 노드가 네트워크를 유지하고 보호할 경제적 인센티브를 갖게 됩니다.

PoW 과정에서는 네트워크 내 참여 노드가 2주마다(난이도 조정과 함께) 교체됩니다. 새로운 주기에서 블록을 구축하는 모든 노드는 해당 난이도 기간 동안 노드로 간주됩니다. 이 메커니즘은 네트워크에서 개방적이고 허가 없는 기반의 운영을 가능하게 합니다.

브루트포스와 유사한 과정을 사용함으로써 PoW 채굴 과정에서 불공정한 이점이 발생하지 않도록 보장합니다. 이 핵심 혁신은 네트워크 내 노드가 신뢰 불필요(trustless)하고 허가 없는(permissionless) 방식으로 참여할 수 있게 하여, 신뢰할 수 없는 중개자로 기능하도록 만듭니다. 다른 방법들이 사용된다면, 이는 중개자에게 신뢰 요소를 부여하게 되고, 시스템이 취약해지며 악용의 표적이 될 수 있습니다. 네트워크에서 신뢰할 수 없는 거래 실행이라는 특성이 블록체인을 혁신적으로 만드는 본질입니다.

## 최초 수신 규칙(First Seen rule)

거래를 수신할 때, 이중지불(double-spend)이 발생한 경우 어느 거래가 유효한지를 결정하기 위해 최초 수신 규칙이 적용됩니다. 노드가 이중지불을 감지하면, 가장 먼저 수신한 거래를 해당 코인의 유효한 사용으로 간주합니다.

이 규칙은 더 확장되어, 이중지불 거래를 포함하는 블록이 발견될 경우 해당 블록 또한 무효로 간주되며, 노드는 해당 블록에 대해 채굴을 계속하지 않아야 합니다. 다만, 그 블록 위에 두 번째 블록이 발견되어 네트워크의 대다수가 다른 거래를 최초 수신 거래로 결정했음을 나타내는 경우는 예외입니다.

## 거래 합의 규칙(Transaction Consensus Rules)

프로토콜은 거래 검증 및 확인 규칙 집합으로 구성되며, 노드는 이 규칙을 사용하여 사용자나 다른 노드로부터 수신한 거래를 해석합니다. 다음과 같은 검증이 수행됩니다:

- **거래 크기(Transaction Size):** 노드들이 합의하여 항상 지원하기로 한 최대 크기가 있습니다. 현재는 10MB입니다.
- **nLockTime과 nSequence:** 이 필드들은 미래에 유효해질 거래를 생성하는 데 사용됩니다. 세부 사항은 거래 라이프사이클과 결제 채널(link)에서 다뤄집니다. 오직 최종 거래만 블록에 확인되며, 그 전까지는 노드의 메모리 풀에 저장됩니다.
- **가치 교환(Value Exchanges):** 입력(소비되는 값)은 모든 출력과 수수료를 총당해야 합니다.
- **코인베이스 거래(Coinbase Transaction):** 노드는 코인베이스 거래가 발생한 블록보다 100 블록 미만의 높이에서 해당 코인베이스 거래의 출력을 소비할 수 없습니다.
- **거래 형식 규칙(Transaction Format Rule):** 거래는 비트코인 프로토콜의 데이터 형식 규칙을 준수해야 합니다.
- **비트코인 스크립트 언어와 그 명세(Bitcoin scripting language and its specification):** 거래의 입력과 출력을 생성하는 데 사용되는 스크립트 언어와 관련된 일련의 규칙이 존재합니다.

## 로컬 정책(Local Policies)

채굴 노드가 시스템을 설정할 때, 자신의 인프라에 따라 소프트웨어를 구성하게 됩니다. 이러한 구성은 로컬 정책에 해당합니다. 일부 정책은 표준 정책에 속하는 프로토콜 수준 규칙 집행 의무를 넘어, 노드가 제공하고 자 하는 서비스에 대한 선호도에 기반하기도 합니다.

이러한 정책은 일반적으로 노드 인프라 및 노드 설정 시의 구성과 관련됩니다.

특정 규칙은 다음과 관련됩니다:

- 노드가 지원할 수 있는 블록 및 거래 크기
- 거래 수수료
- 노드가 비트코인 서버 네트워크를 통해 다른 참여 노드로부터 수신한 거래와 블록을 검증하는 방식

### 합의 규칙 및 로컬 정책 전체 목록

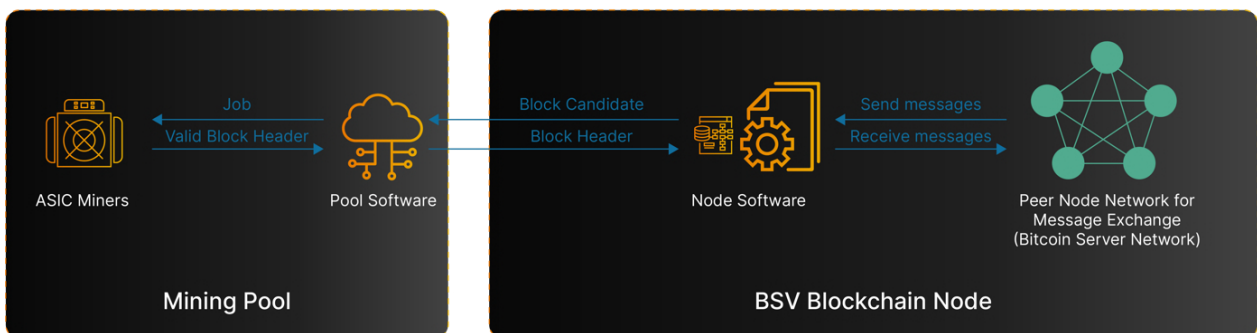
노드가 반드시 집행해야 하는 모든 합의 규칙은, 코인의 발행자로부터 블록 보조금을 수령할 때 법적으로 계약에 의해 구속되는 사항입니다. 블록체인 시스템이 법적 프레임워크를 통합하는 방식이 바로 이것입니다.

로컬 정책은 노드 인프라에 특화된 구성 항목이며, 각 노드마다 다를 수 있습니다. 이러한 정책은 다양한 노드들이 신뢰성 있고 고처리량의 거래 처리, 대규모 거래 지원 등 자신들의 서비스 측면에서 서로 경쟁할 수 있도록 합니다.

## 노드 운영(Node Operations)

앞서 우리는 채굴 과정과 그 과정에서의 노드 참여에 대해 이야기했습니다. 이 섹션에서는 프로토콜에 의해 정의된 블록체인 거버넌스 규칙 집합에 따라 블록체인이 운영되도록 하기 위해 네트워크 정책을 구현하고 노드 간 통신에 참여하는 노드 소프트웨어의 기술적 사양에 초점을 맞춥니다.

노드의 두 가지 주요 구성 요소는 채굴 풀과 기능적 작업을 수행하는 노드 소프트웨어입니다. 이는 아래 다이어그램에 설명되어 있습니다.

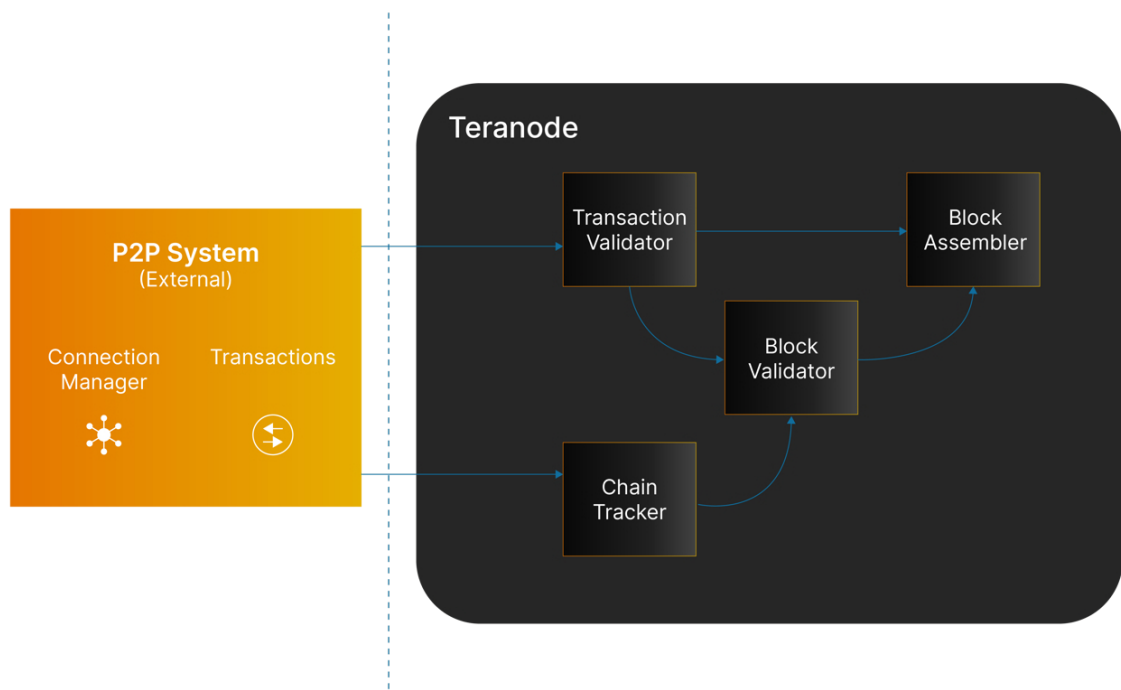


노드 소프트웨어는 일반적으로 **Bitcoin** 또는 단순히 **BSV 노드 소프트웨어**라고 불리며, 원래 모놀리식 (monolith)으로 구현된 비트코인 프로토콜을 기반으로 합니다. 현재는 거래 처리의 훨씬 더 큰 네트워크 처리량을 지원하기 위해 개선된 확장 가능한 마이크로서비스 기반 비트코인 프로토콜 구현을 위한 작업이 진행 중입니다. 이 업그레이드는 테라바이트 크기의 블록과 초당 백만 건 이상의 거래 처리량(TPS)을 지원하는 것을 목표로 합니다. 이렇게 확장된 블록체인 네트워크는 전 세계의 유틸리티 및 상업적 활용을 위해 다양한 유형의 거래와 애플리케이션 사용 사례를 지원하는 것을 목표로 합니다.

현재 BSV 협회가 오픈소스로 공개한 노드 소프트웨어 버전은 하나뿐이지만, 이것이 다른 경쟁 솔루션이 존재할 수 없음을 의미하지는 않습니다. 다른 엔터티가 원한다면 소프트웨어를 처음부터 자체적으로 구축하거나, 참조 구현(reference implementation)을 가져와 개선하거나, BSV 협회가 배포한 소프트웨어를 그대로 사용할 수 있습니다.

## 노드 소프트웨어(Node Software)

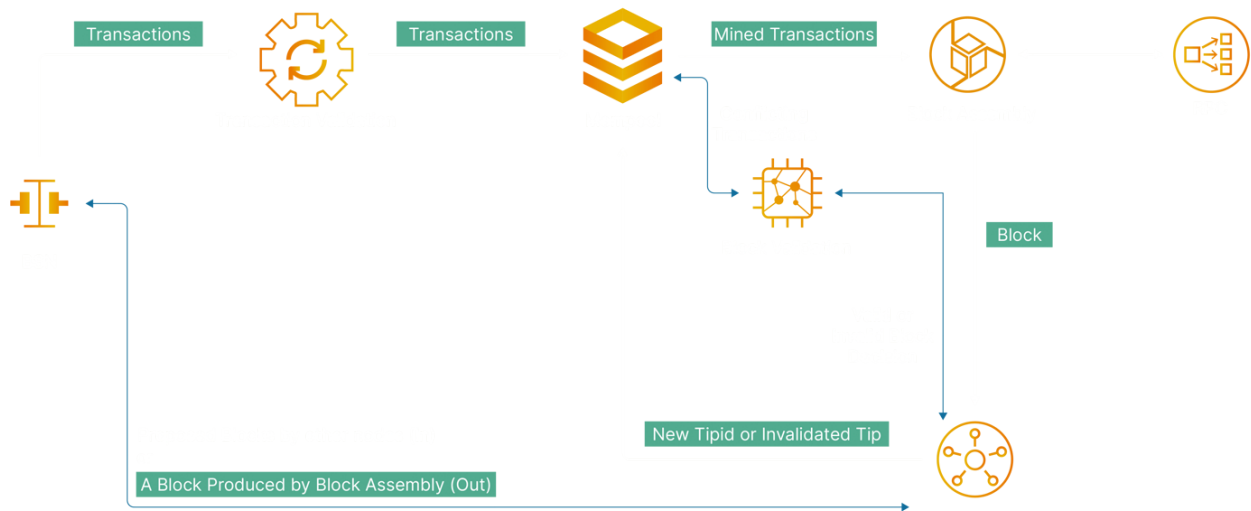
상위 수준에서 노드 소프트웨어는 아래 다이어그램에 나타난 다양한 기능 블록으로 구성됩니다. 다이어그램에는 노드 소프트웨어 설명을 위해 채굴 구성 요소는 포함되어 있지 않습니다.



P2P 시스템(또는 BSN, Bitcoin Server's Network라고도 함)은 네트워크 내 다양한 노드 간의 네트워크 연결과 메시지 교환을 처리하는 하위 시스템을 나타냅니다. P2P라는 용어는 피어 투 피어(Peer to Peer)를 의미하며, 이는 블록체인 네트워크 운영에 참여하는 노드들이 모두 피어라는 것을 뜻합니다. 즉, 각 피어 노드는 네트워크 내에서 다른 피어와 동일한 기능을 수행합니다. 네트워크 사용자에게 추가적인 서비스를 제공할 수는 있지만, 네트워크 관점에서는 다른 어떤 노드와도 완전히 동일한 책임과 기능을 가집니다.

그 외 하위 시스템인 거래 검증기(Transaction Validator), 블록 조립기(Block Assembler), 블록 검증기(Block Validator), 체인 추적기(Chain Tracker)는 각각 필요한 기능을 수행하기 위해 하나 이상의 서비스와 구성 요소로 이루어져 있습니다. 일반적으로 P2P 시스템은 사용자나 네트워크 내 다른 노드로부터 거래를 수신하며, 이는 거래 검증 프로세스로 라우팅되어 검증됩니다. 거래가 검증되면, 해당 거래는 그 노드의 블록 조립기에 의해 구축 중인 제안 블록의 일부가 됩니다. 다른 흐름은 또 다른 노드가 블록을 발견한 경우인데, 이때 체인 추적기는 모든 노드로부터 오는 메시지를 수신하여 이를 추적합니다. 특정 노드가 블록을 발견했다고 알리면, 체인 추적기는 해당 노드로부터 공지된 블록을 다운로드합니다. 다운로드가 완료되면, 블록 검증기에 블록을 전달하여 그 안에 포함된 모든 거래 검증을 포함한 블록 검증이 이루어집니다.

아래는 노드 소프트웨어 운영 중 이러한 기능 블록들이 서로 상호작용하는 상세 뷰입니다.



다이어그램은 두 가지 주요 흐름을 보여줍니다. 첫 번째는 새로운 거래를 수신하고 검증 과정을 거쳐 블록 조립(Block Assembly)에서 새로운 제안 블록에 추가되는 흐름입니다. 이 제안 블록은 이후 채굴 소프트웨어의 입력으로 전달되어 블록 해시 계산을 통해 작업증명(PoW) 해답을 찾습니다. 해답이 발견되면, 제안 블록은 BSN을 통해 네트워크에 전파됩니다. 이 흐름은 녹색으로 강조되어 있습니다. 두 번째 흐름은 다른 노드가 해답을 찾았을 때 발생하며, 이 노드는 새로운 제안 블록을 수신한 후 블록 검증기에 의해 검증합니다. 이 블록에 의해 확인된 거래는 메모리 풀에서 제거되며, 새로운 검증된 거래로 체인 팁(chain-tip) 위에 새로운 채굴 후보 블록이 구축됩니다.

ChainTracker는 항상 체인의 최신 팁 ID를 다양한 구성 요소에 식별하고 내부 업데이트하는 책임을 집니다. 또한 검증 과정에서 실패한 블록과 관련된 통신을 처리합니다.

일반적으로 노드 소프트웨어에서는 한 시점에 세 가지 주요 흐름이 동시에 발생합니다.

1. 노드는 거래를 수신하고 이를 검증합니다. 거래가 검증되면, 해당 거래는 BSN을 통해 노드 네트워크에 브로드캐스트되어 모든 노드가 유효한 거래를 알 수 있게 됩니다.
2. 블록 조립기는 후보 블록 헤더를 기반으로 채굴 해답을 계산하기 위해 채굴 풀 소프트웨어에 전송할 제안 후보 블록을 구축합니다.
3. ChainTracker는 가장 긴 체인 팁을 모니터링하며, 새로운 블록 팁이 발견되면 해당 블록을 다운로드하고 블록 검증기로 전송하여 검증합니다.

이 세 가지 주요 흐름 외에도 병렬로 발생하는 하위 흐름(sub-flows)이 존재합니다.

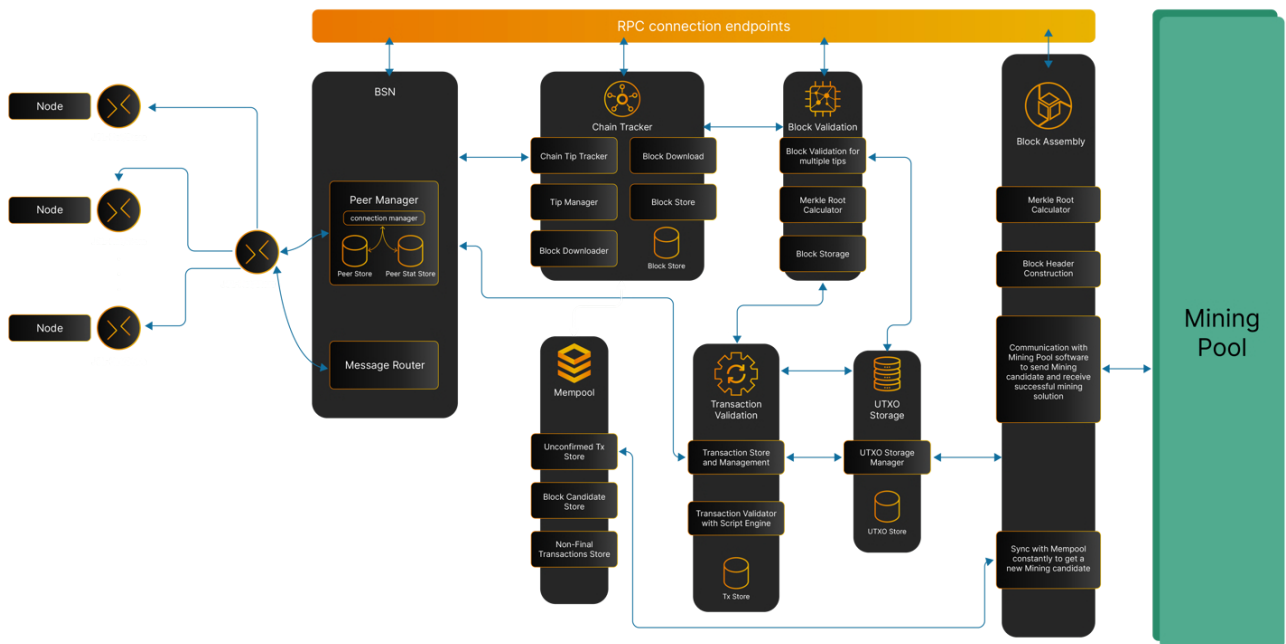
1. BSN은 네트워크에 참여하는 노드들의 통신을 지속적으로 모니터링하며, 앞서 언급된 흐름에서 발생하는 수신 및 발신 메시지를 라우팅합니다. 여기에는 참여 노드들이 브로드캐스트하는 새로운 거래의 수신도 포함됩니다.
2. 채굴 풀 소프트웨어는 네트워크에서 확인된 가능한 최신 거래들을 모두 포함한 후보 블록으로 채굴할 수 있도록 업데이트된 블록 템플릿을 지속적으로 조회합니다. 블록 조립기는 주기적으로 새로운 거래를 후보 블록에 추가하며, 이로 인해 머클 루트가 갱신됩니다.
3. UTXO 저장소는 위에서 언급된 흐름을 기반으로 주어진 UTXO의 상태를 계속 업데이트합니다. UTXO의 최종 상태는 "소비됨(spent)"이며, 이는 블록 조립기에 의해 후보 블록에 포함되거나 블록 검증기에 의해 블록 내에 포함된 것이 확인될 때 결정됩니다.

- 메모리 풀(Mempool)은 성공적으로 검증된 새로운 거래를 지속적으로 수신합니다. 이는 주기적으로 후보 블록을 갱신하며, 이후 블록 조립기와 채굴 풀에 의해 사용됩니다.
- 다른 노드가 제안한 블록을 검증할 때, 노드는 해당 거래의 약 97%를 이미 알고 있지만, 남은 소량의 보지 못한 거래들은 요청되어 노드가 가져오게 됩니다.

참고로, 여기서는 노드 소프트웨어 내부 동작에 대해 상위 수준에서만 다루고 있습니다. 전체 코드베이스는 <https://github.com/bitcoin-sv/bitcoin-sv>에서 확인할 수 있으며, 그곳에서 기능에 대한 심층적인 분석을 찾을 수 있습니다.

## 소프트웨어 구성 요소(Software Components)

노드 소프트웨어의 보다 상세한 개요는 아래 다이어그램에 나타나 있습니다.



이 다이어그램을 기반으로 각 기능 블록을 개별적으로 살펴보면, 다이어그램에 표시된 각 상자에 대해 더 깊이 이해해 보겠습니다.

노드 소프트웨어 및 그 하위 구성 요소에 대한 설명은 코드베이스 수준의 세부 사항으로 들어가지 않고 대략적인 통찰을 제공합니다. 이는 가독성을 유지하면서 소프트웨어에 대한 심층적인 이해를 제공하기 위함이며, 운영 매뉴얼로 사용되기 위한 것이 아닙니다.

## 비트코인 서버 네트워크(Bitcoin Server Network, BSN)

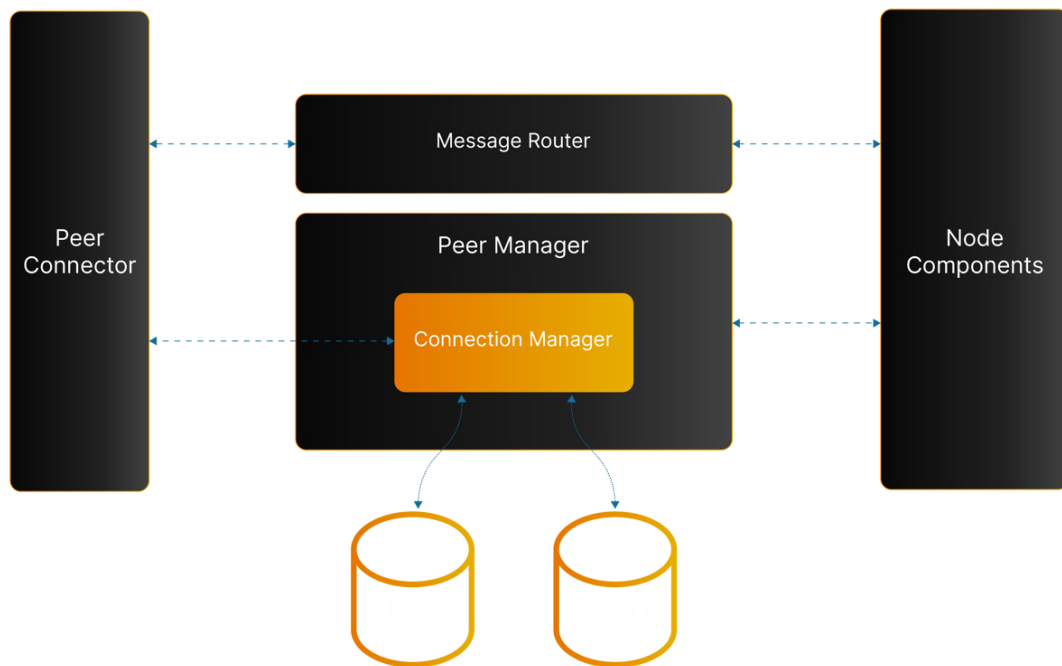
BSN 또는 Bitcoin Server Network는 이전에 P2P 네트워크로 불렸던 구성 요소의 새로운 이름입니다. P2P 네트워크라는 이름은 노드들이 서로의 피어(peer)라는 사실에서 유래했습니다.

■

비트코인 서버 네트워크는 노드 소프트웨어 내 하위 시스템의 이름으로, 외부를 바라보며 노드 소프트웨어의 모든 메시지 교환과 통신을 담당합니다. 여기서 "서버"라는 단어는 블록체인을 사용하는 모든 애플리케이션의 서버 역할을 하는 노드와, 전통적인 클라이언트-서버 아키텍처에서의 클라이언트와의 유사성을 의미합니다. BSN 하위 시스템의 주요 목적은 피어 노드들을 연결하고 관리하는 것입니다:

- 특정 노드의 네트워킹과 통신을 관리하며, 노드와 그 피어들의 "아이덴티티" 역할을 합니다. 또한 연결을 요청하는 모든 다른 노드와의 연결을 관리합니다.
- 네트워크 메시지를 검색하고 배포합니다:
  - 새로운 블록
  - 새로운 거래
  - 체인 상태
  - 요청 시 블록 헤더
  - 요청 시 블록

상위 수준 구성 다이어그램은 아래와 같습니다.



## 피어 커넥터(Peer Connector)

이 구성 요소는 JCL 라이브러리 및 운영 모음(JCL suite of libraries and operations)으로 제공되는 두 개의 하위 모듈과, 다른 노드의 JCL-Net이 노출하는 메시지 이벤트를 구독하는 메시지 라우터(Message Router)로 구성됩니다. 수신된 메시지는 메시지 라우터를 통해 시스템에 주입됩니다. 제한된 수의 피어가 단일 JCL에 연결되며, 해당 JCL은 자체 메시지 라우터와 연결됩니다.

**JCL-Net 모듈**은 블록체인 네트워크에 연결하고, 수신하며, 반응할 수 있는 기능을 제공합니다. 연결 기능에는 핸드셰이크 프로토콜, 타임아웃(Ping/Pong) 설정, 노드 발견 알고리즘(Node-Discovery algorithm), 블랙리스트 등이 포함됩니다. 또한 네트워크 애플리케이션을 지원하여 요청(예: 거래나 블록 요청)을 처리할 수 있도록 이벤트 스트림 및 알림 기능을 제공합니다.

**JCL-Store**는 다른 노드와의 지속적인 통신 과정에서 수신되거나 전송되는 블록 및 거래를 저장하거나 검색하는 작업을 제공합니다.

## 피어 매니저(Peer Manager)

피어 매니저 구성 요소는 JCL을 통해 네트워크의 다른 노드들과의 연결을 조직하고 유지합니다. 또한 피어에 대한 정보를 추적하고, P2P 통신을 지시하며, 피어 정보와 통계를 관리합니다. 이러한 데이터는 피어 저장소(Peer-Store)와 피어 통계 저장소(Peer-Statistics Store)에 보존됩니다.

**Peer-Store**는 연결된 모든 피어에 대한 주요 식별 정보(IP 주소, 포트, 스트림 상태 등)와 피어의 상태(죽음, 활성, 차단, 페널티, 알 수 없음 등)를 저장합니다.

**Peer-Statistics Store**는 Peer-Store에 저장된 특정 피어와 교환된 모든 메시지의 통계 정보를 기록합니다. 또한 피어와의 통신 성능에 대한 특정 데이터를 수집하며, 이는 알고리즘에 의해 피어의 점수를 산출하는 데 사용됩니다. 이 점수는 피어가 활성 상태로 유지될 수 있는지, 아니면 차단되어야 하는지를 결정하는 데 활용됩니다.

블록 헤더 클라이언트(Block Header Clients, BHC)는 블록체인 네트워크와 연결하기 위해 BSN에 접속합니다. 단, BHC는 블록 헤더만 저장하며 블록과 거래 데이터는 저장하지 않습니다.

## 체인 추적기(ChainTracker)

체인 추적기(ChainTracker)는 이름 그대로 블록체인 네트워크에서 가장 긴 블록 체인을 추적합니다. 또한 다른 노드로부터 새로운 블록 발견과 관련된 메시지를 BSN을 통해 수신했을 때 이에 응답하는 역할을 합니다. 이와 더불어 항상 노드가 외부 노드 네트워크와 동기화 상태를 유지하도록 노드 상태를 보장하는 책임을 가집니다.

노드가 동기화되지 않았고 네트워크로부터 블록을 다운로드해야 하는 경우, 체인 추적기는 블록 다운로드 및 저장 서비스와 협력하여 이를 조정합니다. 다운로드가 완료되면 해당 블록을 블록 검증기(Block Validator)에 전달합니다.

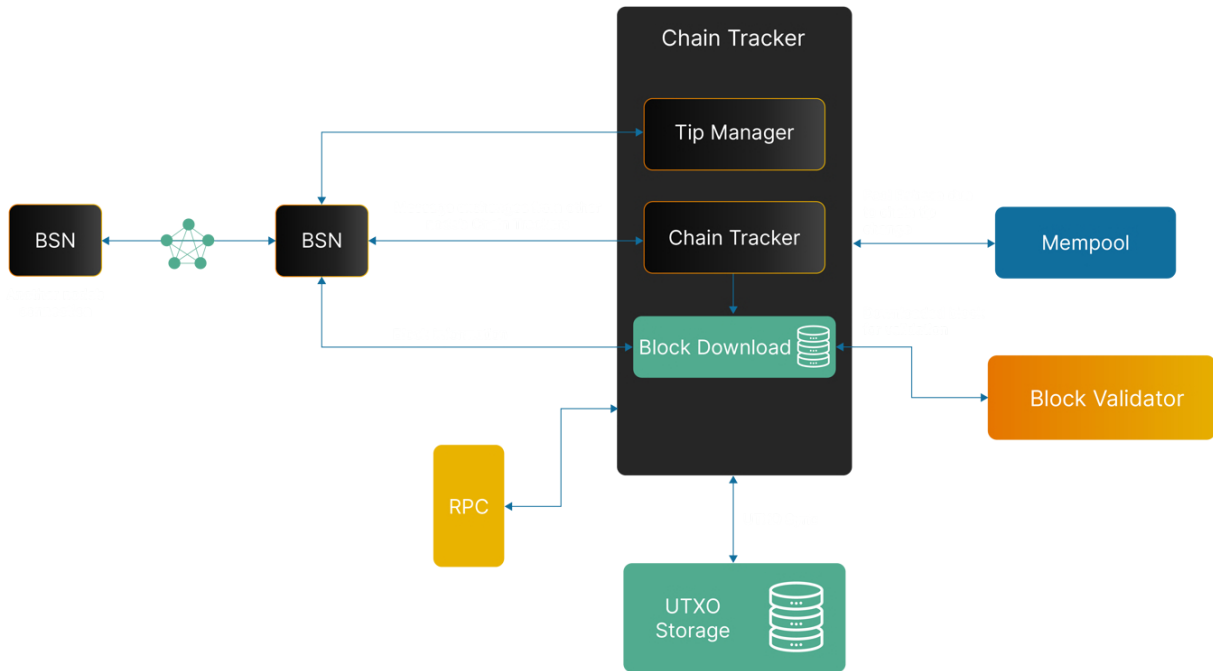
체인 추적기는 체인을 구성하는 모든 블록 헤더를 저장합니다. 각 블록 헤더에 대해 체인 추적기는 “메타데이터(Metadata)”도 저장하는데, 이는 해당 블록과 관련된 플래그나 정보를 저장하는 지표표시자 역할을 합니다. 예시는 다음과 같습니다:

- 거래 수(Number of TX's)
- 다운로드 타임스탬프
- 다운로드 출처

- 검증 타임스탬프
- 검증 횟수(예: 블록이 손상되어 다시 다운로드 및 검증이 필요할 때 여러 번 검증되는 경우)

체인 추적기는 네트워크 내 다른 피어들에게 질의하여 체인에 포함된 블록들의 헤더를 가져오고, 이를 통해 제네시스(Genesis) 블록부터 체인 팁(Tip)까지 내부적으로 체인을 구축합니다. 또한 검증 중인 블록들을 추적하고, 노드의 다른 구성 요소들이 해당 블록들을 인지하고 블록이 유효(Validated) 또는 무효(Invalidated) 상태일 때 알림을 받을 수 있도록 보장합니다.

아래 다이어그램은 체인 추적기에 대한 개요를 보여줍니다:



체인 추적기는 Tip Manager와 상호작용하는 중심 구성 요소로, Tip Manager는 BSN을 통해 다른 노드의 체인 추적기에서 들어오는 통신을 모니터링하여 TipId를 수신합니다.

체인 추적기는 또한 메모리 풀(Mempool)과 통신하여 활성 TipId와 동기화하며, 메모리 풀이 인식하는 유효한 TipId를 갱신해야 할 때 메모리 풀에 메시지를 보내 TipId 재정렬을 수행합니다. 이 과정은 풀 리베이스(pool rebase)라고 불립니다. 또한 체인 추적기는 UTXO 저장 서비스와 상호작용하여, 이들이 인식하는 Tip이 네트워크에서 인식하는 가장 긴 Tip과 동기화되도록 보장합니다. 이를 통해 블록체인에서 가장 긴 작업 체인을 기준으로 UTXO와 그 상태가 올바르게 반영되도록 합니다.

노드의 가장 중요한 기능 중 하나는 항상 가장 긴 블록 체인을 인식하도록 보장하는 것입니다. 이 기능은 체인 추적기에 의해 수행됩니다. 또한 체인 추적기는 잠재적으로 가장 긴 체인이 될 수 있는 다양한 체인 팁을 로그로 유지합니다. 이는 네트워크에서 시간이 지남에 따라 나타났다 사라지는 임시 포크들을 항상 추적하고 있음을 의미합니다.

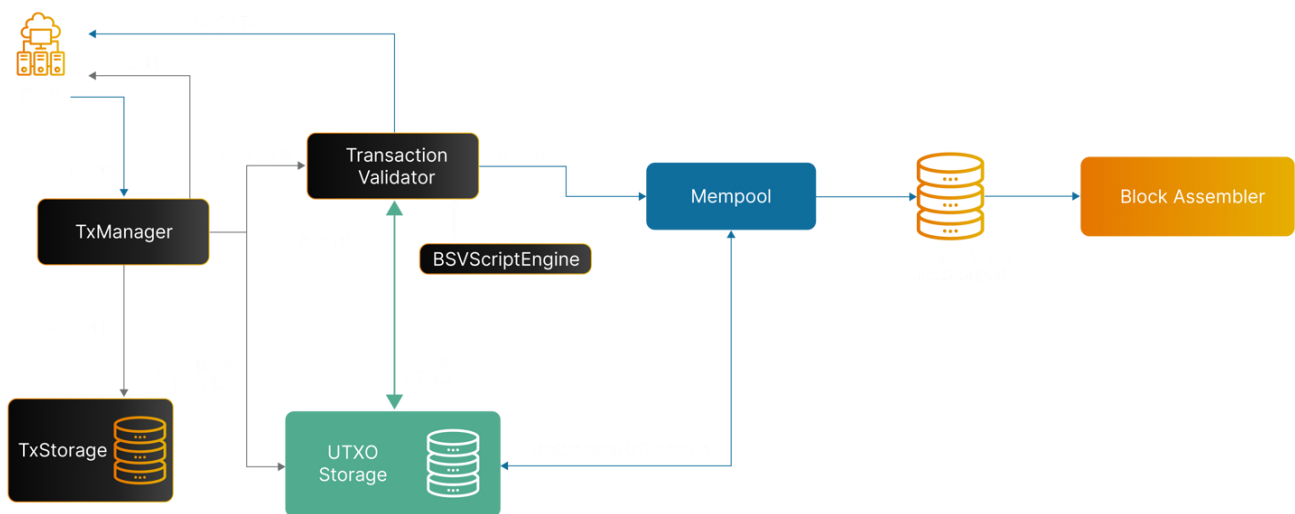
## 거래 검증(Transaction Validation)

거래 검증 과정은 많은 하위 구성 요소들로 이루어져 있습니다. 이 구성 요소들은 함께 거래 검증에 필요한 단계를 실행하도록 조정합니다. 블록 검증을 위한 거래 검증 또한 동일한 기준을 따릅니다.

거래 검증의 일환으로 수행되는 검증 확인의 논리적 요약은 다음과 같습니다:

- 거래의 구문과 데이터 구조가 올바른지 확인한다.
- 입력(Input)과 출력(Output) 목록이 비어 있지 않아야 한다.
- 거래 크기(바이트 단위)가 최대 블록 크기 값보다 작아야 한다.
- 각 출력 값  $x$  및 그 총합은  $0 < x < 21 \times 10^6$  범위 내에 있어야 한다.
- 입력 중 어느 것도 스크립트에 null 해시를 가질 수 없다.
- $nLockTime$  값은 0xFFFFFFFF 이하이어야 한다.
- 거래 크기(바이트 단위)는 최소 100 이상이어야 한다.
- 서명 연산의 수는 서명 연산 한도를 초과하지 않아야 한다.
- 언락 스크립트(unlocking script)와 락킹 스크립트(locking script)는 검증 규칙을 준수해야 한다.
- 모든 입력에 대해, 풀 또는 메인 브랜치의 블록에 일치하는 거래가 존재해야 한다.
- 각 입력에 대해, 참조된 출력이 메모리 풀 내 다른 거래에 존재할 경우(이중 지불 시도), 해당 거래는 거부된다.
- 각 입력에 대해, 참조된 출력 거래가 코인베이스 출력일 경우 최소 100 블록 이상의 컨펌을 가져야 한다.
- 각 입력에 대해, 참조된 출력이 존재해야 하며 이미 소비된 상태일 수 없다.
- 참조된 출력 거래를 사용하여 입력 값을 얻을 때, 각 입력 값 및 그 합은  $0 < x < 21 \times 10^6$  범위 내에 있어야 한다.
- 입력 값의 합이 출력 값의 합보다 작으면 거부된다.
- 거래 수수료가 비어 있는 블록에 포함되기에 너무 낮다면 거부된다.
- 각 입력의 언락 스크립트는 해당 출력의 락킹 스크립트에 대해 유효하게 검증되어야 한다.

이러한 조건들은 거래 검증 과정의 일부이며, 모든 거래는 이러한 검증 단계를 거치게 됩니다. 거래 검증 과정에서 발생하는 일의 상위 수준 개요는 아래 다이어그램에 설명되어 있습니다.



BSN이 새로운 거래를 수신하면, 이는 거래 관리자(Transaction Manager) 구성 요소로 전달되며, 여기서 거래 검증 프로세스가 시작됩니다. 거래 검증 과정은 네 개의 구성 요소로 이루어져 있으며, 각각을 살펴보겠습니다.

노드는 모든 거래를 반드시 검증할 필요는 없습니다. 실제로 백서에서는 “노드는 언제든지 네트워크를 떠나고 다시 합류할 수 있으며, 그들이 떠나 있는 동안 무슨 일이 있었는지는 작업증명 체인을 증거로 받아들인다”고 명시하고 있습니다.

백서는 노드가 수행해야 할 일을 정의하며, 노드가 거래를 수신한다면 반드시 해당 거래를 검증하고 전파해야 한다고 규정합니다.

노드는 거래 수용을 중단할 수 있지만, 이는 모든 거래를 수용하는 다른 노드와 경쟁하는 데 있어 손실을 감수해야 하는 위험을 동반합니다.

## TxManager

TxManager는 새로운 거래에 대해 기본 검사를 수행하고, 거래 검증 구성 요소를 위한 입력을 생성합니다.

- TxManager는 새로운 거래 메시지를 받아 거래에 존재하는 입력과 출력을 처리하기 위해 두 개의 개별 메시지를 생성합니다.
- 이 과정에서 먼저 거래의 스키마, 완전성, 중복 여부를 검증합니다.
- 그런 다음 입력을 위한 메시지를 처리하고, 소비되는 각 UTXO를 검증합니다. 검증이 성공하면, 검증된 거래 메시지를 거래 검증 구성 요소로 전달합니다.
- 또한 거래가 유효한 경우, 거래 저장소(Transaction Storage) 구성 요소를 호출하여 거래를 저장합니다.
- 동시에, UTXOStorage 구성 요소는 거래의 출력에 대해 생성된 메시지를 받아 새롭게 추가된 UTXO로 출력을 저장합니다.

## TxStorage

TxStorage는 TxManager 구성 요소에 의해 사용되며, 중복 검사 및 유효성 검사(sanity check)와 같은 기본 검사를 통과한 새로운 원시 거래(raw transaction)를 저장하는 데 활용됩니다.

## TxValidator

TxValidator는 전체 거래 검증, 스크립트 검증을 수행하며, 거래 검증 상태에 대한 최종 응답을 생성합니다.

- TxManager가 기본 유효성 검사를 수행한 후, TxValidator를 호출하여 합의 규칙 및 로컬 정책 규칙에 따른 거래의 전체 검증을 수행합니다.
- 거래가 모든 검증을 통과하면, 입력에 의해 소비되는 UTXO를 UTXOStorage에서 가져와 BSV 스크립트 엔진에 의해 검증될 스크립트를 구성합니다.
- 각 입력-이전 거래 출력 스크립트 조합은 스크립트 엔진을 통해 실행되어 입력이 사용 가능한지 검증하며, 성공적인 검증 결과를 생성합니다.
- 모든 입력에 대해 스크립트 검증을 반복 실행한 후, 모든 검증이 성공적으로 완료되었는지 평가합니다.

- 검증 중 어느 시점에서든 실패가 발생하면 검증은 실패 메시지와 함께 중단되며, 이 실패 메시지는 BSN으로 전달됩니다.
- 모든 검증이 성공적으로 완료되면, 유효한 거래를 메모리 풀(Mempool)로 전송합니다.

## BSVScriptEngine

BSVScriptEngine은 거래 검증기로부터 제공받은 스크립트에 대해 검증을 수행하고 성공/실패 응답을 반환합니다.

이러한 구성 요소들은 함께 거래 검증 기능을 제공합니다. 이 과정에서 UTXO Storage 구성 요소 및 메모리 풀(Mempool) 구성 요소와도 상호작용합니다.

블록 보조금(block subsidy)은 블록 보상(block reward)으로서, 네트워크의 에이전트(노드)가 거래 타임스탬핑, 정렬, 검증 서비스를 제공한 대가로 지급되는 일방적 계약에 따른 지급입니다.

## UTXO 저장소(UTXO Storage)

코인베이스 거래를 제외한 모든 유효한 거래는 최소 하나의 UTXO를 소비하며, 0개 이상의 새로운 UTXO와 0개 이상의 소비 불가능한 출력(Unspendable Outputs)을 생성합니다. 소비되는 UTXO는 반드시 이전에 성공적으로 완료된 거래에서 나와야 하며, 이는 현재 블록이나 이전 블록에 기록될 수 있습니다.

미사용 출력(UTXO)은 몇 밀리초 만에 생성되고 소비될 수도 있고, 수십 년 동안 미사용 상태로 남아 있을 수도 있습니다. 이는 미사용 출력이 소비되지 않는 한 영구적으로 저장(persisted)되어야 함을 의미합니다.

UTXO는 토큰 집합을 보관하는 봉투와 같습니다. 봉투가 한 번 열리면 다시 닫거나 재사용할 수 없습니다. 토큰은 한 봉투에서 다른 봉투로 이동합니다. 지갑은 토큰이 들어 있는 여러 봉투 집합을 보관합니다. 두 개의 봉투가 거래의 (두 개의) 입력으로 열리면, 토큰은 봉투에서 제거되어 원하는 수량으로 새로운 봉투에 추가됩니다.

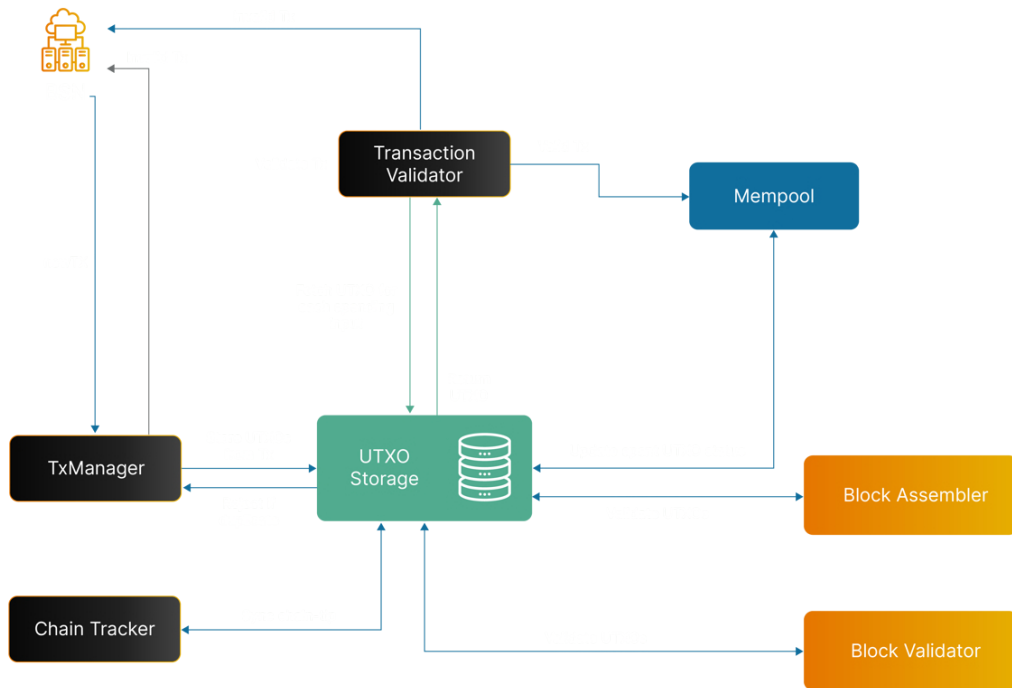
개인키는 다른 사람이 봉투를 열지 못하도록 막는 봉인(seal)과 같습니다. 공개키 또는 주소는 봉투가 전송되거나 접근되는 위치입니다. 비트코인 주소가 편지의 주소와 같은 역할을 하는 것과 같습니다. 노드(채굴자)는 봉투를 열기 전에 봉인이 유효한지 확인합니다. 진정한 봉인 소유자만 봉투를 열 수 있으며, 채굴자는 봉인의 소유자를 검증합니다. 하나의 봉투는 두 명 이상의 당사자에 의해 봉인될 수도 있습니다. 그런 경우 노드는 합의를 검증하여 봉투가 봉인될 때 설정된 규칙에 따라 열리도록 합니다.

그러나 법원은 게이트키퍼인 노드, 즉 검증자들에게 봉투를 열라고 명령할 수 있으며, 채굴자는 봉인을 깨고 봉투를 열어야 합니다.

UTXO는 봉투에 부여된 등록번호 또는 일련번호와 같습니다. 하나의 봉투에는 단 하나의 일련번호만 있으며, 이는 절대 재사용되지 않습니다. 토큰은 새로운 봉투로 옮길 수 있지만, 일련번호는 채굴자가 "스탬프"하여 원장에 기록할 때만 부여됩니다.

그 봉투는 유효하며, 토큰은 노드에 의해 블록체인에 기록되기 전에도 가상 상태로 존재합니다. 그러나 토큰을 등록하는 일련번호는 노드가 원장에 그 번호를 기록할 때만 영구적으로 부여됩니다.

UTXO 저장소는 UTXO의 저장(단기 및 장기)을 처리하는 일련의 구성 요소로 이루어져 있습니다. 저장 특성상 일부 UTXO는 캐시에, 일부는 단기 메모리에, 또 다른 일부는 장기 메모리에 유지될 필요가 있으므로, 저장소 자체는 UTXO의 활성화 정도에 따라 필요한 접근을 지원하도록 설계되었습니다. 또한 대부분의 노드 구성 요소들이 UTXO 상태를 조회하기 위해 사용됩니다. 아래 다이어그램에 설명되어 있습니다.



UTXO는 데이터베이스 내에서 어느 시점이든 다양한 상태에 있을 수 있습니다. 각 프로세스는 UTXO 저장소와 자체적인 상호작용을 수행합니다.

1. 새로운 거래가 검증 과정을 거치면, 이 거래의 출력(Output)에 새로운 UTXO가 생성됩니다.
2. TxValidator가 거래를 검증할 때, 해당 거래의 입력에서 소비되는 UTXO를 가져옵니다. 거래 내의 각 입력을 순회하며 UTXO를 가져오고, 데이터베이스 내의 해당 UTXO 항목은 잠금(lock) 상태가 되어 다른 거래가 해당 UTXO를 소비하지 못하게 합니다. (이 방식이 노드 내에서 최초 수신 규칙(first-seen rule)이 구현되는 방법입니다.)
3. 스크립트 엔진에 의해 검증되고 메모리 풀에 게시되면, 잠금 상태였던 UTXO는 소비됨(Spent) 상태로 변경됩니다.
4. 이 거래에 의해 새롭게 생성된 UTXO는 이후 수신되는 거래에 의해 소비될 수 있게 됩니다.
5. 오류 시나리오도 발생할 수 있으며, 이는 UTXO가 존재하지 않거나 잘못된 스크립트로 인해 소비 불가능(Unspendable)하거나 심지어 누락된 경우입니다. 이 경우에는 유효하지 않은 거래 오류가 발생합니다.
6. UTXO는 항상 Tip ID를 기준으로 생성됩니다. 따라서 Tip ID가 변경되면 UTXO의 상태도 변경됩니다. 이는 체인 추적기와 상호작용하여 동기화됩니다.
7. 블록 검증기(Block Validator)와 블록 조립기(Block Assembler) 또한 자신들이 소비하는 UTXO의 유효성을 보장하기 위해 UTXO 저장소 서비스를 사용합니다.

UTXO 집합은 항상 노드에 의해 유지되며, 노드가 항상 최신 UTXO 집합을 유지하기 때문에 가지치기(pruning)로부터 보호됩니다.

## 메모리 풀(Mempool)

메모리 풀(Mempool)은 검증된 거래가 일정 시간 동안 저장되는 임시 위치를 의미합니다. 그 목적은 확인되지 않은 거래를 관리하고 게시하는 것이며, 다음을 포함합니다:

1. 거래를 메모리에 보관한다.
2. 메모리 풀 내 거래에 의해 소비된 코인에 대한 정보를 제공한다.
3. 메모리 풀 내 거래에 의해 생성된 UTXO에 대한 정보를 제공한다.
4. 블록체인에서의 변경 사항(새로운 블록 추가, 체인 재구성)에 따라 거래를 일관되게 유지한다.
5. 유지 관리: 오래된 미채굴 거래 삭제, 메모리 풀 내 모든 거래의 총 크기 제한.

또한 블록 조립기(Block Assembler)에 다음과 같은 중요한 서비스를 제공합니다:

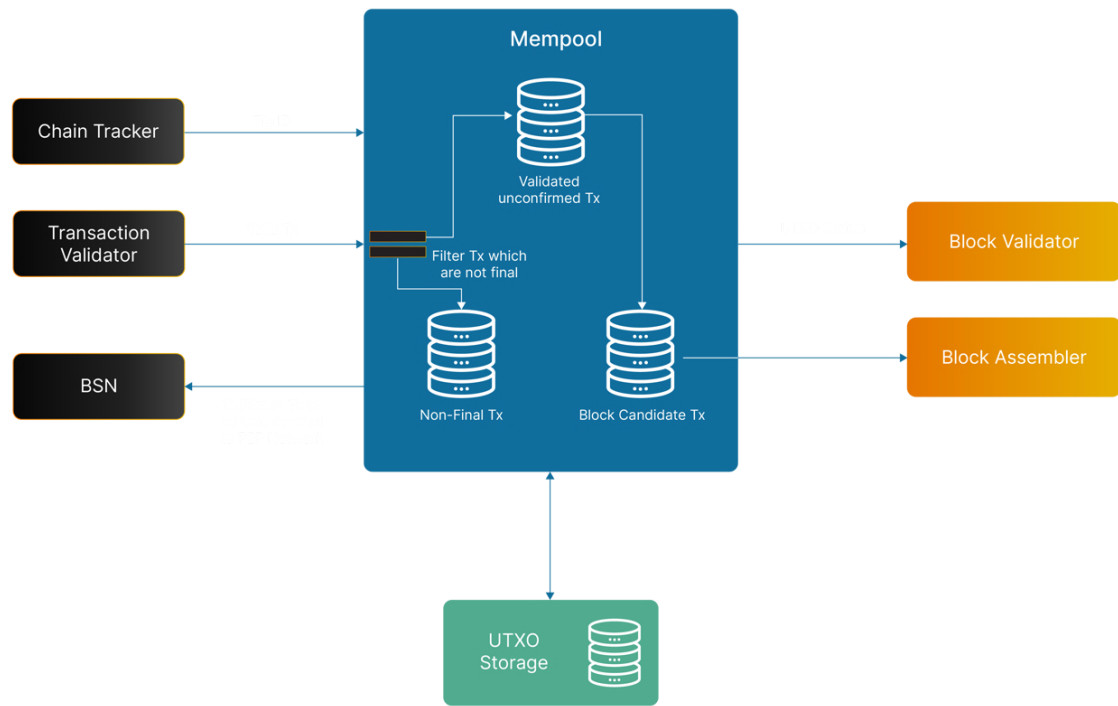
1. 블록 조립기에 토폴로지 순서로 정렬된 채굴 가능한 거래들을 제공한다.
2. 제거된 거래를 삭제하도록 블록 조립기에 알리고, 해당 거래의 모든 자식 거래 또한 제거되도록 한다.
3. 낮은 수수료(또는 수수료 없음), 비최종(non-final), 시간 잠금(time-locked) 거래를 위한 풀을 유지한다. 거래의 수수료 및 우선순위에 따른 필터링도 이 구성 요소에서 수행된다.

모든 거래는 하나의 단일 저장소에 저장됩니다. 그러나 거래 상태에 따라 마치 서로 다른 유형의 메모리 풀이 있는 것처럼 구분된 용어가 사용됩니다.

거래는 다음 중 하나의 메모리 풀에 속합니다:

- **기본 메모리 풀(Primary Mempool):** 이 노드가 구축하는 다음 블록에 선택된 거래
- **보조 메모리 풀(Secondary Mempool):** 다음 블록에 선택되지 않은 거래
- **비최종 메모리 풀(Non-Final Mempool):** 미확정 거래

아래 다이어그램은 다른 구성 요소들과의 상호작용을 보여줍니다.



다음 단계들은 메모리 풀(Mempool)이 다양한 거래 검증, 블록 조립 및 검증 과정에서 사용될 때의 기능을 설명합니다.

- 검증된 거래를 처리하여 블록 조립에 제공한다.
- 거래가 검증되면 BSN을 통해 브로드캐스트한다.
- 검증 서비스에 UTXO 상태(소비됨 및 미소비)를 제공한다.
- 블록 조립기에 검증된 거래를 제공한다.
- 다른 노드로부터 다운로드된 블록을 검증할 때, 블록 검증에 거래 데이터를 제공한다.

메모리 풀은 어떤 거래가 채굴되는지를 결정하는 데 중심적인 역할을 하며, 자체적으로나 네트워크 내 다른 노드에 의해 블록이 성공적으로 생성된 후 지속적으로 업데이트됩니다. 메모리 풀을 거래 집합으로 본다면, 채굴 과정은 다음과 같은 방식으로 메모리 풀을 업데이트합니다:

#### 네트워크 내 다른 노드가 블록을 채굴한 경우:

새로운 Mempool = 기존 Mempool - 채굴된 거래 - 이중지불 거래 - 이중지불 거래의 자식 거래

#### 로컬에서 블록 채굴(Block Mined Locally)

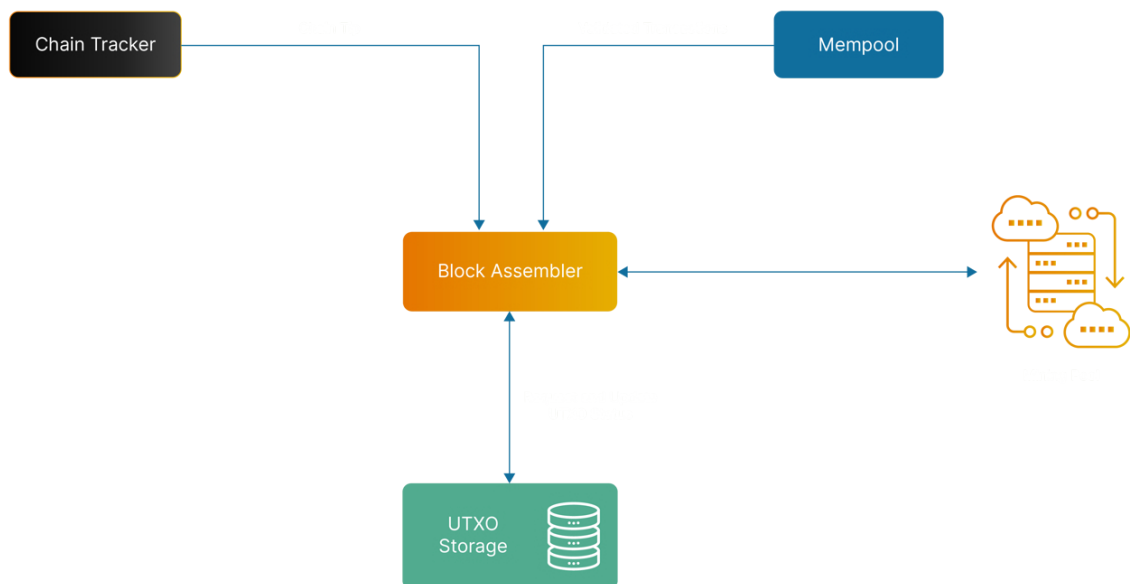
새로운 Mempool = 기존 Mempool - 채굴된 거래

거래는 메모리 풀에 들어온 후 기본적으로 2주가 지나 만료일에 도달하면 제거됩니다. 새로운 블록이 생성되어 다른 노드로 전파된 후, 새로운 블록에 포함된 거래들은 더 이상 메모리 풀에 있을 필요가 없으며 제거될 수 있습니다. 만약 이 노드가 생성한 블록이 승리한 블록이라면, 이제 필요하지 않은 거래는 블록 조립이 완료된 후 추가된 거래를 제외한 기본 메모리 풀(Primary Mempool) 내의 모든 거래입니다.

메모리 풀은 별도의 구성 요소로 간주해야 하는지, 아니면 실행 시점에 생성되는 거래 저장소(Transaction Storage) 또는 UTXO 저장소의 일부로 보아야 하는지에 대해 많은 논의가 있습니다. 본 문서는 현재 메모리 풀을 별도의 구성 요소로 설명합니다.

## 블록 조립기(Block Assembler)

블록 조립기의 주요 목적은 메모리 풀에 저장된 검증된 거래 목록을 가져와 거래를 추가하기 위한 새로운 블록 템플릿 데이터 구조를 생성하는 것입니다. 블록 조립기는 체인 추적기(Chain Tracker), 메모리 풀(Mempool), UTXO 저장소와 상호작용하며 블록 템플릿 생성을 조율합니다. 또한 블록 템플릿에 거래가 포함되기 전에 기본적인 검사를 수행하며, 거래와 UTXO 상태를 업데이트합니다.

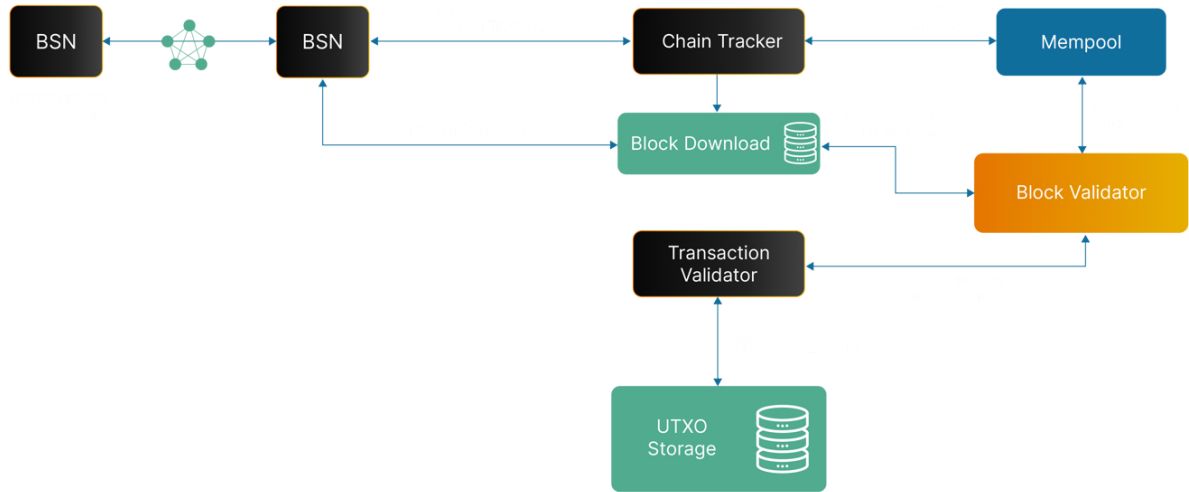


체인 추적기는 블록 조립기에 현재 체인 팁(Chain-tip)을 제공합니다. 조립기는 해당 팁 위에 새로운 블록을 구축하는데, 우선 메모리 풀에 존재하는 모든 검증된 거래를 가져옵니다. 그런 다음 거래들을 최초 수신 순서(first-seen order)로 정렬하고 거래 ID로부터 머클 트리 루트 값을 구축하여 머클 루트 값을 계산합니다. 이 값이 계산되면, 현재 난이도 값을 기준으로 블록 헤더를 구성합니다.

동시에 채굴 풀 소프트웨어는 최신 채굴 후보를 지속적으로 가져오기 위해 블록 조립기와 끊임없이 통신합니다. 블록 조립기는 채굴 풀의 요청에 응답하며, 업데이트된 블록 후보 헤더와 채굴 후보 값을 계속 제공합니다 (자세한 내용은 채굴(Mining) 항목 참조).

## 블록 검증(Block Validation)

블록 검증 과정은 블록과 그 안의 거래 데이터 및 해당 블록이 추가되는 체인 팁(chain-tip)을 검증하는 과정을 포함합니다. 블록 검증은 체인 추적기(ChainTracker)가 새로운 제안 블록에 대한 정보를 받거나, 새로운 노드 설정 시 현재 체인 팁과 동기화된 히스토리를 구축해야 할 때 수행됩니다. 주요 기능은 제공된 블록이 블록 메타데이터 및 해당 거래들의 정확성을 기준으로 검증되는 것입니다.



BSN이 다른 노드로부터 새로운 제안 블록에 대한 정보를 받으면, 해당 블록에 대한 검증 프로세스를 시작합니다. 먼저 체인 추적기와 상호작용하여 내부 체인 팁 세부 정보를 가져오고, 이후 블록 다운로드 과정을 거쳐 다른 노드가 제안한 블록을 수신합니다. 블록이 다운로드되면 블록 검증 프로세스가 수행됩니다. 블록 검증은 블록 메타데이터의 유효성을 확인하고, 블록 내 모든 거래를 검증합니다. 일반적으로 제안된 블록 내 약 97%의 거래는 노드가 자체 블록을 구축하는 과정에서 이미 검증된 상태이며, 이에 대한 확인은 메모리 풀(Mempool)에서 제공됩니다. 아직 노드가 보지 못한 나머지 거래들은 거래 검증 프로세스로 입력되어 유효성을 검증받습니다. 검증이 완료되면, 거래 목록을 기반으로 머클 트리를 계산하여 블록 헤더 값과 대조해 검증합니다. 모든 검증이 성공적으로 이루어지면, 노드는 해당 블록을 유효한 것으로 수용하고 그 위에 새로운 블록을 구축하기 시작합니다. 체인 추적기가 추적하는 체인 팁도 이 변경 사항을 반영하여 업데이트됩니다.

## 채굴 소프트웨어(Mining Software)

채굴은 블록체인의 가장 중요한 구성 요소 중 하나이지만, 그 과정 자체는 노드 소프트웨어의 다른 기능들과 상당히 분리되어 있습니다. 연결은 블록 조립기(Block Assembler)에 의해 이루어지며, 이는 후보 블록과 그 헤더를 준비하고, 이를 채굴 후보(mining candidate)라 불리는 형태로 채굴 풀 소프트웨어에 전달합니다.



후보 블록 헤더는 SHA256D(이중 SHA256 해싱)를 사용해 해시되어 제안 값을 계산합니다. 이 값은 이후 목표 값과 비교됩니다. 계산된 값이 목표 값보다 작다면(값의 선두에 있는 0으로 식별됨), 해답이 발견된 것입니다. 계산된 값이 목표 값보다 크다면, 논스(nonce)는 새로운 값으로 증가하여 SHA256D(블록 헤더)의 결과가 새로운 값이 되도록 합니다. 이 과정은 채굴 칩에 의해 끊임없이 반복됩니다. 해답이 발견되면, 이는 블록 조립기로 다시 전달되고, 블록 조립기는 체인 추적기(ChainTracker)와 BSN에 새로운 해답이 로컬에서 발견되었음을 알립니다. 이후 이 해답은 네트워크의 다른 채굴 노드들에게 전파됩니다.

다른 노드가 이 노드로부터 제안 블록에 대한 통지를 받으면, 해당 노드에서 블록 검증 과정을 시작하여 제안 블록이 유효한 블록인지 확인합니다. 블록 검증이 성공하면, 그들은 체인 팁 ID를 이 제안 블록으로 업데이트하고 가장 최근 블록으로 설정합니다. 이후 이 Tip ID를 가장 긴 체인으로 간주하여 새로운 블록을 구축하기 시작하며, 해답을 찾으면 위에서 설명한 동일한 과정을 따릅니다. 이는 블록체인 네트워크에서 끊임없이 발생하는 과정으로, 노드들에게 매우 시간 제한적이며 되돌리기 어려운 과정을 만듭니다.

만약 이 과정에서 노드가 잠시라도 오프라인이 된다면, 진행 중인 작업증명 과정 및 그들이 위치한 블록 높이와 동기화되지 않게 됩니다. 다시 합류하기 위해서는 먼저 오프라인 동안 생성된 블록을 다운로드해야 하며, 그 후 새로운 블록 채굴을 시작해야 합니다.

## 고아 블록(Orphan Blocks)

앞서 설명한 과정에서, 노드들이 동시에 블록 제안을 위한 해답을 찾는 상황이 발생할 수 있습니다. 이는 서로 다른 노드들이 여러 체인 팁을 가장 긴 체인으로 간주하고 그 위에 블록을 구축하는 일시적인 상황을 만들 수 있습니다. 이러한 상황은 동일하거나 다른 노드가 특정 체인 팁 위에서 다음 블록을 발견하여 그것이 가장 긴 체인이 될 때 해결됩니다. 이 과정은 반복적으로 계속 발생합니다. 두 개 이상의 체인 팁이 동시에 인식되었다가 새로운 제안 블록이 발견됨으로써 해결되는 경우, 새로운 블록이 구축되지 않은 체인 팁은 버려지게 됩니다. 이러한 시나리오에서는 당시에는 성공적인 해답이었지만 다른 노드가 해답을 찾음으로 인해 밀려난 블록이 고아 블록(orphan block)이 되며, 이후 네트워크에서 삭제됩니다.

## 무효 블록(Invalid Blocks)

노드가 블록 검증(Block Validation)에 실패한 블록을 제안하면, 그 제안은 무시되고 다른 노드들은 이전의 유효한 블록 위에 새로운 유효한 블록을 찾기 위한 시도를 계속합니다. 노드가 블록을 무효로 간주하는 이유에는 여러 가지가 있으며, 그 예시는 다음과 같습니다:

- 블록이 합의 규칙에 실패한 경우(예: 크기 초과)
- 블록이 채굴자에게 너무 많은 비트코인을 보상하는 경우
- 블록에 무효한 거래가 포함된 경우
- 블록에 유효한 작업증명 또는 타임스탬프가 포함되지 않은 경우

노드가 무효 블록을 제출한 경우, 해당 블록은 거부됩니다. 노드가 여러 개의 무효 블록을 제출하면, 네트워크의 다른 노드들은 노드의 IP를 차단하거나 네트워크 정보를 공유하지 않는 등 추가 조치를 취할 수 있습니다. 일반적으로 이러한 ‘차단(ban)’은 24~48시간 동안 유지되며, 이는 노드 운영자에게 반복되는 실수를 인식시키기 위한 목적을 가집니다. 각 노드는 이와 관련된 정책을 자체적으로 설정할 수 있습니다.

네트워크의 노드들이 어떤 당사자로부터 온 블록이든 자유롭게 수용하거나 거부할 수 있다는 점을 이해하는 것이 중요합니다. 각 노드는 네트워크의 대다수 노드가 유효한 사건의 체인으로 받아들인 것을 인지해야 하며, 이를 통해 항상 가장 긴 유효 체인 위에 블록을 구축하고 네트워크가 수용하지 않을 블록에 불필요한 자원을 사용하는 것을 최소화할 수 있습니다.

채굴 풀(Mining Pools)은 원래 설계 및 구현 당시 구상된 것이 아니라 이후에 발생한 현상입니다. 백서에서 예외로 언급된 것은 서버 팜과 데이터센터의 형성이었으며, 이들이 채굴 노드가 되는 것이었습니다. 약 10개의 주요 노드가 네트워크 해시 파워의 51%를 담당하고, 다른 지역에서는 약 100개의 더 작은 노드들이 운영될 것으로 예상되었습니다.

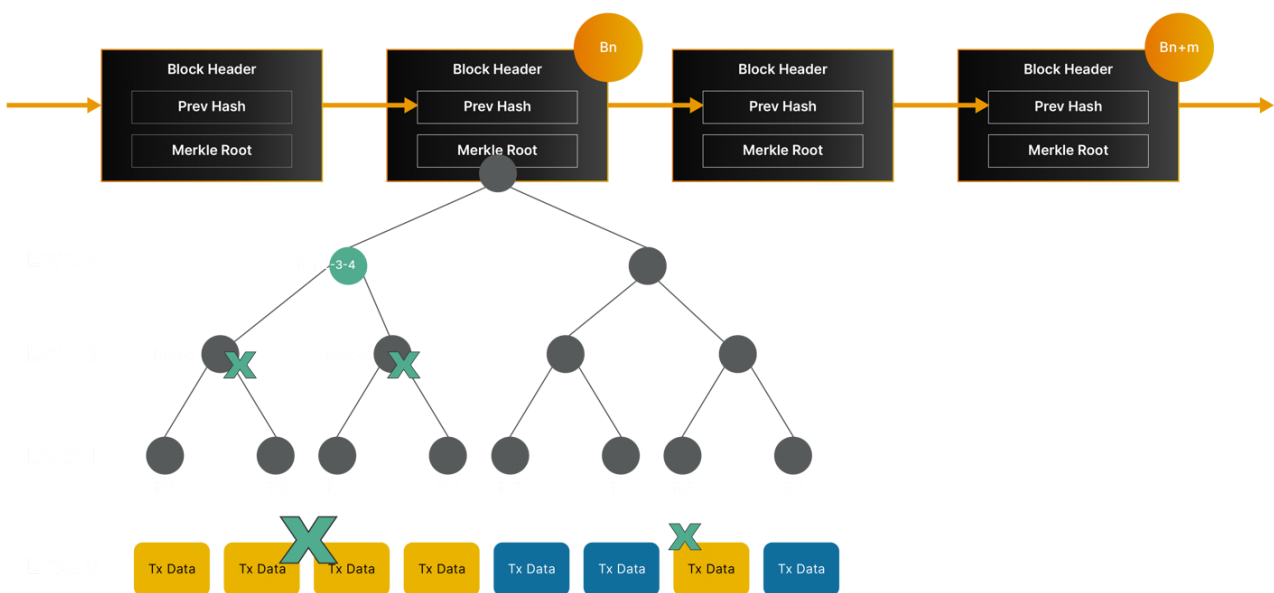
그러나 채굴 풀의 생성은 전 세계적으로 총 15개의 노드만 존재하게 되는 상황을 만들었으며, 이로 인해 언급된 수백 개의 소규모 노드의 존재는 사실상 사라졌습니다. 만약 당신이 채굴 풀에 속한 ASIC을 운영하고 있다면, 당신은 채굴자가 아닙니다. 단지 풀의 일부일 뿐이며, 노드 운영자 또는 풀에 아웃소싱된 기능을 제공하는 공급자일 뿐입니다.

현재는 단 3~4개의 채굴 풀만이 네트워크의 51%를 통제하고 있으며, 가장 큰 풀은 충분히 커서 해당 풀에 대한 어떠한 조치라도 네트워크 전체에 영향을 미칠 수 있습니다.

## 거래 가지치기(Pruning transactions)

노드들은 향후 필요성이 거의 없거나 전혀 없는 거래 데이터를 가지치기(pruning)하여 저장 요구량을 최소화할 수 있습니다. 많은 경우 거래 데이터에는 이후 거래들에 의해 이미 소비된 출력이 포함되어 있으며, 이는 사실상 노드가 저장하기에 불필요한 중복 데이터가 됩니다. 이러한 데이터는 삭제되어 노드의 저장 및 처리 용량을 최적화할 수 있습니다.

이것이 의미하는 바를 살펴보겠습니다.



예를 들어, 다이어그램에 나타난 블록 Bn에는 tx1부터 tx4까지의 거래가 있으며, 이 거래들의 UTXO는 이후 블록들의 거래에서 모두 소비되었고, 체인 팁이 블록 Bn+m에 도달했을 때 이미 모든 UTXO가 사용된 상태라고 가정합니다. 이제 다이어그램에 주황색으로 표시된 거래 데이터 블록은 노드가 더 이상 사용할 필요가 없는 데이터입니다. 따라서 노드는 Tx1, Tx2, Tx3, Tx4의 거래 데이터를 삭제하고 해당 해시(TxID)만 남겨두어도 향후 검증 목적으로 이 블록의 머클 루트를 계산할 수 있습니다. 사실, 다이어그램에서 보이는 것처럼 더 나아가 다음 레벨의 해시까지 포함한 전체 집합도 삭제할 수 있습니다. 즉, 노드는 레벨 1의 Tx1~Tx4 해시와 레벨 2의 HTx1-2 및 HTx3-4 해시까지 삭제할 수 있으며, HTx1-2-3-4 해시는 여전히 향후 머클 루트 계산 시 필요한 해시를 제공할 수 있습니다. 예를 들어, 거래 Tx5의 블록 내 존재를 검증할 때 활용할 수 있습니다.

또한 다이어그램의 Tx7 사례에서 보듯, 채굴자는 단순히 거래 데이터를 삭제하고 거래 데이터의 해시인 TxID만 보관함으로써 저장 공간을 절약하고 시스템을 최적화할 수 있습니다.

이 기능은 노드가 불법 콘텐츠를 데이터로 포함한 거래나 악의적이거나 법적 요구에 의해 블록체인 저장소에 서 제거해야 하는 거래 데이터를 삭제하는 경우에도 유용하게 활용될 수 있습니다.

거래 가지치기는 노드가 운영을 최적화하고 실제로 필요한 데이터만 저장하도록 하는 매우 유용한 기능입니다. 그러나 이로 인해 때로는 소비 불가능한 출력(예: 사토시 값이 0인 OP\_RETURN 데이터 출력)을 통해 데이터를 업로드하기 위해 특별히 생성된 거래들이 삭제될 수도 있습니다. 이러한 출력을 활용하려는 애플리케이션은 반드시 자신의 데이터 거래에 대한 백업, 머클 증명(Merkle proofs)까지 포함하여 저장해야 하며, 이를 통해 블록체인이 여전히 SPV 방법론을 사용하여 거래 검증에 활용될 수 있도록 보장해야 합니다. 대안적으로, 블록체인 데이터를 보관하고 이를 향후 접근하려는 이들에게 유료 서비스를 제공하는 이른바 아카이벌 노드(archival nodes)라는 새로운 비즈니스 모델이 등장할 수도 있습니다.

백서에서는 디스크 공간 절약을 위해 거래가 삭제/가지치기될 수 있다고 명시하고 있습니다. 이중 해시(double hash)의 사용은 블록 내의 정보를 전송하지 않고도 블록 검증을 가능하게 합니다. 이전 거래의 증거(proof)는 구성될 수 있으며, 정보는 가지치기되어도 블록체인은 계속 유지될 수 있습니다.

## 노드의 책임(Responsibilities of a Node)

블록체인 네트워크의 노드들은 네트워크에서 생성된 모든 거래에 대한 규칙 집행자(enforcer)입니다. 규칙 집합을 통과한 거래만이 새로운 블록에 추가되어 기록된 데이터의 불변하는 역사로 남습니다. 그러나 노드들은 새로운 규칙을 만들거나, 거래 내부에 어떤 데이터가 포함될지를 중재하지는 않습니다.

노드는 또한 일반적으로 기업으로서 운영됩니다. 지금까지 살펴본 것처럼, 단순히 고가의 하드웨어를 운영하는 것뿐만 아니라, 블록체인 네트워크의 성장하는 수요와 경쟁자들의 행보에 맞춰 지속적으로 업그레이드해야 합니다. 또한 소프트웨어 개선에 투자하거나 다양한 블록체인 관련 서비스를 제공하여 추가적인 수익원을 창출할 수도 있습니다. 이는 곧, 어떤 엔터티가 노드를 운영하는 경우, 그들의 운영이 상당히 공개적이어야 하며, 항상 자신이 속한 관할권에 대해 책임을 지는 합법적인 사업체여야 함을 의미합니다. 이는 블록체인 및 노드 운영에 있어 자주 간과되는 측면입니다.

그러나 BSV 블록체인과 같이, 작업증명(PoW) 과정뿐만 아니라 대용량 블록 저장에도 상당한 인프라가 요구되는 블록체인은, 노드 운영자가 시작만 하더라도 막대한 초기 설치 비용을 투자해야 합니다. 이러한 운영은 결국 데이터 센터에서 이루어지거나 대규모 클라우드 인프라를 소비하는 방식으로 진행되며, 두 경우 모두 합법적인 세금 및 신원 정보를 공개해야 합니다. 이는 의도적인 설계로, 이러한 노드들이 관할권에 알려진 공적 엔터티로서 자신들이 수행하는 서비스와 운영에 대해 책임을 지도록 하기 위함입니다. 이는 블록체인에서도 난당한 코인의 동결 및 복구 과정, 가지치기(pruning)나 법에 따라 요구되는 검열 활동 등을 구현하는 데 매우 중요한 요소입니다.

## SPV 지갑, 오버레이 및 SPV 프로세스 (SPV Wallets, Overlays and SPV Processes)

거래는 비트코인 원장(Bitcoin Ledger)에 기록을 생성하는 수단입니다. 이 섹션에서는 단순화된 결제 검증(Simplified Payment Verification, SPV) 프로세스를 심층적으로 살펴보고, 이를 사용하는 프론트엔드 사용자 애플리케이션인 SPV 지갑(SPV Wallets)과 백엔드 제공자 애플리케이션 및 서비스인 오버레이(Overlays)를 다룹니다.

### 단순화된 결제 검증(Simplified Payment Verification, SPV)

SPV는 거래가 블록에 존재하는지를 검증하는 과정입니다. '결제(Payment)'라는 용어는 블록체인 자체가 전자 현금 시스템이며, 모든 거래가 결제 행위라는 사실에서 비롯되었습니다. 거래가 원장에 데이터를 업로드하는 데 사용되더라도, 적어도 하나의 입력에서 적어도 하나의 출력으로 최소 1 사토시의 소유권을 이전하는 결제가 반드시 포함되어야 합니다.

이 과정을 설명하기 위해, 앨리스가 밥의 카페에서 커피를 사는 가상의 시나리오를 사용하겠습니다. 밥은 커피숍을 운영하며 CBDC를 사용한 결제를 받습니다.

1. 앨리스는 카운터에서 커피를 주문합니다.
2. 밥은 앨리스에게 결제를 받을 수 있도록 출력(금액 포함)을 미리 채워 넣은 템플릿 거래가 포함된 청구서를 제공합니다.
3. 앨리스는 자신이 소유하거나 제어하는 하나 이상의 UTXO를 사용하여 거래 템플릿의 적어도 하나의 입력을 채우고, 밥이 출력에 지정한 비용을 충당합니다.
4. 앨리스는 이제 입력이 채워진 거래 템플릿을 밥에게 반환하며, 거래 입력을 가져온 거래들의 머클 경로(Merkle Paths)를 함께 제공합니다. (이 과정은 앨리스와 밥이 거래 템플릿에 BEEF(Background Evaluation Extended Format) 포맷을 사용하면 훨씬 간단해집니다: [BRC 62 참고](#))
5. 밥은 거래를 수신하고 제공된 모든 입력에 대해 머클 증명을 수행한 뒤, 그 결과를 자신의 블록 헤더 체

인 사본과 비교하여 검증합니다. 이 시점에서 검증이 성공하면, 밥은 앨리스에게 커피를 건네줄 수 있으며, 단순히 한 잔의 커피라면 앨리스가 사기를 칠 위험은 매우 낮습니다.

6. 이후 밥은 거래를 오버레이 서비스(Overlay Service)에 제출하여 해당 거래 유형(이 경우 법정화폐 거래 유형)이 타임스탬프를 받도록 합니다.
7. 오버레이 서비스는 거래를 수신하고 밥이 수행한 동일한 검증을 실행하며, 거래 유형과 관련된 추가 검증도 수행합니다(예: 이 경우 입력 거래가 범위에 연루되어 법 집행기관에서 감시 중인지 확인). 오버레이 서비스가 검증을 마치면 내부 상태를 업데이트하고 밥에게 확인을 제공하며, 거래를 노드 네트워크에 제출합니다.
8. 노드는 자체 검증 절차를 수행하고 승인되면, 거래를 블록 템플릿에 추가합니다.
9. 1초 이내에 오버레이 서비스는 UTXO 조회 전문 서비스(UTXO Lookup Specialized Service)에 조회 요청을 보내 거래가 승인되었는지 확인할 수 있습니다. 이후 이 전체 확인 결과를 밥에게 전달합니다.
10. 거래가 블록에 타임스탬프되면, 머클 전문 서비스(Merkle Specialized Service)가 거래의 머클 경로를 구성하기에 충분한 정보를 오버레이 서비스에 제공합니다.
11. 오버레이 서비스는 머클 경로를 밥에게 제공하고, 만약 앨리스가 거래 템플릿에 출력을 추가했다면, 밥은 머클 경로를 앨리스에게 전달하여 그들이 제어하는 UTXO를 이후 거래에서 사용할 수 있도록 합니다.

밥은 거래가 블록에 타임스탬프될 때까지 기다릴 필요가 없습니다. 그는 로컬 SPV 검증만으로 결제를 즉시 승인할 수 있으며(0-conf), 또는 몇 초 정도 기다려 거래가 노드에 의해 수락되었는지 확인할 수도 있습니다(seen-conf).

이는 최초 수신 규칙(first-seen rule)이, 결제가 노드에 의해 한 번 인식되면 네트워크 내 노드들이 모든 이중지불 시도를 거부하도록 보장하기 때문에 가능합니다.

## 인프라 요구사항(Infrastructure Requirements)

위의 예시에서 밥과 오버레이 서비스가 필요로 하는 세 가지 요소는 다음과 같습니다:

**블록 헤더(Block Headers)** - 블록당 80바이트 × 연간 52,416블록 ≈ 연간 약 4.2MB 증가

**거래 데이터(Transaction data)** - 입력 TX가 채굴된 단순 p2pkh 거래의 경우 약 400바이트

**머클 경로(Merkle Path(s))** - 하나의 블록에 40억 개의 거래가 있다고 가정할 때 경로당 약 1KB

SPV는 애플리케이션이 전체 블록체인의 하위 집합을, 자신이 관심 있는 블록 헤더와 거래들을 사용하여 연결할 수 있도록 합니다.

## 즉시 결제(Instant Payments)

단순화된 결제 검증(SPV)의 또 다른 중요한 기능은 즉시 결제의 확인입니다.

앞서 설명했듯이, 밥은 거래의 유효성을 보장하기 위해 결제 승인을 받기 위해 노드를 사용합니다. 이때 노드는 원시 거래(raw transaction)에 대해 검증 단계를 수행하며, 여기에는 미사용 UTXO에 존재하는 스크립트 검증, 앨리스가 제공한 서명 검증, 그리고 거래 라이프사이클(transaction-lifecycle)에서 설명한 바와 같이 입력 및 출력 스크립트 모두의 실행이 포함됩니다.

**밥은 왜 즉시 거래를 신뢰할 수 있는가?**

그 답은 밥이 앞서 언급한 거래 데이터와 머클 증명을 수신할 때 수행하는 작업을 이해하는 데 있습니다.

**거래 데이터(Transaction Data)**

밥이 수신하는 거래 데이터에는 원시 결제 거래(raw payment transaction), 이전 거래의 머클 증명(Merkle Proof), 그리고 이전 거래 자체가 포함됩니다.

| 검증 단계(Verification Step) | 설명(Description)                           |
|--------------------------|-------------------------------------------|
| 단계 1, 2                  | 밥이 로컬에서 검증 수행                             |
| 단계 3                     | 밥이 이전 섹션에서 설명된 대로 BHC와 상호작용               |
| 단계 4                     | 밥이 노드를 사용해 서명 검증(Signature validation) 수행 |
| 단계 5                     | 밥이 로컬에서 검증 수행                             |

위에서 설명했듯이, 단계 1, 2, 3, 5는 밥이 로컬에서 수행합니다. 이는 잘못된 거래에 대한 대부분의 오류 시나리오가 밥에 의해 로컬에서 검증됨을 의미하며, 사실상 이 과정을 노드와 무관하게 만듭니다.

단계 4 또한 밥이 직접 수행할 수 있지만, 스크립트 검증을 실행하기 위한 추가 구성 요소가 필요합니다. 이 구성 요소는 노드 소프트웨어의 일부로 제공되며, 그렇기 때문에 위 시나리오에서 밥은 이 검증을 채굴자에게 위임합니다. 왜냐하면 밥이 로컬에서 스크립트 검증을 수행한다 하더라도, 여전히 이중 지불(double spend) 검증은 노드에 의존해야 하기 때문입니다.

입력에 존재하는 서명은 디지털 서명입니다. 이는 신용카드를 받을 때 영수증에 서명하고, 카드에 있는 서명과 일치하는지를 확인하는 상인 서명 절차와 유사합니다. 디지털 서명은 대부분의 국가에서 10년 이상 법적으로 구속력이 있는 것으로 인정되어 왔습니다. 따라서 거래에 포함된 디지털 서명이 유효하다면, 이는 상인에게 제시된 거래에 대해 신뢰를 제공할 수 있으며(신용카드와 마찬가지로), 이를 통해 결제가 안전하고 즉시 이루어질 수 있습니다.

공개키와 신원 사이의 검증 가능한 연결이 필요하며, 상인은 규제 요구 사항에 따라 이를 확인할 수 있습니다(예: 일정 금액 이상의 결제의 경우 송신자의 신원 제공이 법이나 규제로 의무화됨). 이 연결은 개인 정보 보호를 위해 신원은 오프체인에 저장하고, 키는 온체인에 공개하는 방식으로 데이터 저장소에 보관됩니다.

## 디지털 서명이 검증되면 무엇이 일어나는가?

아래 다이어그램은 디지털 서명 과정의 상위 수준 설명을 제공합니다.

이 과정은 다음의 구성 요소로 이루어져 있습니다(자세한 과정 설명은 *privacy* 항목 참조):

- 서명된 메시지(Signed message)
- 디지털 서명(Digital signature)
- 공개키(Public Key)

앞서 다이어그램에서 설명했듯이, 디지털 서명과 공개키는 거래 입력(Input)에 포함되어 있습니다. 서명된 메시지는 거래에서 제공된 정보와 머클 증명(Merkle proof)을 기반으로, 검증 과정 수행 중에 구성됩니다. 메시지 자체는 다음과 같은 형태를 가집니다:

색상은 결제 거래와 이전 거래에서 가져온 정보의 위치를 나타냅니다.\

알고리즘은 Sighash 플래그 값(All, none, 입력 단일 선택 및 수정자, ANYONECANPAY)에 따라 메시지를 구성하는 처리를 수행합니다.

다이어그램에서 플래그 값은 SIGHASH\_ALL | ANYONECANPAY로 가정됩니다.

보는 바와 같이, 구성된 메시지는 이전 거래 스크립트의 무결성뿐만 아니라 UTXO 금액도 요구합니다. 무결성을 보장하기 위해 현재 거래에서 필요한 필드 또한 포함합니다. 이 메시지가 서명되면, 이는 서명의 유효성뿐만 아니라 소비되는 거래 출력(outpoint)의 무결성과 현재 거래의 유효성까지 보장합니다.

서명의 검증이 정확하다면 즉시 결제가 가능합니다. 이때 메시지는 이전 거래와 현재 결제 거래 양쪽의 정보를 사용하여 소비 방식의 무결성을 보장합니다. 밥이 이를 로컬에서 수행한다면, 결제와 서명이 유효하다는 것에 대해 매우 확신할 수 있으며, 안전하게 결제를 수락할 수 있습니다. 반면, 밥이 서명 검증을 노드에 위임한다면, 결제가 유효하다고 수락하기 전에 노드로부터 응답을 받아야 합니다.

요약하자면, 디지털 서명의 검증에는 다음이 필요합니다:

- 서명될 메시지
- 이전 거래로부터 일부 데이터를 포함하는 서명된 메시지 (예: 값과 락킹 스크립트)
- 값과 락킹 스크립트의 무결성

단순화된 결제 검증(Simplified Payment Verification, SPV) 검사는 이전 거래의 모든 데이터에 대한 무결성을 제공할 수 있습니다.

상인인 밥은 앨리스로부터 직접 결제를 수락할 수 있으며(피어-투-피어, 심지어 오프라인에서도 가능), 단순화된 결제 검증 과정을 수행함으로써 앨리스에게 속지 않을 것이라는 확신을 가질 수 있습니다.

이 과정은 사실상 즉시 이루어지며, 모든 결제가 블록체인에서 정산되므로 안전하고 보안이 보장됩니다. 결제 확인에 걸리는 시간은 전통적인 결제 네트워크와 대조되는데, 기존 네트워크에서는 정산에 몇 시간에서 며칠까지 걸릴 수 있습니다.

# 무결성 검사(Integrity Checks)

SPV의 처음 두 가지 기능은 블록체인 상에서 거래의 존재를 검증하는 것이었습니다. 첫째는 소비되는 UTXO를 생성한 이전 거래의 존재를 검증하는 것이고, 둘째는 입력 UTXO가 유효한 서명을 포함하는지를 검증하는 것이었습니다. 그러나 이 두 가지가 검증되더라도, 의도된 기능을 수행하는 디지털 서명의 무결성을 위한 **락킹 스크립트의 무결성**이라는 또 하나의 검증이 필요합니다. 락킹 스크립트는 언락 스크립트를 규정하며, 거래의 완전한 무결성을 위해 반드시 디지털 서명 요구 조건을 포함해야 합니다.

여기서 "완전한 무결성"이란 앨리스가 자금의 소유권을 밥에게 디지털 서명으로 이전하는 것을 의미합니다. 다음은 이러한 개념을 설명하기 위한 예시 스크립트입니다.

이전 거래의 락킹 스크립트:

```
OP_DUP OP_HASH160 <Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG
```

입력(언락) 스크립트:

```
<Signature> <Public Key>
```

위의 락킹 스크립트는 소비하는 입력 스크립트가 앨리스에서 밥으로 자금을 이전하기 위한 디지털 서명을 반드시 포함하도록 요구합니다(공개키에 대한 서명을 통해).

다른 예시를 보겠습니다:

이전 거래의 락킹 스크립트:

```
OP_CHECKSIG
```

입력(언락) 스크립트:

```
<Signature> <Public Key>
```

이 예시가 보여주듯, 어떤 유효한 서명과 공개키의 조합도 거래를 유효하게 만들 수 있습니다. 이는 디지털 서명 과정에서 요구되는 법적 관점의 거래 무결성을 깨뜨립니다. 따라서 앨리스는 이전 거래의 자금의 의도된 수신자이자 정당한 소유자가 아닐 수 있음에도 불구하고, 단순히 가능한 상황 때문에 이를 소비할 수 있고, 밥은 잠재적으로 도난당한 자금을 수취할 수 있습니다.

또 다른 스크립트 예시는 다음과 같습니다:

락킹 스크립트 :

```
OP_DROP OP_DROP OP_TRUE
```

언락킹 스크립트 :

<Signature> <Public Key>

어떠한 문자열 쌍이라도 거래를 유효하게 만들 수 있으며, 이 경우 디지털 서명의 무결성은 보호되지 않습니다.

요약하자면, 락킹 스크립트의 무결성은 게시된 거래의 무결성을 입증하는 데 있어 중요한 요소입니다. 그 무결성은 다음을 통해 보장됩니다:

1. 공개키를 명시적으로 지정하는 것
2. 디지털 서명을 명시적으로 요구하는 것

세 가지 SPV 프로세스의 무결성이 모두 보장될 때, 보안적이고 사실상 즉시 이루어지는 진정한 피어-투-피어 결제가 가능해집니다.

SPV 시스템은 매우 작고 단순한 애플리케이션이며, 비록 이 예시에서는 결제 애플리케이션을 보여주었지만, 동일한 개념과 아이디어를 사용해 데이터 거래를 위한 유사한 애플리케이션을 구축할 수도 있습니다. 이러한 애플리케이션은 라이트 클라이언트(Light Clients)라고 불리며, 그 인프라 설계는 SPV 인프라(SPV infrastructure)라고 합니다.

## SPV 지갑 및 오버레이(SPV Wallets & Overlays)

진정한 글로벌 블록체인은 단순히 대규모 거래 처리 능력을 보여줄 뿐만 아니라, 어떻게 확장할 수 있는지를 고려할 수 있는 네트워크입니다.

블록체인과 관련하여 흔히 오해되는 점은, 애플리케이션에서 블록체인을 활용하고자 하는 기업과 사용자가 반드시 노드를 운영해야 한다는 것입니다. 이는 Web3 솔루션을 구축하려는 기업과 개발자들에게 막대한 인프라 부담을 줍니다.

사토시 나카모토 -

"설계는 전체 블록체인을 필요로 하지 않는 라이트웨이트 클라이언트를 설명합니다. 설계 PDF에서는 이를 단순화된 결제 검증(Simplified Payment Verification)이라고 부릅니다. 라이트웨이트 클라이언트는 거래를 송수신할 수 있지만 블록을 생성할 수는 없습니다. 결제 검증을 위해 노드를 신뢰할 필요도 없으며, 여전히 스스로 검증할 수 있습니다.

라이트웨이트 클라이언트는 아직 구현되지 않았지만, 필요할 때 구현할 계획입니다. 현재로서는 모든 사람이 전체 네트워크 노드를 실행하고 있습니다.

나는 노드가 10만 개를 넘지 않을 것이라고 예상합니다. 아마도 더 적을 것입니다. 더 많은 노드가 참여할 가치가 없는 균형 상태에 도달할 것입니다. 나머지는 수백만 개의 라이트웨이트 클라이언트가 될 수 있습니다.

균형 상태에서 많은 노드들은 서버 팜이 될 것이며, 한두 개의 네트워크 노드가 LAN을 통해 서버 팜의 나머지에 데이터를 공급할 것입니다."

SPV 지갑과 오버레이를 사용하면, 기업이 직접 노드를 운영할 필요가 없습니다.

네트워크 토폴로지 측면에서, P2P 상호작용과 수신자가 로컬 검증을 수행할 수 있는 능력이 결합되면, 네트워크 활동의 대부분이 네트워크 가장자리(edge)로 이동하게 되어 네트워크 부하와 데이터 저장 요구가 크게 분산되고 지역화됩니다.

라이트 클라이언트가 어떻게 설계되어야 하는지에 대한 엄격한 정의는 없습니다. 다만, 이러한 애플리케이션은 일반적으로 SPV 인프라를 직접 실행하거나 이를 대신 수행하는 서비스 제공자에게 연결됩니다. 따라서 블록을 생성하지 않는 모든 애플리케이션은 라이트 클라이언트가 됩니다. 여기서 '클라이언트'라는 용어는 웹 애플리케이션에서 사용되는 클라이언트-서버 아키텍처의 클라이언트 역할과 유사합니다. 이 경우 중앙의 노드 네트워크가 블록체인 서버 역할을 하고, 그 외의 모든 애플리케이션은 그 클라이언트가 됩니다.

블록체인 네트워크의 전체 모습을 보면, 네트워크의 중심에는 소수의 노드만 존재하고, 나머지 대부분의 애플리케이션은 라이트 클라이언트로서 기능하게 됩니다.

아래 다이어그램은 네트워크 토폴로지의 전체 뷰를 보여주며, 노드를 제외한 모든 요소들을 라이트 클라이언트로 식별합니다.

### 이러한 애플리케이션은 어떤 모습일까?

데이터 센터나 클라우드 플랫폼에 호스팅되는 애플리케이션은 블록체인과 상호작용할 수 있는 일부 구성 요소를 포함하게 됩니다. 이러한 애플리케이션은 주로 거래를 블록체인에 제출하여 타임스탬프를 받는 데 집중합니다. 애플리케이션은 자신들의 거래와 해당 머클 증명(Merkle Proof)을 직접 저장할 수 있으므로 블록체인으로부터 데이터를 읽어올 필요는 없습니다.

클라이언트 애플리케이션의 블록체인 인프라 요구사항은 다음과 같습니다:

1. **SPV 지갑(SPV Wallet)** — 최소한 다음 기능을 포함해야 함:
  1. 키 관리(Key Management)
  2. 디지털 서명(Digital Signatures)
  3. 키, 사용자 신원 및 데이터의 백업과 저장 같은 지갑 기능
  4. 거래 관리자(Transaction Manager)
  5. 기능 요구사항에 따른 UX/UI
2. **오버레이 서비스(Overlay Service)** 또는 구성 요소(지갑 자체의 일부일 수도 있음)
  1. 거래 검증(SPV 및 추가 검증 로직 포함)
  2. 거래를 노드에 브로드캐스트
  3. 머클 증명 검색 및 저장
  4. SPV 프로세스 검증기
  5. 서명 및 스크립트 검증기

현재 대부분의 노드는 거래 및 UTXO 조회를 허용하는 API 엔드포인트를 제공합니다. 그러나 테라노드(Teranode)와 만다라(Mandala) 네트워크 토폴로지가 도입되면, 노드들은 더 이상 이러한 API를 제공하지 않게 됩니다. 대신, 이러한 접근은 노드 레벨에 존재하지만 노드 운영의 일부는 아닌 **전문화된 서비스(Specialized Services)**에 의해 제공됩니다. SPV를 위해 필요한 두 가지 전문화 서비스는 **머클 서비스(Merkle Service)**와 **UTXO 조회 서비스(UTXO Lookup Service)**입니다.

## 머클 서비스(Merkle Service)

머클 서비스는 서브트리나 부분 머클 트리와 같은, 노드들이 사용하는 것과 유사한 정보를 수신하여 각 블록에 대한 머클 경로(Merkle Path)의 상위 부분을 생성합니다. 오버레이 서비스는 이 정보를 기반으로 전체 머클 경로를 구축할 수 있으며, 이를 SPV 지갑으로 전달하여 향후 거래에서 사용할 수 있습니다.

## UTXO 조회 서비스(UTXO Lookup Service)

UTXO 조회 서비스는 또 다른 전문화 서비스(Specialized Service)로, 네트워크 UTXO의 현재 상태를 추적하여 노드 활동을 따릅니다. 오버레이 서비스는 UTXO 조회 서비스에 조회 요청을 보내 자신이 관심 있는 UTXO의 현재 상태를 확인하고, 로컬 UTXO 저장소를 그에 맞게 업데이트할 수 있습니다.

비트코인 협회(Bitcoin Association)는 이러한 인프라를 위한 참조 구현(reference implementations)을 시작점으로 제공합니다. 아래 다이어그램은 이 구현의 개요를 보여줍니다.

SPV 지갑 및 오버레이 서비스의 참조 구현은 기업과 개발자가 SPV, 타임스탬핑(timestamping), 소액 결제/마이크로트랜잭션을 애플리케이션에서 사용하기 위해 필요한 구성 요소를 제공합니다:

- 간단한 웹 지갑
- 블록 헤더 클라이언트
- 거래 생성기 및 브로드캐스터
- ARC(브로드캐스트 클라이언트)
- Paymail(사용자 경험에서 공개키 사용을 단순화하기 위한 이메일 형태의 사용자 가독 주소)
- 대부분의 SPV 프로세스 및 지갑 기능을 수행하기 위한 완전한 라이브러리

블록체인이 탈중앙화된 것은 채굴자를 위한 피어 네트워크가 있기 때문이 아닙니다. 노드를 허가 없이 많이 실행할 수 있기 때문도 아닙니다. 그것을 탈중앙화된 교환 시스템으로 만든 것은 SPV와 IP 대 IP 거래를 수행할 수 있다는 사실이었습니다.

탈중앙화되고 중개자가 없다는 것은 앨리스와 밥이 직접 통신할 수 있음을 의미합니다. 예를 들어, 앨리스가 밥과 거래를 교환하고, 밥이 해당 거래를 등록할 수 있도록 전송하는 것입니다. 이것이 탈중앙화 시스템을 만드는 방식입니다.

노드들은 분산된 무결성 서비스를 형성하지만, 탈중앙화되거나 탈중앙화된 교환을 만드는 데 관여하지는 않습니다. 블록체인을 탈중앙화된 것으로 만드는 것은 노드가 아니라, 앨리스에서 밥으로의 직접적인 전송입니다.

# 네트워크 토폴로지(Network Topology)

## 만다라 업그레이드(Mandala Upgrade)

만다라 업그레이드는 블록체인 네트워크에서 확장성, 비용 효율성, 전반적인 성능을 향상시키는 중요한 발전입니다. 이 업그레이드는 주로 비트코인 SV(BSV) 네트워크를 개선하는 데 초점을 맞추고 있으며, 이를 더욱 견고하고 엔터프라이즈 솔루션에 적합하도록 만듭니다.

### 핵심 구성 요소(Key Components)

#### 테라노드(Teranode)

이 핵심 노드 네트워크는 효율성, 보안성, 초고속 처리량을 제공하는 데 필수적입니다.

#### 오버레이 서비스(Overlay Services)

이 서비스들은 네트워크의 확장성과 성능을 확장하며, 디지털 화폐 및 데이터 서비스와 같은 다양한 애플리케이션을 지원합니다.

#### 애플리케이션(Applications)

SPV를 기반으로 구축되어, 피어-투-피어 엣지 검증(p2p edge validation)과 블록체인과의 통합을 가능하게 합니다.

---

## 블록체인 만다라 개념(The Blockchain Mandala Concept)



**초소규모 세계 네트워크(Ultra-Small-World Network)**

빠르고 비용 효율적이며, 장애와 공격에 강인한 고도로 연결된 다층 네트워크입니다.

**높은 확장성과 성능(High Scalability and Performance)**

네트워크 아키텍처는 방대한 거래량을 고속으로 처리할 수 있으며, 이는 엔터프라이즈 수준의 애플리케이션에 필수적입니다.

**현재 네트워크의 한계(Current Network Limitations)**

현재의 블록체인 네트워크는 여러 가지 문제에 직면해 있습니다:

- **제한된 계층 구조(Limited Layers):** 채굴 노드와 애플리케이션이라는 두 계층만 존재하여 전문화와 확장이 제한됩니다.
- **피어-투-피어 연결(Peer-to-Peer Connectivity):** SPV의 채택 부족과 비채굴 노드 의존으로 인해 제한적입니다.
- **노드 소프트웨어 한계(Node Software Limitations):** 성능이 하드웨어 및 설정에 따라 달라집니다.
- **자원 소모(Resource Drain):** 비채굴 노드는 네트워크에 기여하지 않으면서 자원만 소모합니다.

## 만다라 업그레이드 해결책(Mandala Upgrade Solutions)

만다라 업그레이드는 3계층 네트워크 아키텍처를 도입하여 이러한 한계들을 해결합니다:

1. **테라노드 계층(Teranode Layer):** 초고속 처리와 대규모 확장을 보장합니다.
2. **오버레이 서비스 계층(Overlay Service Layer):** 전문화와 비즈니스 로직의 효율적 처리를 가능하게 합니다.
3. **애플리케이션 계층(Application Layer):** P2P 통신과 검증을 통해 프라이버시와 기능을 강화합니다.

## 노드(Nodes)

비트코인 백서에서는 노드의 동작을 섹션 5에서 다음과 같이 정의합니다:

1. 새로운 거래는 모든 노드에 브로드캐스트된다.
2. 각 노드는 새로운 거래를 수집하여 블록에 담는다.
3. 각 노드는 자신의 블록에 대해 어려운 작업증명(proof-of-work)을 찾는다.
4. 노드가 작업증명을 찾으면, 그 블록을 모든 노드에 브로드캐스트한다.
5. 노드는 블록 내의 모든 거래가 유효하고 이미 소비되지 않았을 경우에만 해당 블록을 수용한다.
6. 노드는 수용된 블록의 해시를 이전 해시로 사용하여 다음 블록을 생성함으로써 해당 블록의 수용을 표현한다.

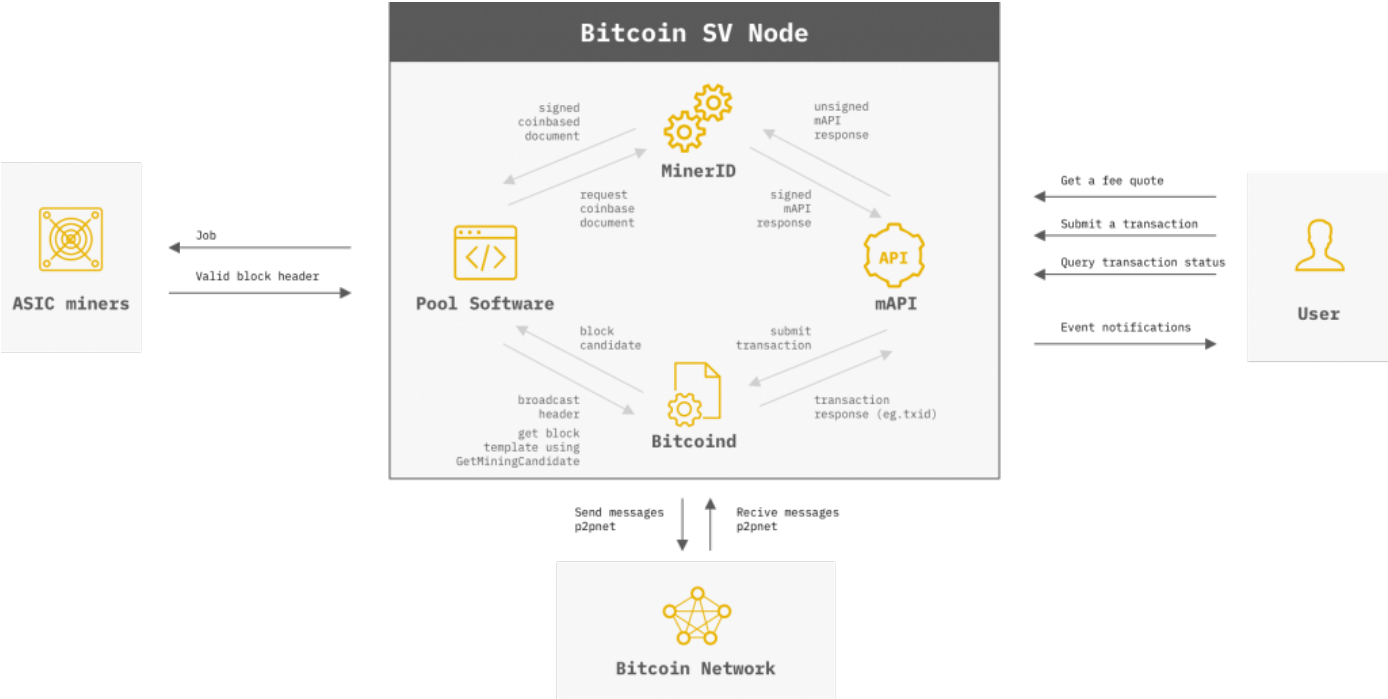
위 내용을 풀어서 설명하면, 노드는 다음과 같은 네트워크 엔터티입니다:

1. 새로운 블록을 체인에 추가하기 위해 적극적으로 경쟁하며, 실제로 블록을 생성하는 데 성공해야만 자신을 노드라고 부를 수 있습니다.
2. 거래를 검증하고 이를 타임스탬프를 찍어 블록에 기록합니다. 중요한 점은, 이들이 거래를 저장하거나 제공할 책임은 없다는 것입니다.
3. 노드는 네트워크 합의 규칙과 자체 로컬 정책을 집행하면서 요구되는 행동을 수행합니다.

노드는 네트워크의 중심에 위치하며, 경제적 필요성으로 인해 서로 밀접하게 연결되어 작은 세계 네트워크(small-world network)를 형성합니다.

사용자 및/또는 서비스는 거래를 노드 네트워크에 제출하여 타임스탬프를 받거나, 단순화된 결제 검증(SPV)을 위해 필요한 블록 정보를 수신하는 방식으로 노드 네트워크와 상호작용합니다.

# 아키텍처(Architecture)



## 외부 (P2P 네트워크):

- 다른 노드를 발견하고 연결한다.
- 다른 노드로부터 메시지를 송수신한다.

## 내부:

- 풀 소프트웨어 및 기타 도구에 RPC를 노출한다.
- 선택적으로 REST 인터페이스를 활성화할 수 있다.

## 외부 (Stratum 프로토콜):

- ASIC 채굴기가 연결하여 블록 헤더 채굴을 시작할 수 있도록 API를 노출한다.
- ASIC 채굴기에 작업을 전송한다.
- 유효한 공유(valid shares) 또는 유효한 블록 헤더를 수신한다.

## 내부 (Bitcoin RPC):

- 거래 제출을 위해 Bitcoin RPC에 연결한다.
- 거래 응답(예: txid)을 수신한다.
- 이중 지불(double spend) 및 머클 증명(Merkle Proofs)에 대한 이벤트 알림을 제공한다.

# 테라노드(Teranode)

[라이브 대시보드](#)

# 오버레이 서비스(Overlay Services)

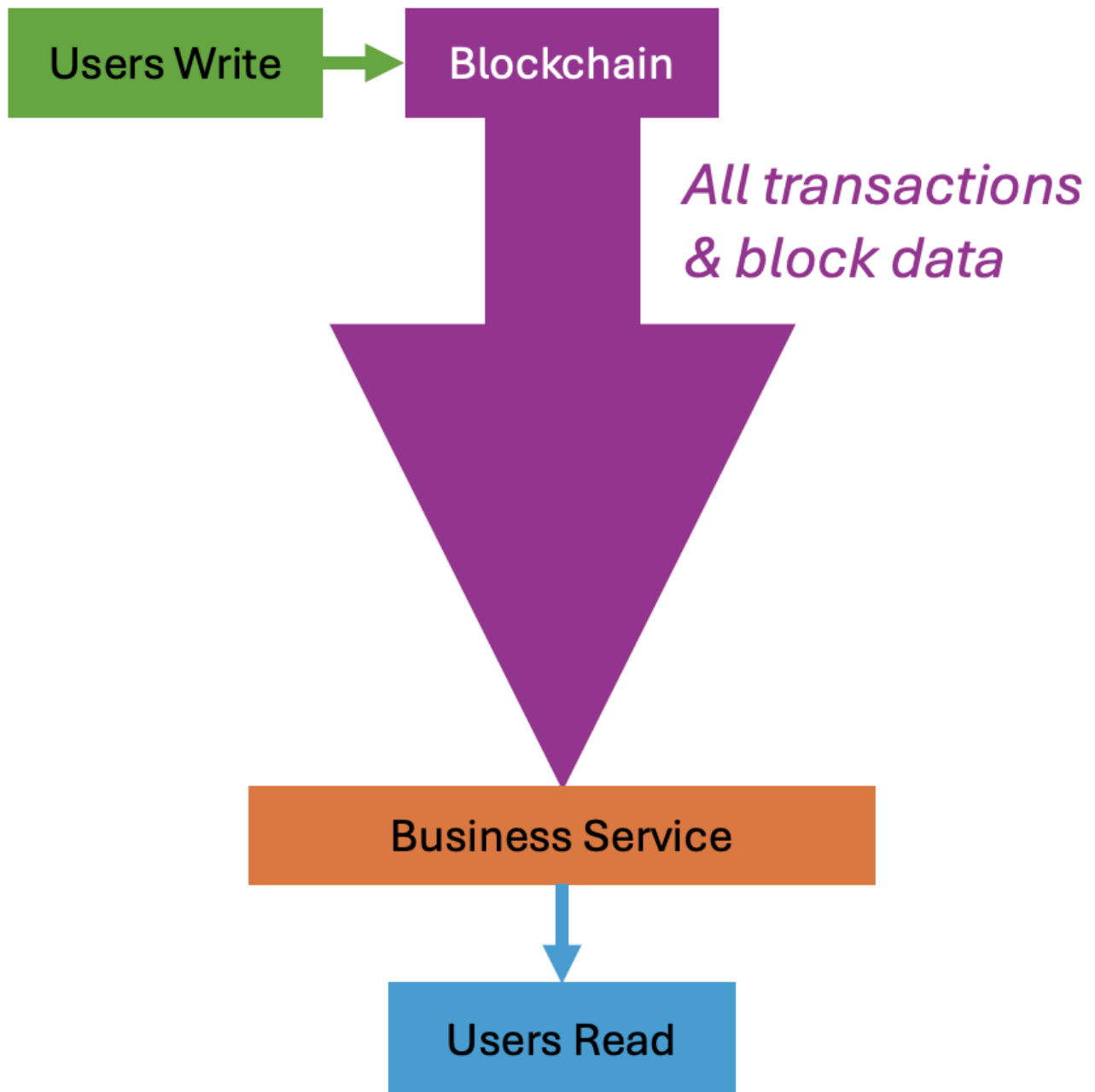
## 정의(Definition)

컴퓨터 네트워킹에서 오버레이(Overlay)란 기존 물리적 네트워크 위에 구축된 가상 네트워크를 의미합니다. 이는 라우팅, 피어-투-피어 네트워킹, 분산 컴퓨팅 등의 서비스를 제공하며 기존 네트워크(Underlay)를 보완하거나 확장합니다. BSV에서 오버레이는 BSV 노드 네트워크 위에서 운영되며, 거래 조회, 토큰 관리, 오픈 프레디케이트(Open Predicates) 등의 서비스를 제공합니다.

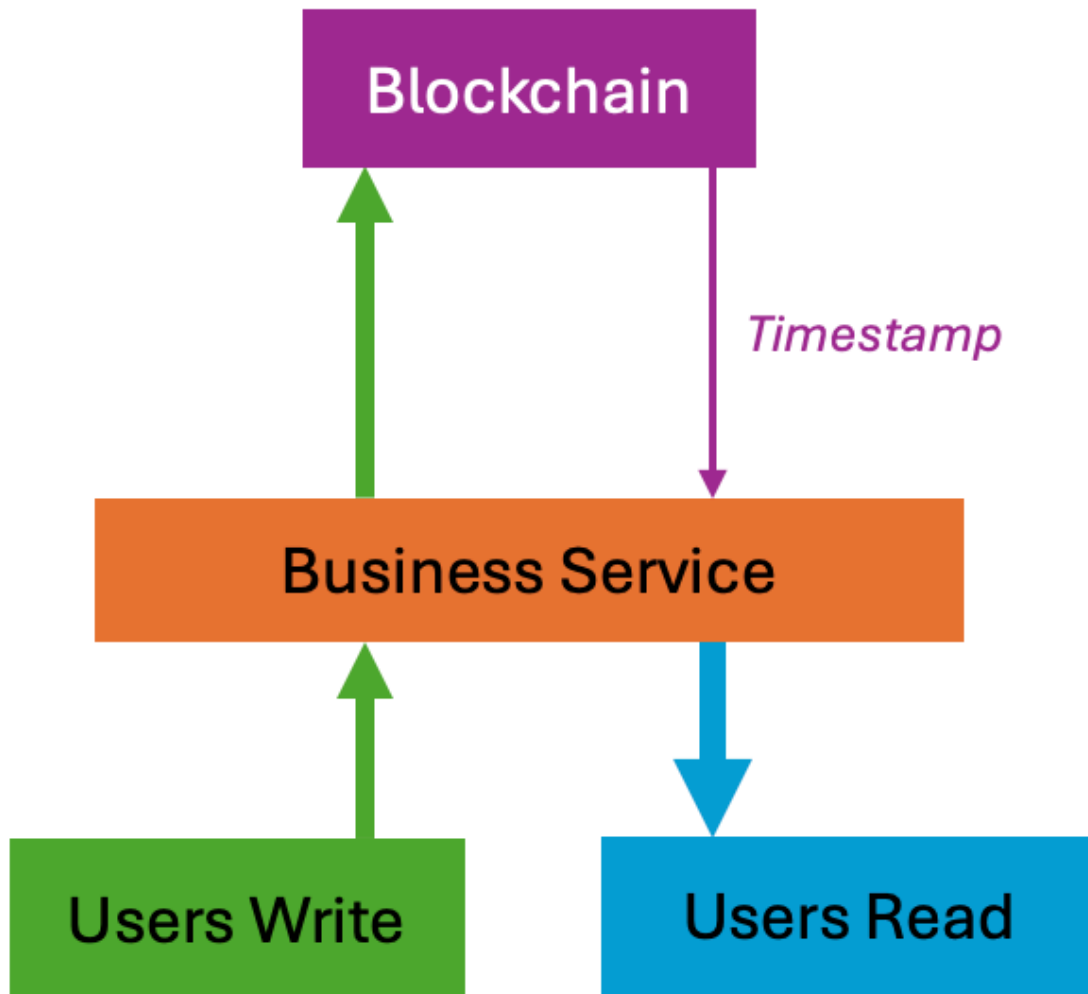
---

## 오버레이 개요(Overlays at a Glance)

글로벌 리스닝(Global Listening)은 블록체인에서 거래를 수집하여 클라이언트 애플리케이션이 인덱싱하고 읽어올 수 있도록 하는 전통적인 방식입니다.



오버레이는 다른 접근 방식을 채택합니다. 오버레이는 클라이언트로부터 수신한 거래를 SPV를 통해 검증하며, 모든 블록 데이터를 인덱싱하지 않고도 사용자가 거래 데이터를 다시 읽을 수 있도록 허용합니다.



---

## 비즈니스 맥락(Business Context)

현재 BSV 애플리케이션은 종종 블록체인에서 타임스탬프가 찍힌 불변 데이터를 읽는 데 의존합니다. 그러나 이는 단순화된 결제 검증(SPV)과 업무 분담(*division of labor*) 없이 높은 거래량에서 실행 가능하지 않습니다. 오버레이는 불변 데이터에 대한 수요를 여러 서비스에 분산시켜, 기업이 낭비를 최소화하고 필요와 비용에 따라 서비스를 선택할 수 있도록 합니다.

---

## 오버레이의 기능(Features of an Overlay)

오버레이는 SPV를 사용하여 거래를 수집하고 검증하며, 유효한 블록 헤더 체인을 유지하고, 유효한 거래를 BSV 노드 네트워크에 제출하고, 거래 전파 상태를 유지합니다. 또한 채굴된 거래에 대한 머클 경로를 획득 및 배포하며, 피어와 동기화하고, 선택적으로 UTXO 및 거래 조회 기능을 노출할 수 있습니다.

## 인프라 의존성(Infrastructure Dependencies)

오버레이는 새로운 헤더 공지를 위한 BSV 노드 네트워크, 머클 경로 계산을 위한 머클 서비스, 그리고 지갑 및 애플리케이션 내에서의 SPV 데이터 구조의 광범위한 사용에 의존합니다. 이를 통해 데이터 무결성과 네트워크 탄력성을 보장하면서 기업들에게 비용 효율적이고 확장 가능하며 안전한 솔루션을 제공합니다.

## 사용자 유형(User Types)

오버레이는 다음과 같은 다양한 사용자들을 대상으로 합니다:

- **프라이빗 오버레이(Private Overlays):** 특정 개인이나 기업을 위한 서비스
- **퍼블릭 오버레이(Public Overlays):** ARC와 같이 인프라가 없는 개발자를 위한 서비스
- **폐쇄형 오버레이(Ring Fenced Overlays):** 관할권 제한이 있는 금융 기관을 위한 서비스
- **오픈 프로토콜 오버레이(Open Protocol Overlays):** 창의적인 개발자들이 실험적 애플리케이션을 구축하기 위한 서비스

## 사용 사례(Use-Cases)

오버레이는 다양한 산업에서 폭넓은 사용 사례를 가집니다:

- 이벤트 및 항공권 발권
- 클라우드 스토리지 및 전자상거래(eCommerce)
- 중앙은행 디지털 화폐(CBDC)
- **토큰 프로토콜(Token Protocols):** STAS, Tokenized와 같은 특정 거래 유형 지원
- **지갑 제공자(Wallet Providers):** Handcash, Centbee, RockWallet 등
- **대체 가능한 토큰(FTs, Fungible Tokens):** CBDC, PIDM, 스테이블 코인 등
- **대체 불가능 토큰(NFTs, Non-Fungible Tokens):** 호텔 키, 배정된 금(gold allocation) 등
- **오픈 프레디케이트(OPs, Open Predicates):** 연산 시장(Computation Markets)
- **데이터 프레디케이트(DPs, Data Predicates):** 스토리지 시장(Storage Markets)
- **백업 서비스(Backup Services):** 거래 및 메타데이터 복구
- **탐색기(Explorers):** 개발, 영수증, 상태 확인 등을 위한 서비스

## 기술 구성 요소(Technical Components)

### 웹 API(Web API)

거래 제출 및 ID를 통한 거래 조회를 위한 엔드포인트를 노출합니다.

### 저장소(Store)

거래, UTXO, 헤더, 머클 경로, 메타데이터를 유지합니다.

### 검증기(Validator)

SPV 및 추가적인 비즈니스 로직을 실행합니다.

### 리스너(Listener)

헤더, 알림, 거래 거부를 모니터링합니다.

### 동기화기(Synchronizer)

다른 오버레이 노드와 상태를 동기화합니다.

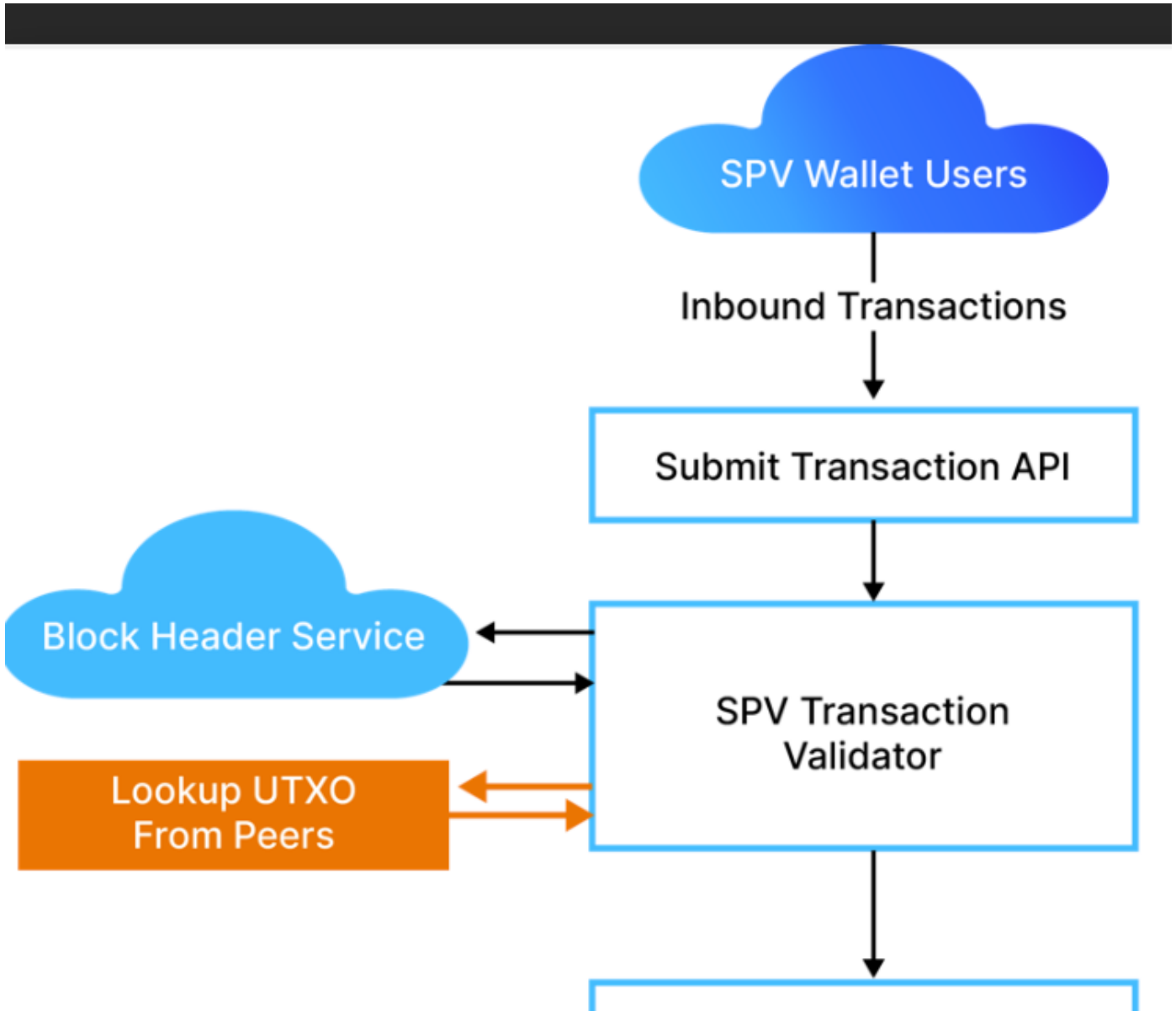
### 경로 확인기(Path Confirmer)

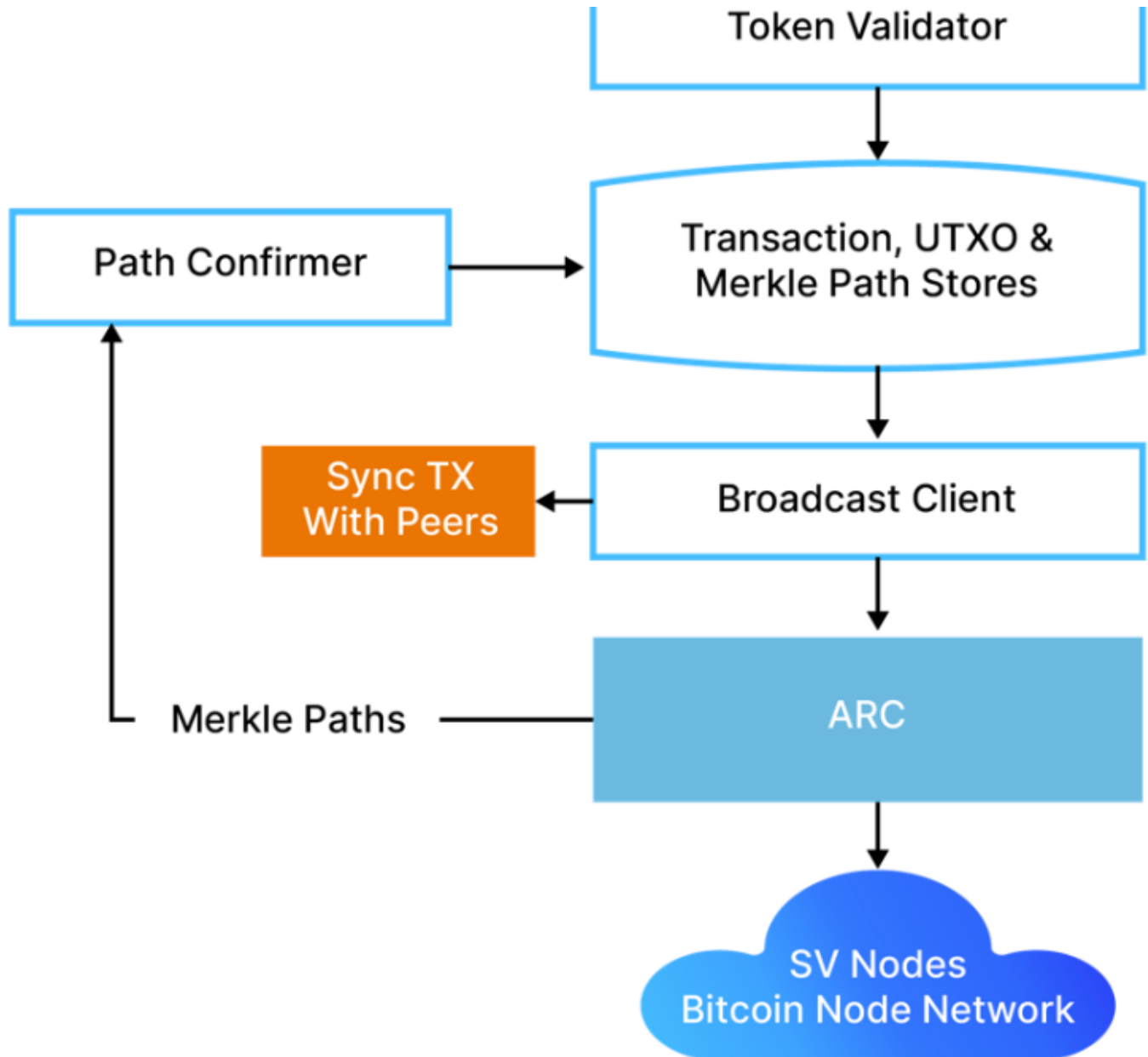
확정되지 않은 거래에 대한 머클 증명을 요청합니다.

---

## 아키텍처(Architecture)

현재의 구조는 아래와 같은 모습입니다:

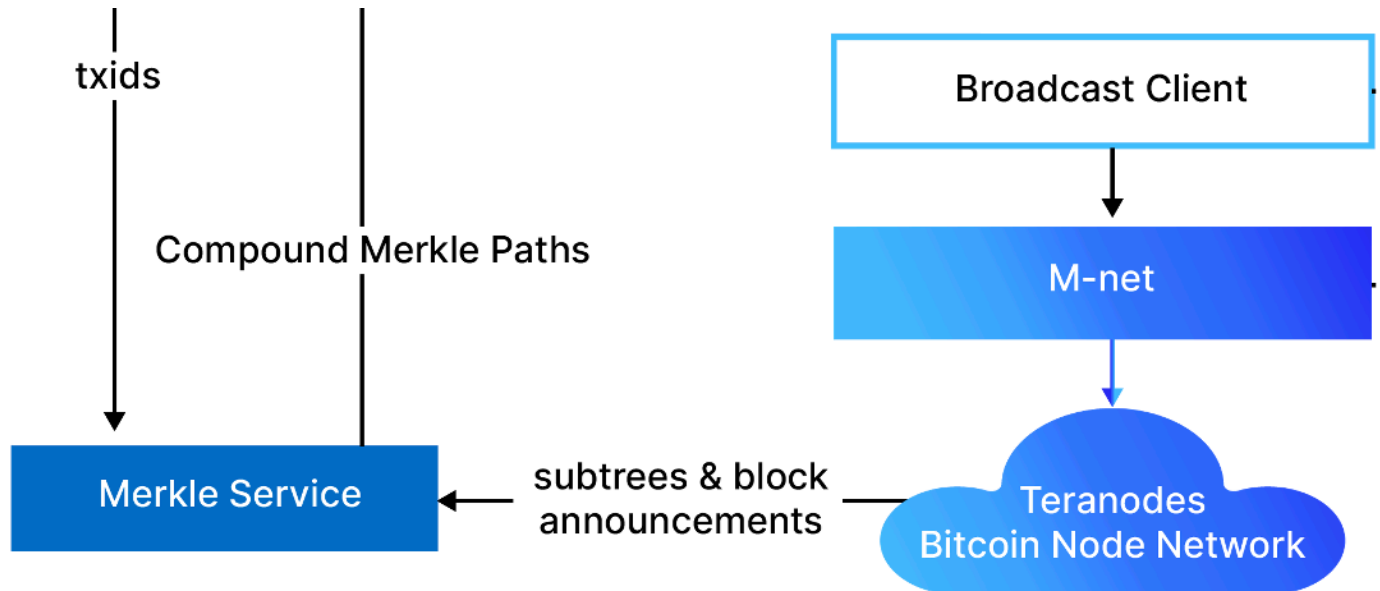




## 미래 전망(Future Outlook)

오버레이 네트워크의 미래는 확장성, 보안, 규제 준수 측면에서의 발전을 포함하며, 이를 통해 BSV는 다양한 산업을 위한 선도적인 플랫폼으로 자리매김할 것입니다.

## 기술적 변화(Technical Changes)



향후에는 ARC의 마이크로서비스 BlockTx를 대체하여 머클 경로를 계산하는 구성 요소로 확장된 머클 서비스가 도입될 것으로 예상됩니다. 이 변화는 테라노드 블록이 상당히 커질 수 있으며, BlockTx는 4GB보다 큰 블록을 처리할 수 없기 때문에 필요합니다. 테라노드는 자체 블록을 구축하는 동안 서브트리를 공지하므로, 작업은 일찍 시작될 수 있으며, 블록 발견 시 전파 과정은 특정 순간에 막대한 계산 노력이 급증하는 대신 블록 조립 과정 전체에 걸쳐 분산됩니다. 이에 대한 자세한 내용은 알파 버전이 출시될 때 공개될 예정입니다.

## SPV 지갑(SPV Wallet)

### 무엇인가?(What is it?)

- 오픈 소스 비수탁형 호스팅 지갑(Open Source Non-Custodial Hosted Wallet)
- 기존 BSV 생태계와 호환(Compatible with Existing BSV Ecosystem)
- 단순화된 결제 검증(SPV)의 참조 구현(Reference Implementation for Simplified Payment Verification)
- BSV 협회에서 유지 관리(Maintained by the BSV Association)
- 노드 운영 비용 대비 100배 저렴(100x Cheaper to run than a node)

SPV 지갑은 오픈 소스 비수탁형 호스팅 지갑으로, 기존 BSV 블록체인 생태계와 원활하게 통합됩니다. 이는 단순화된 결제 검증(SPV)의 참조 구현으로, 안전하고 효율적이며 사용자 친화적인 경험을 제공합니다.

BSV 협회에서 개발 및 유지 관리하는 SPV 지갑은 비용 효율적이고 접근성을 고려하여 설계되었습니다. 이는 풀 노드 실행 대비 100배 저렴하기 때문에, 채굴자가 아니더라도 BSV 네트워크에 참여하고자 하는 기업에 이상적인 솔루션입니다.

다음 섹션에서는 SPV의 기술적 세부 사항을 살펴보고, 작동 방식에 대해 설명하며, 지갑 설정 및 사용을 위한 단계별 지침을 제공합니다. SPV 지갑과 함께 비트코인 SV의 미래를 탐구하며, 디지털 자산을 안전하고 효율적으로 관리할 수 있는 새로운 방법을 발견해 보십시오.

## 이점(Benefits)

### 보안성(Secure)

거래는 SPV를 사용하여 즉시 검증되며, 네트워크 승인은 5초 이내에 획득되고, 채굴되자마자 포함 증명이 제공됩니다.

비수탁(non-custodial) 모델은 개인키가 광범위하게 분산된 상태로 유지되도록 하여, 공격에 대한 유인을 줄이고 사용자 자금을 보호합니다.

### 확장성(Scalable)

주소 기반 결제는 수신자가 모든 거래를 필터링하여 관련 거래를 찾아야 하며, 이는 전역 인덱싱을 요구하고 확장이 어렵다는 것이 입증되었습니다.

SPV 접근 방식은 외부 요인에 의해 확장성이 제한되지 않고, 거래 당사자들이 직접 통신할 수 있도록 함으로써 이러한 문제를 완전히 회피합니다.

### 비용 절감(Cost Savings)

{% hint style="success" %}

운영 비용은 전체 네트워크 거래량이 아니라 실제 사용량에 비례합니다. 이는 블록 헤더를 유지하고, 외부 거래를 무시하며, 머클 증명을 사용하는 방식으로 달성됩니다.

또한 BSV 협회는 오버레이 네트워크 및 테라노드로의 네트워크 토폴로지 전환을 통해 오픈 소스 소프트웨어를 적극적으로 지원할 예정입니다. 이를 통해 오픈 소스 소프트웨어를 사용하는 기업들의 유지 관리 비용이 외부화됩니다.

{% endhint %}

### 합법성(Legal)

거래 당사자 간 직접 전송을 통해 SSL 인증서, IP 주소, PKI 서명, 결제 메타데이터 등을 원하는 방식으로 얻을 수 있습니다. KYC, AML, Travel Rule 요구 사항을 고려할 때도 사용자 프라이버시를 손상시키지 않고 규제 준수가 용이합니다.

### "LiteClient" → "SPV Wallet"

LiteClient라는 용어는 종종 오해되었습니다. 전체 시스템에는 여러 구성 요소가 있으며, 단일 구성 요소를 의미하는지 전체 시스템을 의미하는지 명확하지 않았습니다. SPV Wallet은 이러한 도구 모음의 일부로, 여러 클라이언트와 서버가 함께 구성되어 있습니다.

# BSV 아카데미(BSV Academy)

## 시작하기(Getting Started)

BSV는 혁신적인 기술이며 상당히 복잡할 수 있습니다. 대부분의 사람들에게는 학습 곡선이 가파르지만, 반드시 그래야 할 필요는 없습니다. BSV 협회의 일환으로, BSV 아카데미는 교육 정보와 자료를 엄선하여 커리큘럼을 수립하였고, 이를 바탕으로 BSV 커뮤니티의 필요를 가장 잘 충족시키기 위한 교육 모듈과 과정이 개발되었습니다.

우리의 목표는 다음과 같습니다:

- 기존 자료원을 강화하고 확장한다.
- BSV를 위한 전체 인재 풀과 기술 기반을 성장시킨다.
- 입문용 BSV 블록체인 과정부터 전문가 수준의 자료까지, 모든 수준에 적합한 교육을 제공한다.
- 기업, 엔터프라이즈 및 기타 산업 참여자들이 직원을 온보딩하기 쉽게 만든다.
- 블록체인 개발 전문성을 독창적이고 자기 규율적인 직업으로 강화한다.

우리의 과정은 네 가지 주요 흐름으로 나뉩니다:

- BSV 기본(BSV Essentials)
- BSV 이론(BSV Theory)
- BSV 개발(BSV Development)
- BSV 인프라(BSV Infrastructure)

## BSV 기본(BSV Essentials)

BSV 기본 과정은 BSV를 처음 접하는 학생들에게 설계 기능, 기존 엔터프라이즈에의 적용, 그리고 시스템에서 활용되는 컴퓨터 과학 기법을 더 잘 이해할 수 있도록 돕는 세 가지 교량 과정을 포함한 입문적 관점을 제공합니다.

## BSV 기초: 프로토콜과 설계(BSV Basics: Protocol and Design)

BSV 기초: 프로토콜과 설계 과정은 학생들에게 BSV 원장(Ledger), 코인(Coins), 거래(Transactions) 및 시스템 이론 전반에 대한 상위 수준 개요를 소개합니다.

## BSV 엔터프라이즈(BSV Enterprise)

BSV 엔터프라이즈 소개 과정은 BSV 블록체인이 기존 엔터프라이즈의 많은 측면을 근본적으로 혁신할 수 있는 잠재력에 초점을 맞춥니다.

## BSV 프리미티브(BSV Primitives)

BSV 프리미티브 과정은 정식 컴퓨터 과학 배경이 없는 학생들이 BSV 블록체인에 적용된 특정 기법들을 완전히 이해할 수 있도록 돕는 교량 과정에 해당합니다. 세 가지 프리미티브 과정은 해시 함수(Hash Functions), 머클 트리(Merkle Trees), 디지털 서명(Digital Signatures)를 다룹니다.

## BSV 이론(BSV Theory)

BSV 이론 과정은 학생들이 비트코인 백서를 한 줄씩 읽고, 그 깊은 의미를 설명받으며 비트코인 시스템에 대한 철저한 이해를 갖도록 하는 것에서 시작됩니다. 이 과정은 비트코인 프로토콜을 심화 학습하기 위한 필수 선수 과정으로 간주되어야 하며, 이를 통해 모든 수강생이 비트코인 프로토콜의 기술적 선언문으로서 백서를 표준화된 방식으로 이해할 수 있도록 합니다.

## 비트코인 스크립트 소개(Introduction to Bitcoin Script)

비트코인 스크립트 소개 과정은 거래 검증 중 비트코인 가상 머신(Bitcoin VM)에서 사용되는 포스(Forth) 기반 스크립트 언어를 상세히 탐구합니다. 이 과정은 학습자들에게 언어 내 연산자(opcode)들의 기능적 그룹을 안내하며, 기본 스크립트 템플릿을 작성하는 방법과 OP\_PUSHTX 방법론과 같은 혁신적 기법을 사용하여 재귀적 동작과 유사한 동작을 시뮬레이션하는 방법을 보여줍니다.

## BSV 인프라(BSV Infrastructure)

BSV 인프라 과정은 비트코인 채굴에 참여하거나 BSV 네트워크 기능을 활용하여 정보 기술 인프라로서 사용하려는 이들에게 근본적인 기초 지식을 제공하는 BSV 인프라 소개로 시작됩니다. 이 과정은 학생들이 비트코인 프로토콜 규칙을 학습하여, 노드 클라이언트의 어떤 매개변수를 구성할 수 있고, 어떤 것은 반드시 유지해야 하는 불변의 합의 규칙인지 이해하도록 합니다. 이를 통해 소규모 세계 네트워크(small world network)의 채굴자 집합 내에서 운영할 수 있도록 합니다.

# BSV 기초: 프로토콜과 설계(BSV Basics: Protocol and Design)

## 소개(Introduction)

비트코인은 2008년 사토시 나카모토(Satoshi Nakamoto)라는 가명을 사용한 개인 혹은 그룹에 의해 만들어진 혁신적인 기술입니다. 이는 “*Bitcoin: A Peer-to-Peer Electronic Cash System*”이라는 백서를 통해 소개되었습니다. 피어-투-피어 전자 화폐 시스템은 1990년대 초반부터 탐구되었지만, 이들 시스템은 지속적으로 "이중 지불(double-spending) 문제"에 부딪혔습니다.

이중 지불이란 하나의 디지털 화폐 단위가 여러 번 소비될 위험을 의미합니다. 초기 시스템들은 거래를 모니터링하고 이중 지불을 방지하기 위해 신뢰할 수 있는 제3자에 의존했는데, 이는 탈중앙화라는 목표를 훼손했습니다. 비트코인은 중개자에 대한 신뢰를 필요로 하지 않는 혁신적인 시스템으로 이 문제를 해결했습니다. 암호학은 해결책의 중요한 구성 요소이지만, 비트코인의 진정한 혁신은 이중 지불을 방지하는 경제적 설계에 있습니다. 우리는 이 과정에서 이러한 경제적 해결책을 더 깊이 탐구할 것입니다.

전통적 회계에서는 장부(ledger)를 사용하여 자금의 지출과 수입을 추적합니다. 비트코인은 이 개념을 발전시켜 글로벌 원장을 사용해 모든 비트코인 거래 상태를 기록하고 유지합니다. 이 **비트코인 원장(Bitcoin ledger)**은 네트워크 참여자 간에 지속적으로 업데이트되고 공유되며, 모든 피어가 단일 글로벌 상태에 동의하도록 보장합니다. 우리가 비트코인 원장을 언급할 때, 이는 모든 거래의 글로벌 기록을 의미합니다.

비트코인은 또한 디지털 희소성(digital scarcity) 개념을 포함합니다. 비트코인 프로토콜 내에는 한정된 공급량의 비트코인이 존재합니다. 비트코인의 가장 작은 단위는 “사토시(satoshi)”라 불리며, 이는 비트코인 1억분의 1을 나타냅니다. 프로토콜은 총 2,100만 비트코인을 초과하여 발행되지 않도록 보장하며, 이는 비트코인을 디지털 희소 자산으로 만듭니다.

비트코인 프로토콜은 이러한 혁신적인 개념들을 도입했지만, 모든 구현체가 백서에 명시된 본래의 목적을 충실히 따르지는 않았습니다. **BSV 블록체인**은 비트코인의 원래 설계와 기능을 보존하는 유일한 구현체로, 글로벌 원장으로서 지불 및 데이터 모두에 대한 확장성과 활용성을 제공합니다.

## 비트-코인(Bit-Coin)

비트코인(Bitcoin)이라는 이름은 중요한 의미를 담고 있습니다. 인터넷에서는 데이터 패킷이 연결된 장치 간에 송수신되며 통신을 가능하게 합니다. 이와 유사하게, 비트코인이 송수신될 때 거래는 데이터 패킷으로 네트워크에 제출됩니다. 비트코인은 “비트(bit, 데이터)”와 “코인(coin, 화폐)”의 결합을 의미하며, 데이터와 함께 화폐 가치를 원활하게 전송할 수 있게 해줍니다. 이는 인터넷 인프라에서 빠져 있던 핵심 요소였습니다.

흥미롭게도, 인터넷은 이미 설계 단계에서 이 개념을 고려하고 있었습니다. HTTP 프로토콜에는 결제를 위한 예약 상태 코드(HTTP 402)가 포함되어 있었는데, 이는 적절한 디지털 현금 솔루션이 등장했을 때 사용될 예정이었습니다. 비트코인은 이 공백을 채워, 화폐 거래가 데이터 전송과 네이티브하게 통합되도록 합니다.

이 과정에서는 이러한 혁신의 기초를 제공하는 **비트코인 프로토콜(Bitcoin protocol)**을 탐구합니다. 특히, **BSV 블록체인**이 비트코인의 원래 설계를 보존하고 확장함으로써, 전 세계적 결제 및 데이터 원장으로서의 약속을 실현할 수 있는 유일한 구현체임을 중점적으로 다룰 것입니다.

이제 우리는 **비트코인 원장(Bitcoin Ledger)**을 자세히 살펴보며 비트코인을 이해하는 여정을 시작하겠습니다.

---

## BSV 원장(The BSV Ledger)

BSV 원장이 모든 BSV 거래의 글로벌 역사라는 것을 소개했으니, 이제 BSV 네트워크의 데이터베이스 요소를 더 깊이 살펴보겠습니다. BSV 원장은 네트워크 전체의 모든 거래에 대한 글로벌 기록으로 기능하며, 네트워크에 참여하는 피어들에게 공유된 신뢰 가능한 진실의 원천을 제공합니다.

여러분은 “블록체인(blockchain)”이라는 용어를 들어본 적이 있을 것입니다. 이 섹션에서는 BSV가 어떻게 회계 시스템을 혁신하는지, 그리고 BSV 블록체인이 진정으로 무엇인지를 명확히 설명할 것입니다.

## 원장(The Ledger)

앞서 소개했듯이, BSV 원장은 모든 거래의 글로벌 역사를 기록합니다. 원장이 어떻게 업데이트되는지를 이해하는 것은 매우 중요합니다. BSV 네트워크에 참여하는 노드들은 사용자가 제출한 거래를 수신하고, 유효한 거래를 원장에 기록할 책임을 집니다.

BSV 원장은 **WORM 데이터베이스(Write Once, Read Many)** 입니다. 이는 한 번 기록된 데이터는 변조 흔적 없이 변경될 수 없음을 의미합니다. 이러한 특성으로 인해 원장은 “변조 증거(tamper-evident)” 성질을 가지게 되며, 거부되거나 변경 시도가 있었던 내역은 항상 드러납니다. 시간이 지남에 따라, 경제적·계산적 비용 때문에 원장을 변경하는 것은 사실상 불가능해집니다. 매일 수백만 건의 거래가 이 원장에 추가되며, 이는 영구히 읽을 수 있습니다.

대중 매체에서는 이 원장을 흔히 “블록체인(blockchain)”이라고 부르며, 거래 묶음을 “블록(blocks)”이라 명명합니다. 이러한 블록들은 순차적으로 추가되어 연속적인 체인, 즉 블록체인을 형성합니다.

### BSV 원장의 투명성(The Transparency of the BSV Ledger)

BSV 원장의 가장 중요한 속성 중 하나는 **공개적이고 투명한 성격**입니다. 전통적인 원장은 원장 관리자의 정직성에 대한 신뢰가 필요하지만, 비트코인은 원장을 모든 참여자가 접근할 수 있도록 함으로써 이러한 필요성을 제거했습니다. 이러한 공개적 투명성은 어떤 단일 주체도 원장을 조작하거나 “장부를 조작(cook the books)”할 수 없도록 보장합니다.

앞서 설명했듯이, BSV 원장은 모든 비트코인 거래의 글로벌 역사를 기록합니다. 원장이 어떻게 업데이트되는지를 이해하는 것은 매우 중요합니다. 비트코인 네트워크에 참여하는 노드들은 사용자가 제출한 거래를 수신하고, 유효한 거래를 원장에 기록할 책임을 집니다.

그러나 이 글로벌 역사의 무결성을 보장하기 위해, 노드들은 원장을 임의로 변경할 수 없습니다. 대신, 노드들은 **유효한 거래들의 묶음(batches of valid transactions)** 을 질서 있게 원장에 기록합니다. 원장에 포함되기를 기다리는 거래들은 일시적으로 노드의 **메모리 풀(Mempool)** 에 저장됩니다. 주목할 점은, 메모리 풀은 원장과는 독립적이며, 노드들은 메모리 풀 상태에 대해 합의할 필요가 없다는 것입니다. 합의는 오직 원장에 대해서만 필요하며, 이를 통해 거래의 글로벌 상태가 일관되고 변조 불가능함이 보장됩니다.

비트코인 원장은 **WORM 데이터베이스(Write Once, Read Many)** 입니다. 이는 한 번 기록된 데이터는 변조 흔적 없이 변경될 수 없음을 의미합니다. 이러한 특성으로 인해 원장은 “변조 증거(tamper-evident)” 성질을 가지며, 거부되거나 변경 시도가 있었던 내역은 항상 드러납니다. 시간이 지남에 따라 경제적·계산적 비용 때문에 원장을 변경하는 것은 사실상 불가능해집니다. 매일 수백만 건의 거래가 이 원장에 추가되며, 이는 영구히 읽을 수 있습니다.

대중 매체에서는 비트코인 원장을 흔히 “블록체인(blockchain)”이라 부르며, 거래 묶음을 “블록(blocks)”이라 명명합니다. 이러한 블록들은 순차적으로 추가되어 연속적인 체인, 즉 블록체인을 형성합니다.

### BSV 원장의 투명성(The Transparency of the BSV Ledger)

BSV 원장의 가장 중요한 속성 중 하나는 **공개적이고 투명한 성격**입니다. 전통적인 원장은 원장 관리자의 정직성에 대한 신뢰가 필요하지만, 비트코인은 원장을 모든 참여자가 접근할 수 있도록 함으로써 이러한 필요성을 제거했습니다. 이러한 공개적 투명성은 어떤 단일 주체도 원장을 조작하거나 “장부를 조작(cook the books)”할 수 없도록 보장합니다.

**BSV 블록체인**은 이러한 투명성을 보존하면서도 무한히 확장할 수 있으며, 저렴한 수수료와 뛰어난 효율성으로 하루에 수백만 건의 거래를 처리할 수 있도록 합니다. 다른 블록체인 구현체들이 비트코인의 원래 설계에서 벗어난 반면, BSV는 결제와 데이터 모두를 위한 글로벌 원장이라는 본래 목적을 충실히 따릅니다.

### 삼중 장부 회계(Triple Entry Accounting)

비트코인은 혁신적인 개념을 도입했습니다. 모든 거래가 디지털 서명되며, 이는 새로운 회계 모델에서 세 번째 항목으로 기능하는 **공개 영수증(public receipt)**을 생성합니다. 이 영수증은 **BSV 원장**에 기록되어, 누구나 거래의 존재 여부를 검증할 수 있게 합니다. 이러한 투명성과 검증 가능성은 금융 기록의 신뢰성을 근본적으로 향상시킵니다.

BSV 원장은 금전적 거래를 위한 글로벌 데이터베이스로 작동합니다. 역사적으로 회계 장부가 경제 활동을 기록해온 것처럼, BSV 원장은 밥이 앨리스에게 지불했고, 앨리스가 짐에게 지불했다는 사실을 증명하는 글로벌 공개 기록을 제공합니다.

BSV 원장은 단순한 금전적 교환을 넘어 광범위한 의미를 가집니다. 앞서 언급했듯이, 거래에는 데이터 요소도 포함됩니다. 예를 들어, 밥이 앨리스에게 3코인을 지불한다면, 이 거래는 원장에서 단지 1킬로바이트(KB)의 데이터만을 필요로 할 수 있습니다.

BSV는 더 복잡한 거래도 지원합니다. 예를 들어:

- 밥이 앨리스와 짐에게 각각 1코인을 지불하는 거래는 약 1.1KB의 데이터를 사용할 수 있습니다.
- 수천 명의 수신자가 있는 거래는 약 3KB가 필요할 수 있습니다.

이러한 유연성은 BSV를 **글로벌 데이터 원장(Global Data Ledger)**으로 변모시킵니다. 이는 언제든지 원하는 양의 데이터를 기록할 수 있는 **WORM(Write Once, Read Many) 데이터베이스**이며, 불변성 속성을 통해 데이터 무결성을 검증할 수 있는 신뢰할 수 있는 방법을 제공합니다.

2005년, 이안 그리그(Ian Grigg)는 디지털 서명이 전통적인 이중 장부 회계(double-entry accounting)를 어떻게 향상시킬 수 있는지를 설명하기 위해 "삼중 장부 회계(Triple Entry Accounting)"라는 용어를 만들었습니다. 전통적인 회계에서는 한 장부에 차변(debit)이 기록되고, 다른 장부에 대변(credit)이 기록되어 거래를 반영합니다. 그러나 이 방식은 차변과 대변이 일치하지 않을 경우 감사 과정에서 실패할 수 있습니다.

비트코인은 혁신적인 개선을 도입했습니다. 모든 거래는 디지털 서명되며, 이는 새로운 회계 모델에서 세 번째 항목으로 기능하는 **공개 영수증(public receipt)**을 생성합니다. 이 영수증은 **비트코인 원장(Bitcoin Ledger)**에 기록되어, 누구나 거래의 존재 여부를 검증할 수 있습니다. 이러한 투명성과 검증 가능성은 금융 기록의 신뢰성을 근본적으로 향상시킵니다.

비트코인 원장은 금전적 거래를 위한 글로벌 데이터베이스로 작동합니다. 역사적으로 회계 장부가 경제 활동을 기록해온 것처럼, 비트코인 원장은 밥이 앨리스에게 지불했고, 앨리스가 짐에게 지불했다는 사실을 증명하는 글로벌 공개 기록을 제공합니다.

## 화폐 거래를 넘어(Beyond Monetary Transactions)

BSV 원장은 단순한 화폐 교환을 넘어서는 광범위한 의미를 가집니다. 앞서 언급했듯이, BSV 거래에는 데이터 요소가 포함됩니다. 예를 들어, 밥이 앨리스에게 3비트코인을 지불한다면, 이 거래는 원장에서 단지 1킬로바이트(KB)의 데이터만을 필요로 할 수 있습니다.

BSV는 또한 더 복잡한 거래를 지원합니다. 예를 들어:

- 밥이 앨리스와 짐에게 각각 1 BSV를 지불하는 거래는 약 1.1KB의 데이터를 사용할 수 있습니다.
- 수천 명의 수신자가 있는 거래는 약 3KB가 필요할 수 있습니다.

여기서 중요한 점은, **거래가 포함할 수 있는 데이터의 양에 고정된 한도가 없다는 것**입니다. 유일한 제약 조건은 해당 거래를 처리하는 노드가 정하는 경제적 실행 가능성입니다.

이러한 유연성은 BSV를 **글로벌 데이터 원장(Global Data Ledger)**으로 변모시킵니다. 이는 언제든지 원하는 양의 데이터를 기록할 수 있는 **WORM(Write Once, Read Many) 데이터베이스**이며, 불변성 속성을 통해 데이터 무결성을 검증할 수 있는 신뢰할 수 있는 방법을 제공합니다.

---

## 코인과 거래(Coins and Transactions)

BSV 원장이 거래의 역사를 보유하고 있지만, BSV에서 거래란 무엇인지 더 깊이 살펴보는 것이 중요합니다. 코인은 개인 간에 피어 투 피어(P2P) 방식으로 이전되며, 코인의 공급량은 고정되어 있습니다.

BSV에서는 고정된 코인 공급량이 채굴(mining)이라는 과정을 통해 시스템에 도입됩니다. 이 섹션에서는 코인이 어떻게 발행(minting)되고, 소유자 간에 어떻게 이전되는지를 다룰 것입니다.

BSV 원장이 거래의 역사를 보유하고 있지만, BSV에서 거래란 무엇인지 더 깊이 살펴보는 것이 중요합니다. 코인은 개인 간에 피어 투 피어 방식으로 이전되며, 코인의 공급량은 고정되어 있습니다.

BSV에서는 고정된 코인 공급량이 채굴이라는 과정을 통해 시스템에 도입됩니다. 이 섹션에서는 코인이 어떻게 발행되고, 소유자 간에 어떻게 이전되는지를 다룰 것입니다.

## 코인(Coins)

거래 묶음이 블록으로 번들링되면, 해당 블록은 “채굴(mined)”된 것으로 간주되어 블록체인에 추가됩니다. 블록을 채굴하면 **블록 보조금(block subsidy)**이라 불리는 고정된 수의 코인이 발행되며, 이는 블록을 성공적으로 채굴한 노드에 보상으로 지급됩니다. 이 보조금은 시간이 지남에 따라 감소하며, 약 4년마다 절반으로 줄어듭니다. 현재 블록 보조금은 **블록당 3.125코인**으로 고정되어 있습니다.

사토시 나카모토가 비트코인 네트워크를 출시했을 때, 그는 총 **2,100만 코인**의 고정 공급량을 설계했으며, 각 코인은 **1억 단위**인 사토시(satoshi)로 분할될 수 있도록 했습니다. 사토시는 BSV의 가장 작은 단위이며, 전송 가능한 최소 금액을 나타냅니다.

네트워크 출시 시점에 2,100조( $21,000,000 \times 100,000,000$ ) 사토시가 발행되었지만, 사토시는 **블록 보조금**이라는 점진적 분배 메커니즘을 통해 경제에 점차적으로 도입되었습니다.

## 블록 보조금과 채굴(The Block Subsidy and Mining)

거래 묶음이 블록으로 번들링되면, 해당 블록은 “채굴”된 것으로 간주되어 블록체인에 추가됩니다. 블록을 채굴하면 **블록 보조금**이라 불리는 고정된 수의 코인이 발행되며, 이는 블록을 성공적으로 채굴한 노드에 보상으로 지급됩니다. 이 보조금은 시간이 지남에 따라 감소하며, 약 4년마다 절반으로 줄어듭니다. 현재 블록 보조금은 **블록당 3.125코인**입니다.

모든 코인이 제네시스에서 발행되었지만, 채굴 과정을 통해 이들이 점차적으로 경제에 유입됩니다. 이러한 설계는 네트워크를 부트스트랩하는 데 필수적이었으며, 블록 보조금은 노드들이 채굴에 참여하고 원장을 유지하도록 장려하는 인센티브 역할을 했습니다.

## 채굴이 작동하는 방식(How Mining Works)

채굴은 노드들이 유효한 거래 묶음(블록)을 원장에 추가하기 위해 경쟁하는 과정입니다. 블록을 성공적으로 채굴한 노드는 블록 보조금(block subsidy)으로 보상을 받습니다. 그러나 이 보상은 쉽게 얻을 수 있는 것이 아닙니다. 노드들은 **해시 퍼즐(hash puzzle)**이라 불리는 복잡한 수학적 문제를 해결하기 위해 경쟁해야 합니다.

이 퍼즐을 푸는 과정을 복권에 비유할 수 있습니다:

- 각 잠재적 해답은 긁는 복권(scratch-off lottery ticket)과 같습니다.
- 가장 많은 복권을 가장 빠르게 생성하고 긁어낸 노드가 당첨 해답을 찾을 가능성이 높습니다.
- 이 과정은 **해싱(Hashing)**이라 불리며, 노드가 암호학적 해시 함수를 반복적으로 적용하여 유효한 해답을 발견할 때까지 수행됩니다.

공정성과 일관된 블록 생성을 보장하기 위해, 사토시는 **난이도 조정 알고리즘(Difficulty Adjustment Algorithm)**을 도입했습니다. 이 알고리즘은 네트워크의 총 연산력에 따라 해시 퍼즐의 난이도를 매 2016블록(약 2주마다)마다 높이거나 낮춥니다.

---

## 난이도 조정의 중요성(Why the Difficulty Adjustment is Important)

난이도 조정 알고리즘은 두 가지 중요한 목적을 수행합니다:

### 1. 자원 기여와 보안(Resource Contribution and Security):

더 많은 노드가 네트워크에 참여할수록 퍼즐은 더 어려워져 더 큰 계산 자원이 필요합니다. 이는 상당한 자원을 투자한 노드만이 경쟁력을 유지할 수 있도록 하며, 경제적 인센티브를 네트워크 보안과 일치시킵니다.

### 2. 예측 가능한 블록 생성 시간(Predictable Block Times):

이 알고리즘은 블록 생성 주기를 평균 **10분** 간격으로 유지하도록 설계되었습니다. 이 예측 가능한 속도는 원장이 시간이 지남에 따라 꾸준히 성장하도록 보장합니다. 10분 간격의 장점은 이 과정의 범위를 벗어나지만, 이 설계가 원장 업데이트의 일관성과 신뢰성을 유지한다는 점을 이해하는 것이 중요합니다.

## BSV 블록체인의 장점(The BSV Blockchain Advantage)

**BSV 블록체인**은 사토시의 원래 경제적 설계를 보존하면서, 다른 구현체들이 달성할 수 없는 확장성을 제공합니다. 무제한 블록 크기를 지원함으로써, BSV 블록체인은 보안이나 효율성을 훼손하지 않고도 하루에 수백만 건의 거래를 처리할 수 있으며, 채굴이 경제적으로 실행 가능하고 확장 가능하게 유지되도록 합니다.

고정된 코인 공급량, 경쟁적인 채굴, 확장 가능한 인프라의 결합은 BSV 블록체인이 비트코인의 원래 비전을 글로벌 결제 및 데이터 네트워크로서 실현할 수 있는 독보적인 능력을 갖추게 합니다.

---

## 거래(Transactions)

**BSV 블록체인**은 근본적으로 디지털 현금 시스템이므로, 코인이 한 사람에서 다른 사람으로 어떻게 이전되는지를 이해하는 것이 시스템을 이해하는 데 매우 중요합니다. 궁극적으로 코인은 소유자에서 소유자로 여러 가지 방식으로 이전될 수 있습니다. BSV 블록체인은 **비트코인 스크립트(Bitcoin Script)** 라는 복잡한 스크립트 시스템을 구현하여 코인을 복잡하고 혁신적인 방식으로 이동시킬 수 있습니다.

이 스크립트 시스템의 특성은 본 과정의 범위를 벗어나지만, 우리는 코인을 전송할 수 있는 가장 단순한 방법에 초점을 맞출 것입니다. 그것은 바로 공개키와 개인키 쌍을 사용하는 방식입니다.

비트코인 백서에 나온 이미지를 활용하면, 코인이 어떻게 이전되는지 다음과 같은 비유로 설명할 수 있습니다:

- **소유자 1**이 코인을 **소유자 2**에게 보내고 싶다면, 소유자 2의 공개키(사용자명과 유사)를 확보하고, 소유자 1의 공개키와 연결된 개인키(비밀번호와 유사)를 사용해 전송을 승인합니다.
- 코인이 소유자 2에게 이전되면, 오직 소유자 2만이 자신의 개인키를 사용하여 동일한 코인을 다른 사람에게 전송할 수 있습니다.

아직 **BSV 블록체인**에 기록되지 않은 모든 거래는 노드에 의해 수집되어 다음 블록에 포함됩니다. 그림에서 보듯, 코인은 소유자에서 소유자로 추적이 가능합니다. 그러나 프라이버시를 보호하기 위해, 소유자는 공개키 재사용을 피하는 것이 권장됩니다.

**BSV 블록체인**은 근본적으로 디지털 현금 시스템이므로, 코인이 한 사람에서 다른 사람으로 어떻게 이전되는지를 이해하는 것이 시스템을 이해하는 데 매우 중요합니다. 궁극적으로 코인은 소유자에서 소유자로 다양한 방식으로 이전될 수 있습니다. BSV 블록체인은 **비트코인 스크립트(Bitcoin Script)** 라는 복잡한 스크립트 시스템을 구현하여 코인을 복잡하고 혁신적인 방식으로 이동시킬 수 있습니다. 그러나 이 스크립트 시스템의 특성은 본 과정의 범위를 벗어나므로, 우리는 코인을 전송할 수 있는 가장 단순한 방법에 초점을 맞출 것입니다. 바로 공개키와 개인키 쌍을 사용하는 방식입니다.



단순한 디지털 현금 결제의 경우, 수수료는 낮게 유지될 것으로 예상되며, 높은 수수료는 마이크로페이먼트를 가능하게 하는 디지털 현금 시스템으로서의 비트코인의 효용을 훼손하게 될 것입니다. 블록 보조금을 효과적으로 대체하기 위해 가능한 두 가지 시나리오는 다음과 같습니다:

1. 높은 수수료와 낮은 거래량이 결합된 경우
2. 낮은 수수료와 높은 거래량이 결합된 경우

첫 번째 시나리오는 비트코인을 디지털 현금 솔루션으로서 비현실적으로 만들지만, 두 번째 시나리오는 확장을 통해 달성될 수 있으며, 네트워크가 낮은 수수료로 대량의 거래를 효율적으로 처리할 수 있도록 합니다.

BSV 블록체인은 무한한 확장성을 통해 이러한 저수수료, 고거래량 모델을 가능하게 합니다. 코카콜라가 단위당 적은 이윤으로 엄청난 양의 제품을 판매하여 수익을 창출하는 것처럼, BSV 블록체인의 채굴자들은 거래당 작은 수수료를 받으며 막대한 수의 거래를 처리하도록 인센티브를 가집니다. 이 접근 방식은 블록 보조금이 사라지더라도 수익성을 보장합니다.

효율적인 하드웨어, 혁신적인 소프트웨어, 강력한 인프라에 투자하는 채굴자들은 이 확장 가능한 생태계에서 번성할 것으로 예상되며, BSV 블록체인의 높은 처리량과 경제적 효율성으로부터 보상을 얻게 될 것입니다.

## 이론(Theory)

이제 비트코인의 기초를 다뤘으니, 원래의 비트코인 백서를 살펴보고 쉽게 이해할 수 있습니다.

비트코인 백서는 총 12개의 섹션으로 나누어져 있으며, 참고 문헌을 포함해 9페이지에 불과합니다. 짧지만 백서는 방대한 정보를 담고 있습니다. 여기서는 섹션들을 간략히 다루지만, BSV 이론 과정에서는 이 주제들을 훨씬 더 깊이 탐구합니다.

## 소개(Introduction)

비트코인은 디지털 현금 결제를 위한 이중 지불 문제의 해결책으로 제시되었습니다. 첫 번째 섹션에서는 직접적으로 이렇게 말합니다:

“필요한 것은 신뢰 대신 암호학적 증거에 기반한 전자 결제 시스템으로, 제3자에 대한 신뢰 없이 두 당사자가 직접 거래할 수 있는 시스템이다.”

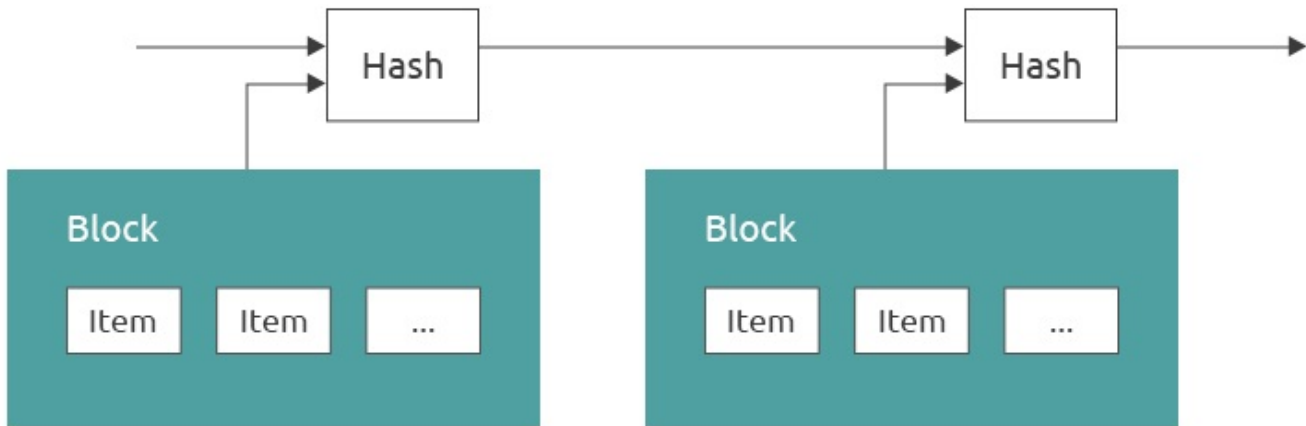
각 섹션은 제안된 해결책을 점진적으로 소개합니다.

## 거래(Transactions)

코인은 디지털 서명의 체인으로 정의됩니다. 코인은 디지털 서명을 사용하여 한 소유자에서 다른 소유자로 이전됩니다. 거래가 유효한지 확인하는 유일한 방법은 이중 지불 문제를 해결하는 것입니다. 여기서 해결책의 실마리가 주어집니다: 거래는 공개적으로 발표됩니다. 우리는 비트코인의 핵심 혁신 중 하나가 시스템의 공개적 성격임을 알 수 있습니다.

## 타임스탬프 서버(Timestamp Server)

제안된 해결책은 타임스탬프 서버의 사용을 필요로 합니다. 이미 “블록”이 무엇인지 다뤘습니다. 블록은 원장에 기록되는 거래 묶음입니다. 각 블록의 해시는 계산되어 네트워크에 공개적으로 발표되며, 이는 타임스탬프 서버 역할을 합니다. 해시는 데이터 무결성을 보장하며, 네트워크 전체에 이 소량의 데이터를 공개함으로써 모든 노드가 공통 원장에 합의할 수 있도록 합니다.



### 작업증명(Proof of Work)

앞서 논의했던 복잡한 “채굴(mining)” 과정의 이름을 여기서 배우게 됩니다. 작업증명(Proof-of-Work, PoW)은 블록을 찾는 과정에서 블록 보상과 거래 수수료를 얻기 위해 노드들이 경쟁하도록 만드는 시스템입니다.

여기서 BSV의 중요한 철학이 소개됩니다: **의사결정은 CPU 파워에 의해 이루어진다**는 점입니다. 네트워크에서 노드들은 IP 주소의 다수가 아니라, 컴퓨팅 파워의 다수로 표현됩니다. 이는 BSV의 경제적 기반을 확고히 합니다. 즉, 노드 인프라와 하드웨어에 대한 투자가 해당 노드에게 네트워크 내 다른 노드들에 비해 경쟁적 우위를 부여합니다. 이러한 노드들은 네트워크에 이해관계를 가지기 때문에, 네트워크에 거의 투자하지 않은 공격자가 이를 방해하기는 어렵습니다.

### 네트워크(Network)

노드는 BSV 블록체인에서 블록 생성에 참여하는 존재로 명확히 정의됩니다. 오직 여섯 가지 필수 단계를 모두 수행하는 엔터티만이 네트워크를 운영하는 노드로 간주됩니다. 이 단계는 다음과 같습니다:

1. **거래 검증(Validating Transactions)** – 노드는 합의 규칙에 따라 거래를 검증하여 이중 지불 방지와 스크립트 조건 준수 등 프로토콜을 따르도록 보장합니다.
2. **거래 전파(Propagating Transactions)** – 유효한 거래는 다른 노드로 브로드캐스트되어 블록에 포함될 수 있도록 합니다.
3. **거래를 블록으로 조립(Assembling Transactions into Blocks)** – 노드는 메모리 풀에서 유효한 거래를 모아 자신이 설정한 블록 크기 정책에 맞는 블록을 구성합니다.
4. **작업증명 퍼즐 해결(Solving Proof of Work Puzzles)** – 노드들은 계산 퍼즐(해시 연산)을 해결하기 위해 경쟁하며, 이는 다음 블록을 추가할 권리를 결정합니다.
5. **블록 전파(Propagating Blocks)** – 블록이 성공적으로 채굴되면 네트워크에 브로드캐스트되어 다른 노드들이 이를 검증할 수 있도록 합니다.
6. **블록체인 상태 유지(Maintaining the Blockchain State)** – 노드들은 전체 블록체인 기록을

유지하며, 가장 긴 유효 체인이 올바른 상태로 일관되게 채택되도록 보장합니다.

네트워크 내 모든 노드는 이러한 단계들을 규율하는 명확히 정의된 규칙을 따라야 합니다. 만약 BSV 블록체인의 상태에 대한 불일치가 발생하면, 노드들은 나카모토 합의(Nakamoto Consensus)를 통해 이를 해결합니다. 이 충돌 해결 메커니즘은 가장 많은 작업증명이 누적된 가장 긴 유효 체인이 블록체인의 권위 있는 버전으로 받아들여지도록 보장합니다.

## 인센티브(Incentive)

여기서 우리는 블록 보조금(block subsidy)과 코인이 시스템에서 어떻게 분배되는지를 배웁니다. 이 지점에서 처음으로 채굴(mining)에 대한 비유가 언급됩니다. 또한 사토시의 비전이 소개되는데, 블록 보조금이 줄어들고 2,100만 코인이 모두 분배된 후 시스템이 어떻게 유지될 수 있는가에 대한 설명입니다. 인센티브는 전적으로 거래 수수료로 전환되며, 시스템은 완전히 인플레이션이 없는 구조가 됩니다. 사토시는 또한 노드가 정직하게 남아 있을 유인에 대해 설명합니다. 그는 노드가 시스템을 공격하는 것보다 정직하게 새로운 코인을 생성하는 것이 더 수익성이 높다고 주장합니다.

## 디스크 공간 회수(Reclaiming Disk Space)

사토시는 끊임없이 커지는 블록체인에 대응하기 위해 노드가 디스크 공간을 회수할 수 있는 지침을 제시합니다. 그는 블록체인에서 충분히 오래된 소비된 거래들은 삭제될 수 있으며, 노드는 단순히 해시만 유지하여 시스템의 무결성을 보존할 수 있다고 말합니다. 그는 블록체인 저장은 우려할 필요가 없다는 증거로 무어의 법칙(Moore's Law)을 인용합니다.

## 단순화된 결제 검증(Simplified Payment Verification)

여기서 우리는 사용자가 네트워크에서 노드를 운영하지 않고도 결제를 위해 시스템과 상호작용할 수 있는 방법을 배웁니다. 이 시스템은 단순화된 결제 검증(Simplified Payment Verification, SPV)이라 불리며, 사용자가 섹션 5에서 언급된 노드 운영에 필요한 단계나 블록체인의 전체 복사본을 보관하지 않고도 블록체인과 상호작용할 수 있는 방법을 설명합니다. 이들은 오직 블록 헤더 체인에만 의존합니다.

## 가치의 결합과 분할(Combining and Splitting Value)

여기서는 코인이 여러 입력과 출력을 사용하는 거래를 통해 전송될 수 있으며, 이를 통해 코인이 현금이 전송되는 방식과 유사하게 이전될 수 있음을 배웁니다.

## 프라이버시(Privacy)

사토시는 신원이 시스템에서 방화벽으로 차단되며, 공개키를 재사용하지 않음으로써 프라이버시가 유지될 수 있다고 설명합니다. 그러나 그는 분명히 BSV는 익명 시스템이 아니라 가명(pseudonymous) 시스템임을 밝힙니다. BSV 블록체인은 공개적이고 추적 가능하기 때문에, 결국 거래들 간에 연결(linking)이 발생할 수밖에 없습니다.

## 계산(Calculations)

여기서 사토시는 네트워크의 대다수가 정직한 노드에 의해 통제되는 한 네트워크를 공격하는 것이 매우 어렵다는 것을 보이기 위해 많은 수학적 계산을 전개합니다.

## 결론(Conclusion)

여기서는 결론을 한 글자도 바꾸지 않고 그대로 인용할 것입니다. 결론은 전체 시스템을 매우 간결하게 요약하고 있으며, 이 과정을 통해 준비된 여러분은 이를 명확하게 따라갈 수 있을 것입니다:

“우리는 신뢰에 의존하지 않는 전자 거래 시스템을 제안했습니다. 우리는 디지털 서명으로 구성된 코인의 일반적인 틀에서 출발했는데, 이는 소유권에 대한 강력한 통제를 제공하지만, 이중 지불을 방지하는 방법이 없으면 불완전합니다. 이를 해결하기 위해, 우리는 작업증명(proof-of-work)을 사용하는 피어 투 피어 네트워크를 제안하여 거래의 공개 기록을 남기도록 했으며, 정직한 노드가 CPU 파워의 과반을 통제할 경우 공격자가 이를 변경하는 것이 신속히 계산적으로 비현실적이 되도록 했습니다. 이 네트워크는 비구조적 단순성 속에서 견고합니다. 노드들은 거의 조정 없이 동시에 작동합니다. 메시지가 특정한 곳으로 라우팅되지 않고 최선의 노력(best effort) 기반으로만 전달되면 되므로, 노드들은 신원을 식별할 필요가 없습니다. 노드들은 원할 때 네트워크를 떠났다 다시 합류할 수 있으며, 부재 중에 무슨 일이 일어났는지에 대한 증거로 작업증명 체인을 받아들입니다. 노드들은 CPU 파워로 투표하며, 유효한 블록을 확장하는 작업을 수행함으로써 그 수용 의사를 표현하고, 유효하지 않은 블록에 대해 작업을 거부함으로써 이를 거부합니다. 필요한 모든 규칙과 인센티브는 이 합의 메커니즘으로 집행될 수 있습니다.”

## 결론(Conclusion)

BSV 이론 과정은 백서의 다양한 구성 요소와 자료를 완전히 이해하는 데 필요한 여러 학문 영역을 훨씬 더 깊이 탐구합니다.

우리의 BSV 프리미티브(BSV Primitives) 시리즈는 BSV에서 활용되는 세 가지 컴퓨터 과학의 기본 기술(해시 함수, 머클 트리, 디지털 서명)을 다루며, 이 분야 외부의 사람들도 시스템을 보다 깊이 이해할 수 있도록 돕습니다.

이 과정은 여러분에게 비트코인 프로토콜과 BSV 블록체인의 기초를 소개했지만, 배울 것은 훨씬 더 많습니다! 우리는 여러분이 아카데미에 존재하는 다른 많은 과정들로 학습을 이어가기를 권장합니다.

BSV 이론 과정은 백서의 다양한 구성 요소와 자료를 완전히 이해하는 데 필요한 여러 학문 영역을 훨씬 더 깊이 탐구합니다.

우리의 BSV 프리미티브(BSV Primitives) 시리즈는 BSV에서 활용되는 세 가지 컴퓨터 과학의 기본 기술(해시 함수, 머클 트리, 디지털 서명)을 다루며, 이 분야 외부의 사람들도 시스템을 보다 깊이 이해할 수 있도록 돕습니다.

---

## BSV 엔터프라이즈(BSV Enterprise)

이 과정은 기업가들을 대상으로 하며, 학생들은 BSV 엔터프라이즈 블록체인을 차세대 플랫폼을 구축하기 위한 기반으로 활용하는 방법을 배우게 됩니다. BSV 네트워크가 디지털 서비스 제공 방식을 근본적으로 어떻게 변화시킬 수 있는지를 학습합니다.

## 소개(Introduction)

이 과정은 C-레벨 임원들을 대상으로 하며, BSV를 기술 기반으로 활용하여 차세대 플랫폼을 구축하려는 이들을 위해 설계되었습니다. 이 과정의 목적은 다음과 같은 질문들에 대한 답을 제공하는 것입니다:

- BSV와 암호화폐는 무엇이 다른가?
- 블록이란 무엇인가?
- 거래란 무엇인가?
- 블록체인과 거래 원장의 분리란 무엇인가?
- 작동하는 블록체인 – 가지치기(Pruning) vs SPV와 블록 연계 데이터베이스
- 왜 프로토콜은 고정되어야 하는가?
- ‘프라이빗 블록체인’이란 무엇인가?
- 왜 작업증명(Proof of Work)이 지분증명/권위증명(Proof of Stake/Authority)보다 우월한가?
- 왜 작업증명은 BTC에서는 비효율적이지만 BSV에서는 효율적이며, 확장될수록 더 효율적인가?
- BSV 블록체인을 활용하기 시작하려면 무엇을 이해해야 하는가?

지난 수십 년 동안 정보 기술, 결제 서비스, 금융 분야에서 일어난 급격한 변화를 되돌아보면, 과거 종이에 의해 지배되던 시스템들이 점점 디지털화되는 패턴을 쉽게 확인할 수 있습니다.

편지에서 이메일로, 수표에서 EFTPOS로, 서명에서 디지털 서명으로, 인쇄된 종이에서 디지털 파일로의 변화처럼, 물이 스펀지에 스며들 듯 디지털 기술은 우리가 개인적·비즈니스 관계를 관리하는 모든 도구에 스며들었습니다.

비트코인이 지난 10여 년 동안 등장하면서, 디지털 금융 및 데이터 활동에서 중개자를 더 줄이는 기술 계층으로서의 가능성에 대한 많은 기대가 있었습니다. 네트워크의 성공은 각 기업이나 기관이 개별적으로 보관하고 주기적으로 막대한 노력과 비용을 들여 조정하던 원장 시스템에서, 제3자 노드의 글로벌 네트워크가 모든 비즈니스 활동을 단일 원장으로 관리하는 새로운 패러다임으로의 전환을 의미합니다. 원장의 규모와 효율성은 거래 비용을 지금까지 본 적 없는 수준으로 줄일 수 있으며, 완전히 개별화된 서비스에 대해 극소액 단위로 별도의 결제를 받을 수 있는 방식을 제공합니다. 원장을 올바르게 사용하면 삼중 장부 회계(triple entry accounting)를 가능하게 하여, 거래 당사자 모두가 참조할 수 있는 단일 기록을 남기고 초 단위로 동기화된 단일 클릭 감사 시스템을 구축할 수 있습니다.

블록체인/디지털 화폐 환경에서 BTC의 대안을 살펴보면, 공공 원장을 관리하기 위해 개발된 다양한 시스템을 구분하는 것이 어려울 수 있으며, 어떤 프로젝트가 기업과 정부의 개방적이고 무제한적인 사용으로 인해 발생할 수 있는 활동 수준을 관리할 수 있는지 판별하기도 어렵습니다.

동시에, 일부 프로젝트는 단지 초기 내부자 집단이 무규제 시장에서 순진한 개인 투자자들을 상대로 가짜 기술(vapourware)을 과대 홍보하여 부를 축적하려는 잘 포장된 계획에 불과하다는 것도 쉽게 알 수 있습니다.

BSV는 비트코인 설계의 제1원칙(first principles)을 따르며, 고성능·신뢰성·저비용의 공공 네트워크 및 원장으로 기능합니다. 프로토콜은 무제한적이며, 이를 통해 전 세계적으로 고속·저비용의 금융, 통신, 데이터, 기술 서비스를 제공할 수 있는 기회를 제공합니다.

BSV 블록체인은 부유층이나 초기 참여자만 사용할 수 있는 배타적인 시스템이 아니라, 모든 사람이 통신, 교육, 상업의 기반(backbone)으로 사용할 수 있는 범용 네트워크이자 원장입니다. BSV는 BSV 원장을 관리하는 네트워크 구현체로서, '투자'라는 순수 투기적 산업 내러티브를 배격하고 오직 성능 구축에만 집중합니다. BSV 블록체인은 사적으로 소유된 인프라이지만 대중에게 연중무휴 24/7 제공되며, 기존 시스템들이 본래 기능의 일부만 모방하기 위해 필요한 수많은 레거시 시스템보다 훨씬 더 빠르고 극히 적은 비용으로 작동합니다.

## 예측 가능한 저비용으로 안전하고 즉시 처리되는 거래(Safe, Instant Transactions at a Predictably Low Cost)

비트코인은 처음부터 확장성을 염두에 두고 설계되었습니다. 전 세계적 수요를 관리할 수 있는 시스템으로 확장하기 위해 직관적이지 않은 일부 설계 선택이 이루어졌습니다. 이러한 선택은 네트워크에서 토큰의 회계를 어떻게 관리할지, 토큰이 교환될 때 어떻게 작동할지 등을 결정합니다.

Forth라는 초기 어셈블리 언어와 유사한 저수준 스크립트 언어, 직관적이지 않은 데이터 포맷, 혁신적인 경제적 가정 등이 결합되어 이 기술의 전문가가 되는 것은 어렵고 까다로운 일이 되었습니다. 그 결과 비트코인의 독창적인 설계 선택들은 제대로 이해되지 못했고, 추가 계층 없이는 확장할 수 없거나 스마트 계약과 같은 기능을 제공할 만큼 유연하지 않다는 잘못된 믿음으로 이어졌습니다.

이러한 **순진한 가정(naive assumptions)** 들은 수년간의 논쟁을 초래했고, 결국 개발자들이 기본 프로토콜을 변경하여 인센티브 구조를 영구적으로 변질시키고 확장을 막게 되었습니다.

이와 같은 자기 제한적 확장성과 기능 제약에 대응하기 위해 수많은 해결 시도가 등장했으며, 이를 통칭해 ‘암호화폐(cryptocurrency)’라 부릅니다. 그러나 비트코인은 수십 년간의 연구에서 탄생한 반면, 암호화폐들은 거의 연구적·학문적 기반이 없습니다. ‘암호화폐’가 모든 상상 가능한 사용 사례마다 새로운 블록체인을 만들어 블록체인 확장 문제를 해결할 수 있다는 생각은 결국 시장 투기 외에는 아무런 실제 사용 사례도 제공하지 못하는 결과를 낳았습니다.

비트코인 프로토콜은 모든 형태의 거래를 지원하도록 설계되었습니다. 보안성이 높은 시간 잠금 신탁(time-locked trusts), 계층적 계정, 스트리밍 결제, 조건부 결제 등 복잡한 거래들이 스크립트 언어로 정의되고 네트워크에 의해 완전히 관리될 수 있어, 비즈니스 운영과 고객 상호작용 비용을 획기적으로 줄일 수 있습니다.

전문 연구 및 개발팀들의 엄청난 기여 덕분에 잘못된 가정하에 변경되었던 비트코인 프로토콜은 BSV 블록체인에서 거의 완전히 되돌려졌으며, 현재 BSV 네트워크에서 사용되는 프로토콜은 원래 비트코인 프로토콜에 최대한 가깝게 복원되었습니다.

노드 클라이언트 소프트웨어의 개발은 사토시의 다소 비전통적으로 보이는 설계 선택을 활용하여 네트워크 처리량, 용량, 기능에서 엄청난 혁신을 이루어냈습니다. 인프라와 소프트웨어 개발은 계속 이어지고 있으며, 특히 클라우드 마이크로서비스 아키텍처에 적합하게 완전히 재설계된 노드 클라이언트인 테라노드 (Teranode)의 출시가 예정되어 있습니다.

## 안정적으로 낮은 수수료(Reliably Low Fees)

BSV 네트워크는 일반적인 수요보다 최소 한 자릿수 이상 많은 거래를 처리할 수 있도록 설계되어, 다른 블록 체인 네트워크에서 흔히 보이는 시장 기반의 수수료 압박이 발생하지 않습니다. 이는 채굴자들이 사용자들에게 낮고 안정적인 거래 수수료를 설정할 수 있도록 합니다. 비트코인은 원래부터 무제한 확장을 목표로 했으며, 바로 이 확장이 긍정적인 사용자 경험과 지속 가능한 블록 보상을 가능하게 합니다.

네트워크가 더 많은 거래량을 처리할수록 채굴자들의 수수료 수익은 증가하고, 경쟁의 힘은 더 유능한 노드들이 가능한 최적의 효율로 거래 처리를 제공하도록 만듭니다. 이러한 경쟁은 네트워크가 더 많은 거래량을 수용하고 수수료가 낮아짐에 따라 더 많은 사용 사례들이 저렴한 수수료로 경제적으로 실행 가능해지고, 거래량은 증가하며 저렴한 거래를 처리하는 계약을 중개하는 더 유능한 노드들에게 보상이 돌아가도록 보장합니다.

이러한 수요와 공급, 규모의 경제의 결합은 네트워크 처리량이 증가함에 따라 더 많은 사용 사례를 창출하고, 상호운용성, 책임성, 가치 포착 측면에서 향상된 효율성이 사회 전체에 많은 혜택을 가져다주도록 합니다.

## 기존 거래 시스템과의 비교(Comparison to Legacy Transaction Systems)

네트워크에 제출된 유효한 거래는 네트워크 노드에 제출된 지 몇 초 만에 승인 및 정산된 것으로 간주될 수 있다는 점을 이해하는 것도 중요합니다. 거래 상태를 확인하는 것도 빠르고 간단하며, 지갑 소프트웨어 내에서 자동화될 수 있습니다.

일반적으로 BSV 네트워크를 통한 단순 거래 비용은 약 0.0005센트(USD)로, 단지 100달러만으로도 1,000,000건의 거래를 처리할 수 있습니다. 이러한 거래는 1센트 미만 단위의 가치를 전송하는 것도 가능합니다. 일반적인 신용카드 거래 비용이 약 25센트(USD)임을 고려하면, 이는 비용을 2500배 절감하는 효과입니다. 또한 거래는 청구 취소(chargeback) 및 기타 비즈니스 리스크를 제거하는 방식으로 처리되어, 공급업체가 마진을 높여 소비자 가격에 영향을 미칠 필요가 없습니다. 이러한 고유한 특성은 개발자들이 BSV 블록체인을 플랫폼의 기반 기술로 활용하여 기존 디지털 결제 시스템으로는 불가능했던 비즈니스 모델을 구현할 수 있도록 합니다.

## 결제 채널(Payment Channels)

BSV의 또 다른 기능은 사용자가 결제 채널을 활용할 수 있다는 것입니다. 결제 채널은 유효하지만 미래의 특정 시점까지 블록에 포함되지 않는 거래입니다. 그 사이에 거래 당사자들은 데이터 패킷 공유, 지불 금액 등 거래 내용의 일부를 변경하는 새로운 업데이트를 자유롭게 게시할 수 있으며, 이를 통해 혁신적이고 매력적인 디지털 서비스를 거래 자체 내에서 관리할 수 있습니다. 결제 채널은 혁신적인 신기술로, BSV 네트워크에서만 지원됩니다.

BSV의 결제 채널 기능을 활용함으로써, 기업들은 고객에게 훨씬 더 반응성 높은 서비스를 제공할 수 있습니다. 예를 들어, 초 단위 과금 스트리밍 콘텐츠와 VoIP 통신을 결제 시스템에 직접 내장할 수 있으며, 이를 통해 제3자에 대한 의존 없이 서비스 제공 중에 수익을 확보할 수 있습니다.

## 글로벌 수요를 수용할 확장성(Scalability to Accommodate Global Demand)

BSV 블록체인의 가장 중요한 측면 중 하나는 무제한으로 확장할 수 있는 능력으로, 초당 수억 건 또는 수십억 건의 거래를 관리할 잠재력을 가진다는 점입니다. 2009년, 비트코인은 블록 크기, 거래 크기, 스크립트 복잡성 또는 연산 코드(opcodes) 사용에 제한 없이 출시되었습니다. 그러나 2010년부터 2017년 사이, 기본 프로토콜에 수많은 변경이 가해져 확장 능력이 제한되었습니다. 하지만 2018년 이후, BSV 노드 클라이언트 소프트웨어를 개발하는 팀들이 원래의 무제한 프로토콜 설계를 복원하기 위해 노력해왔습니다.

무제한 인센티브 구조 외에도, 비트코인 스크립트는 IPV6와의 호환성을 보장하는 연산 코드(op\_codes)를 포함하며, 필요할 경우 추가 해시 함수를 도입할 수 있는 확장 연산 코드도 지원합니다. 더 나아가 IPV6가 IPV4를 대체함에 따라, BSV는 온라인에 접속할 것으로 예상되는 수십억 개의 IoT 기기를 지원하는 데 핵심적인 역할을 하게 될 것입니다.

마이크로 트랜잭션을 통해, BSV 블록체인은 글로벌 검증 및 타임스탬프 서비스로 기능하며, 데이터와 통신을 정제(clean)하고 무결성을 유지하며 AI 및 머신러닝을 가속화하는 효과적인 방법을 제공합니다.

메타버스와 웹3의 개념이 실제 제품과 서비스로 전환됨에 따라, 사용자당 매시간 수백 건의 거래를 처리할 수 있는 전용 기술 기반이 필수적입니다. 기존 데이터 및 결제 네트워크는 이러한 사용 조건을 고려해 처음부터 설계된 것이 아니기 때문에, 이러한 제품과 서비스를 실현하는 것은 비현실적이거나 불가능할 수 있습니다.

## 대형 블록이 보여주는 큰 잠재력(Big Blocks Show Big Potential)

2024년 현재, BSV 노드들은 이미 100만 건이 넘는 거래를 포함하고 최대 4GB 크기에 달하는 블록을 정기적으로 처리하고 있습니다.

네트워크가 원활하게 확장되도록 하기 위해, BSV 노드 소프트웨어 팀은 소프트웨어 성능 최적화에 집중하고 있으며, 기본 프로토콜을 일관되게 유지하는 것이 이를 가능하게 합니다. 노드의 확장을 지원할 뿐만 아니라, 지속적인 효율성 개선과 변하지 않는 기본 프로토콜은 네트워크가 상당한 처리 능력을 잃는 경우에도 강건함을 보장합니다. 노드 클라이언트와 이를 실행하는 시스템을 확장하는 것은 네트워크의 견고한 아키텍처와 기능을 떠받치는 핵심 기둥입니다.

중요한 점은, 노드가 보상을 받기 위해서는 블록을 획득해야 하고, 큰 용량과 처리 능력을 가진 노드들이 서로 잘 연결되어 있을수록 보상을 받을 확률이 크게 증가하기 때문에, 네트워크는 수요가 아무리 커지더라도 항상 이를 수용할 수 있다는 점입니다.

BSV의 정교한 경제적 인센티브는 또한 노드들이 처리량을 늘려 더 많은 수수료 수익을 끌어들이기 위해 적극적인 전략을 펼치도록 장려합니다. 그러나 동시에 인센티브 구조는 네트워크의 다른 노드들을 앞질러 불균형적으로 성장하지 못하도록 설계되어 있습니다.

BSV는 협력적이며 실력주의적인 시스템입니다. 노드가 더 야심차고 경쟁적일수록 더 큰 보상을 얻을 수 있지만, 그 전제 조건은 노드들이 서로 완전히 개방적이고 정직해야 효율성을 극대화할 수 있다는 점입니다. 이러한 경제 게임의 규칙은 보상을 증대시키고, 네트워크 참가자 모두에게 상호 이익이 되는 행동을 보장합니다.

이러한 행위들은 네트워크 내 개별 노드 운영자들이 자기 이익을 추구하는 관점에서 설명될 수 있습니다. 네트워크의 기능에는 이타주의가 개입할 여지가 없으며, 항상 개방적인 경쟁이 존재하여 시스템 사용자 모두에게 최상의 서비스를 제공하도록 합니다.

BSV 네트워크의 운영에 대해 더 배우고 싶은 학생들은 **BSV 인프라 소개(Introduction to BSV Infrastructure)** 과정을 수강할 것을 강력히 권장합니다.

## 규제 수용을 위한 계획(A Plan for Regulatory Acceptance)

암호화폐와 블록체인 환경의 많은 부분에서, 법적 절차와 규제를 거의 고려하지 않는 흔적을 볼 수 있습니다. 흔히 제기되는 주장은 기술이 너무 새롭기 때문에 법과 규제가 적용될 수 없다는 것입니다. 그러나 이는 새로운 서비스 매체에도 미디어 소유 관련 법률이 적용되는 것과 다르지 않습니다. BSV 블록체인은 현재의 법과 규제 체계 내에서 작동할 수 있을 뿐만 아니라, 법적 요구 사항을 단순하고 저렴하게 준수할 수 있도록 설계되었음을 보여줄 수 있습니다.

비트코인은 결코 법률 시스템을 전복하거나 중앙은행을 파괴하기 위해 만들어진 것이 아니라, 훨씬 더 효율적이고 확장 가능하며 수익성 있는 방식으로 새로운 플랫폼과 서비스를 구축하기 위한 도구로 만들어졌습니다. 초저비용, 고효율 결제를 기반으로 한 마이크로 결제 비즈니스 모델은 이러한 시스템에서만 가능합니다.

원장에 발행된 각 사토시는 단순히 그 자체 이상의 데이터를 담거나 더 높은 가치를 지닌 항목을 운반하는 데 사용될 수 있어, 모든 형태의 제품과 서비스가 법적 요구 사항을 준수하면서 운영될 수 있는 효과적인 기반 시스템을 제공합니다.

## 준비된 규제 준수(Ready-made Compliance)

기술 표준 위원회(Technical Standards Committee, TSC)가 수행하는 중요한 작업 중 하나는 기업들이 플랫폼을 구축할 때 엄격한 규제를 쉽고 저렴하게 준수할 수 있도록 돕는 준비된 도구 세트를 구현하고 서비스하는 것입니다. 여기에는 국제적으로 적용되는 고객 확인 제도(KYC, Know Your Customer) 및 자금 세탁 방지 규정(AML, Anti Money Laundering)이 포함됩니다. 모든 가상자산 서비스 제공자(VASP)는 고객 이체를 다룰 때 반드시 이를 준수해야 합니다.

또한 Paymail/BSVAlias와 같은 시스템은 기업들이 고객의 프라이버시에 영향을 주지 않으면서도 책임을 최소화하는 방식으로 고객 신원을 간단하고 쉽게 관리할 수 있도록 지원합니다.

TSC는 지속적으로 새로운 표준을 개발하여 기존 레거시 시스템의 기능을 능가하는 빠르고 저비용의 디지털 서비스를 제공하고 있으며, 이를 통해 BSV 블록체인 위에 구축되는 모든 플랫폼이 오늘날과 미래의 규제를 충족할 수 있도록 보장합니다.

## 오픈 BSV 라이선스(The Open BSV License)

오픈 BSV 라이선스(<https://github.com/bitcoin-sv/bitcoin-sv/blob/master/LICENSE>)는 소프트웨어나 애플리케이션을 오직 BSV 블록체인에서만 오픈(무료) 사용 가능하게 하고자 하는 개발자, 프로젝트 또는 기업을 위해 만들어졌습니다. 이는 MIT 라이선스를 수정한 버전으로, 오픈 소스 소프트웨어를 BSV 블록체인과 그 관련 테스트넷에서만 자유롭게 사용 및 수정할 수 있도록 허용합니다.

오픈 BSV 라이선스가 만들어진 이후, 다음을 포함한 수많은 프로토콜, 툴킷, 소프트웨어 요소들이 공개되었습니다:

- Nakasendo
- Go-SVDB
- ElectrumSV
- Bitbus
- 그 외 다수

## 프로토콜 안정성(Protocol Stability)

BSV 블록체인의 채택, 장수, 신뢰성에 기여할 가장 중요한 측면 중 하나는 프로토콜로서의 안정성입니다. 2010년부터 2018년까지, 노드 클라이언트 개발자들은 시스템의 ‘문제’라고 잘못 인식한 부분을 ‘수정’하려 하면서 비트코인 프로토콜을 여러 근본적인 방식으로 변경했습니다. 그러나 이러한 ‘수정’은 많은 영역에서 더 큰 하위 문제들을 야기했고, 당시 애플리케이션과 비즈니스를 구축하던 개발자들에게 심각한 혼란을 안겼습니다.

이러한 불확실성은 자신들이 구축하는 것이 앞으로도 계속 작동할 것인지, 아니면 원치 않는 불필요한 기본 프로토콜 변경으로 인해 무용지물이 될지 확신할 수 없게 만들었습니다.

BSV 노드 클라이언트가 출시되면서, 네트워크의 중재자인 노드 운영자들은 이미 가해진 변경 사항을 되돌리는 경우(예: 거래 및 블록 크기 제한 제거, 스크립트 언어에서 비활성화된 기능 재활성화)를 제외하고는 프로토콜에 더 이상의 변경을 가하지 않겠다는 정책을 확립했습니다.

## 반석 위에 기초를 세우다(Building Foundations on a Bedrock of Stone)

맨해튼의 화강암 기반암이 세계에서 가장 높은 밀도의 마천루들을 떠받치는 기초를 제공하듯이, 안정적이고 변하지 않는 기본 프로토콜은 기업가와 투자자들에게 BSV 위에 애플리케이션과 비즈니스를 구축하는 데 필요한 시간과 돈을 투자할 자신감을 줍니다. 기술에 의존하는 기업에게 있어 그 기술이 계속 변한다면, 애플리케이션과 프로세스가 작동 불가능해지는 상황이 발생합니다. BSV 블록체인의 경우, 이는 네트워크에 의존하는 애플리케이션이나 서비스가 더 이상 접근 불가능해지거나, 더 심각하게는 미래의 특정 시점에 실행되도록 사전에 서명된 거래들이 더 이상 처리될 수 없게 되는 것을 의미할 수 있습니다.

이것은 모래 위에 성을 짓는 것과 같아, 기초 아래의 지반이 움직이면 결국 성이 무너질 수 있습니다.

BSV 네트워크의 관리자와 중재자들이 변하지 않는 기본 프로토콜을 유지하겠다고 약속했기 때문에, 개발자들은 자신들의 시간, 노력, 자금을 투자해 구축한 애플리케이션과 비즈니스가 경험 없는 소수 개발자 집단의 자의적인 변덕으로 인해 중단되거나 작동 불능 상태에 빠지지 않을 것이라 믿을 수 있습니다.