한 번에 끝내는
블록체인 개발 A to Z

Chapter 1

Blockchain 1.0 - Bitcoin

Chapter 1

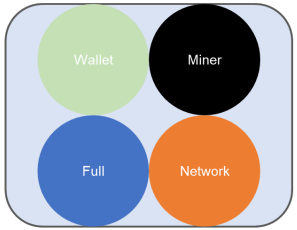
Blockchain 1.0 - Bitcoin

블록체인
노드와 지갑

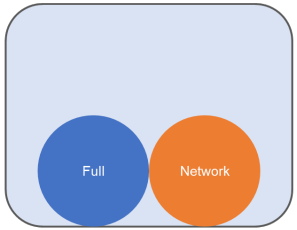
Bitcoin Node와 역할에 따른 구분

- Bitcoin 네트워크 참여자를 부르는 용어는 Node, Peer 등이 있다.
- 최초 Bitcoin Network에서는 Bitcoind 을 통해서만 Network에 참여가 가능했기 때문에 모두다 Node 역할을 하였지만, 최근에는 Explorer, Miner, Wallet User(Client), Exchange 등 Network 참여목적에 따라 역할이 구분되고 있다.
- 각 구분된 Node의 역할에 따라 bitcoin Node을 사용 방법이 다양하게 이루어진다.
- 공식적인 문서에서는 Full Node, LightWeight(SPV) Node로만 구분하고 있다.

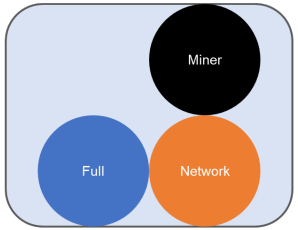
Bitcoin Node와 역할에 따른 구분



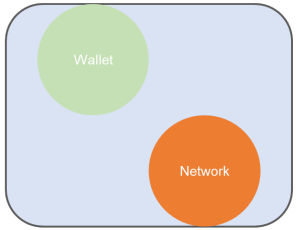
Bitcoin Core Full Node



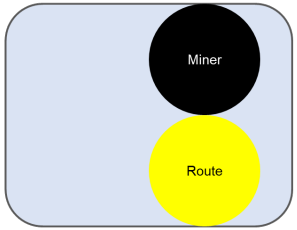
Full Node



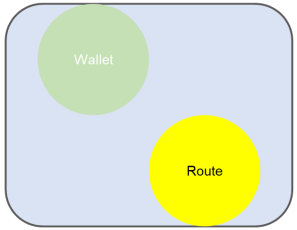
Miner Node



SPV Node

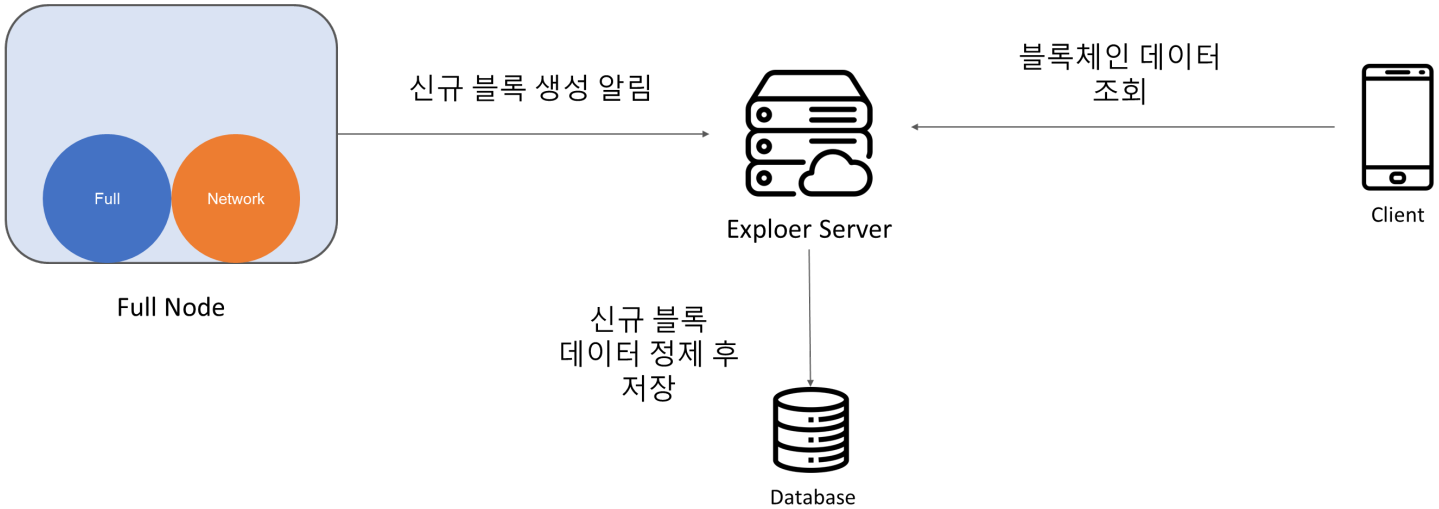


Mining Pool Node

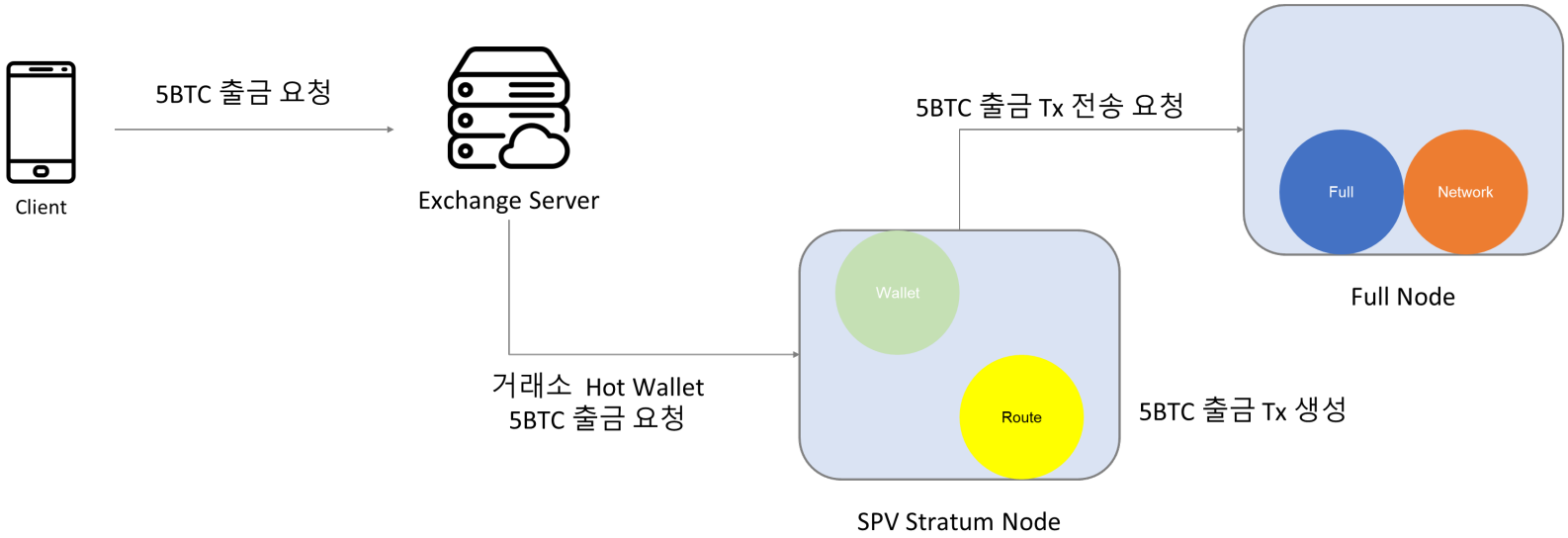


SPV Stratum Node

Explorer 구조


Full
Network
Full Node
신규 블록 생성 알림
Exploer Server
블록체인 데이터
조회
Client
신규 블록
데이터 정제 후
저장
Database

Exchange 구조


Client
5BTC 출금 요청
Exchange Server
5BTC 출금 Tx 전송 요청
Full
Network
Full Node
Wallet
Route
거래소 Hot Wallet
5BTC 출금 요청
5BTC 출금 Tx 생성
SPV Stratum Node

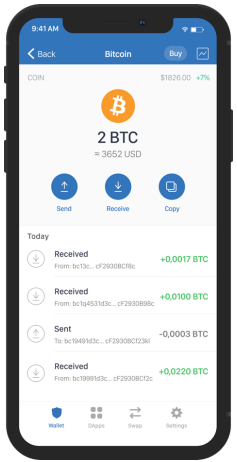
Bitcoin Wallet

- Bitcoin Wallet 의 역할은 사용자의 키를 안전하게 관리하고 이를 통해서 사용자가 쉽게 거래(송금)을 생성하는 것을 지원해준다.

- 사용자가 필요로 하는 기본적인 기능들을 아래와 같이 제공한다.
  1) 거래 조회
  2) 사용자 잔액 조회
  3) 신규 블록 생성 알림
  4) 주소록 관리
  5) 사용자 키 관리

Bitcoin Wallet 종류

- Bitcoin Wallet은 Web Wallet, App Wallet, Paper Wallet , Hardware Wallet 등이 있다.
- 개인키만 따로 json이나 string 형태로 Email이나 file형태로 저장하는 경우도 있지만, 이런 경우에는 해킹의 위험이 매우 높다.



출처) commons.wikimedia.org

출처) lotteon.com

Hardware Wallet

- 기존 지갑들은 Private Key를 보관을 해주는 역할은 하였지만, 안전하게 보관을 해주는 기능이 부족함에 따라 개인키를 안전하게 보관할 수 있는 Hardware Wallet이 개발되었다.
- 개인키를 Export 할 수 있는 기존 Wallet 과는 달리 Hardware Wallet은 Private Key를 Export 하거나 조회 할 수 없게 생성되었다.
- 하나의 Hardware Wallet은 다수의 Address를 생성하고 관리 할 수 있게 관리된다.
- 지문이나 PIN 번호 등 Hardware Wallet 자체의 보안기능을 제공한다.
- Hardware Wallet 고장 시 복구할 수 있는 방법인 Mnemonic 기능을 제공한다.
- 가상자산 고액 자산가들이 대부분 사용한다.

Samsung Wallet

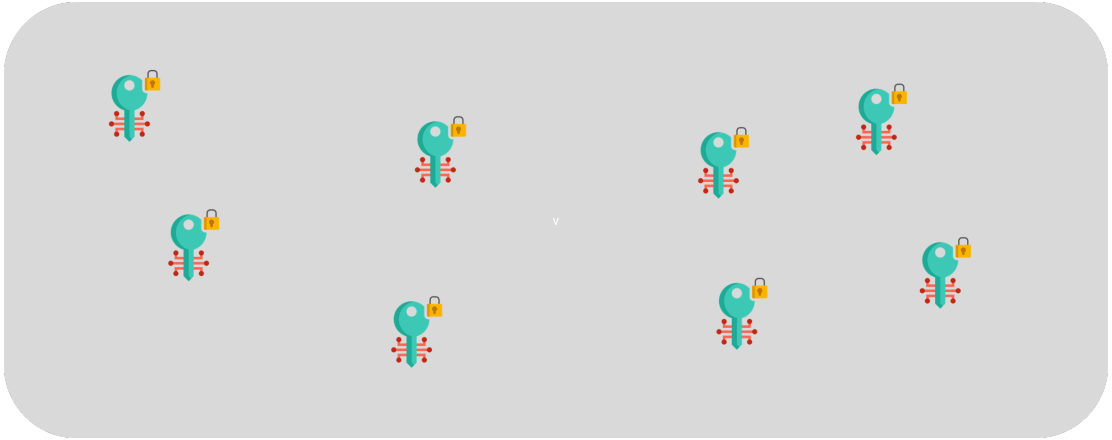
- Samsung Blockchain은 삼성 스마트폰을 이용하는 사용자들이 따로 Wallet을 다운로드 받지 않고, 서비스를 제공 받을 수 있게 제공하는 기본 탑재 Wallet Application 이며, 이와 함께 Dapp Store를 출시하여 Wallet에서 바로 Dapp 서비스들을 이용할 수 있는 기능을 제공한다.
- Samsung Blockchain은 Hardware상에서 보안 안전 공간(Trust Zone)인 TEE(Trust Execution Environment)에서 사용자의 개인키를 보관 관리하는 기능을 제공한다.
- Hardware Wallet과는 달리 개인키를 안전하게 보관하며 Export 기능도 제공을 하고 있다.
- 단점은 TEE 환경에서 동작하기 위해서 기본 Wallet에서 보안 관련 설정이 추가로 진행해야 된다.

Cold와 Hot Wallet

- Cold Wallet과 Hot Wallet은 개인키를 관리하는 소프트웨어(지갑)이 인터넷 환경과 연결된 상태인지, 아닌지에 따라 구분된다.
- Exchange는 사용자의 입출금이 활발하고 해킹의 위험이 항상 존재하기 때문에 Cold와 Hot Wallet으로 구분하여 자산을 관리한다.
- Hot Wallet은 Web Wallet, App Wallet, Desktop Wallet등이 있다.
- Cold Wallet은 Hardware Wallet, Paper Wallet, Offline Computer Wallet등이 있다.

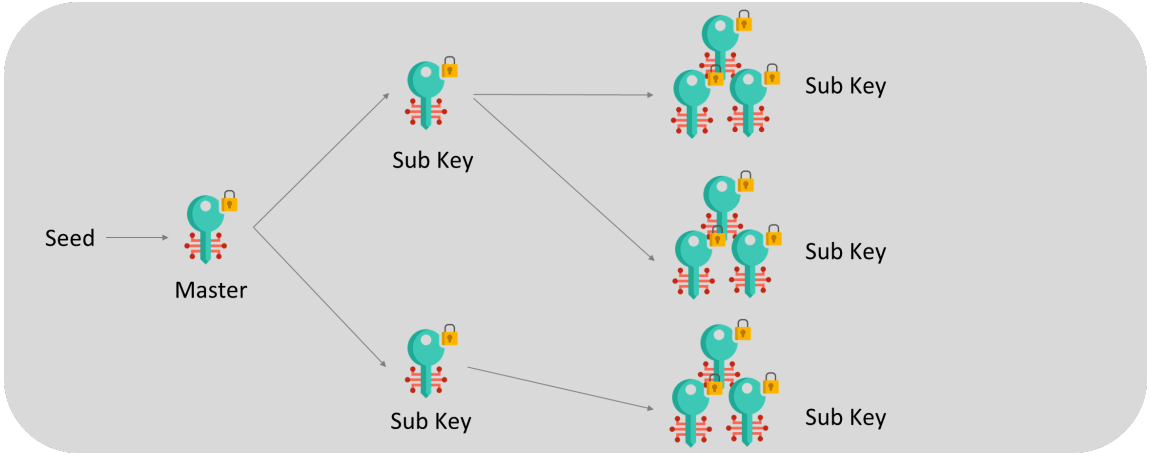
Nondeterministic(Random) Wallet

- 100 개의 Random 개인키를 생성하고, 이를 한번씩만 사용하는 지갑
- 주소를 한번만 사용하다보니 Privacy 보장이 높아짐
- Private Key 관리를 위해서 주기적인 BackUp이 필요함



Hierarchical Deterministic(Seed) Wallet

- 하나의 Seed값에서 생성된 Master Key를 중심으로 계층적으로 개인키를 생성
- 개인키(Master) 하나로 여러 개의 주소를 관리 가능
- 여러 Branch 키를 생성하여, Branch 마다 용도에 맞는 주소 그룹 분류 가능



Mnemonic이란?

- BIP-39에서 제안된 새로운 Seed 관리 방안
- 기존 Random Seed를 통해 개인키 생성을 하고 개인키 분실 시 복구가 불가능
- Mnemonic을 통해 개인키를 분실해도 Mnemonic을 통해 개인키 재 생성 가능