한 번에 끝내는
블록체인 개발 A to Z

Chapter 1

Blockchain 1.0 - Bitcoin

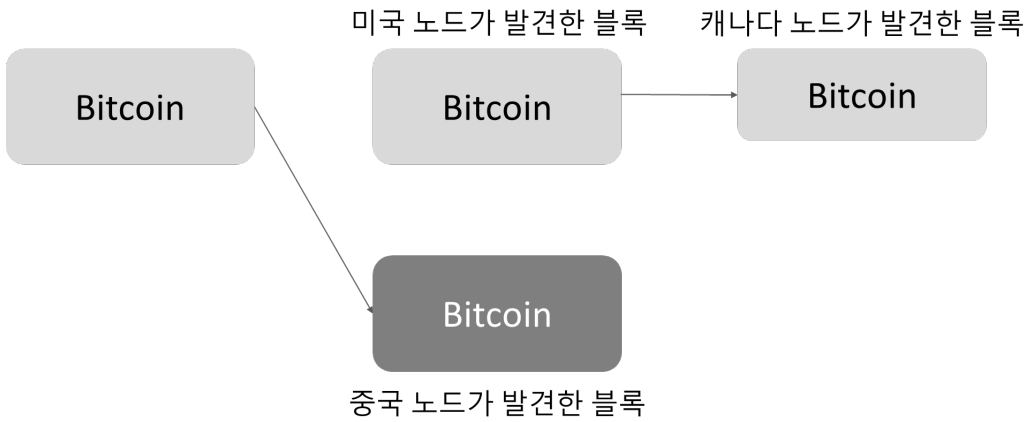
Chapter 1

Blockchain 1.0 - Bitcoin

Hard Fork와 Soft Fork

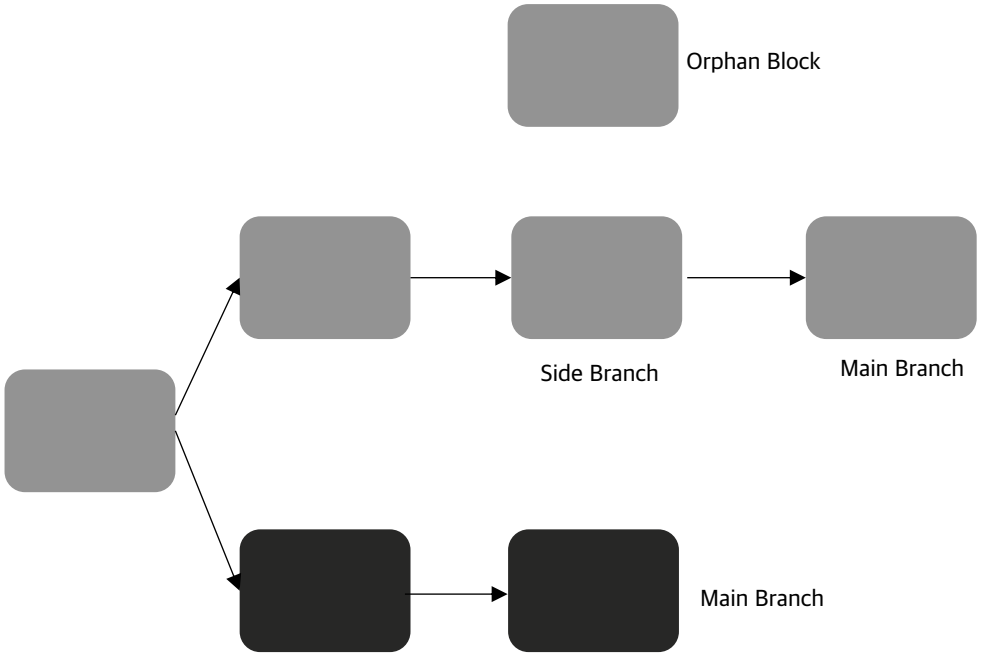
Fork

- Bitcoin은 노드가 글로벌하게 분포되어 있으며, 각 채굴자들은 모두 동시에 PoW를 통해 신규 블록 채굴에 도전한다.
- 혹시 미국의 노드와 중국의 노드가 동시에 블록 정답(Nonce) 찾기에 성공하는 경우에는 어떻게 될까?
- 이런 경우를 우리는 Blockchain Network가 일시적으로 분기되었다고 이야기하고 이를 Fork 라고 부른다.
- 하지만 Bitcoin은 Longest Blockchain Rule을 통해 이렇게 Fork 된 네트워크를 하나로 유지시키고 있다.



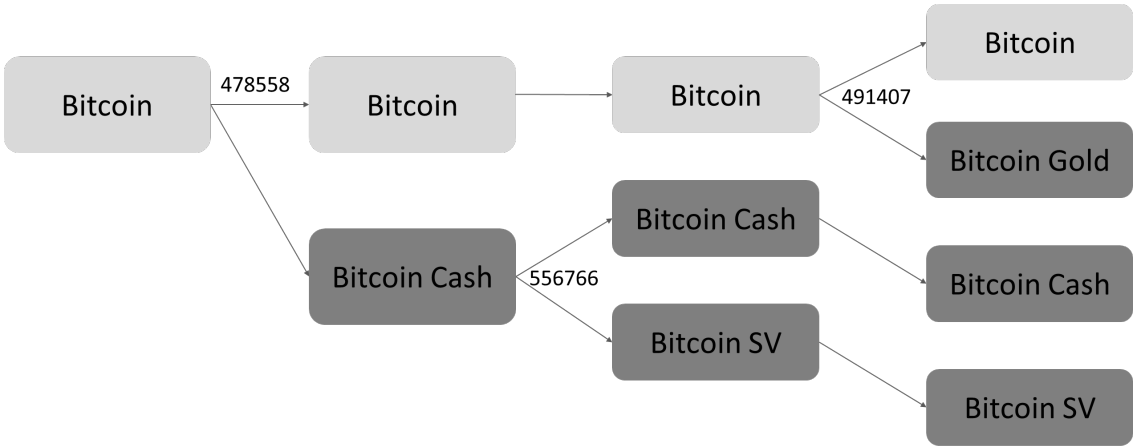
Fork Rule

- Bitcoin Block은 어떤 Block이 전달될지 모르기 때문에, Fork 발생 시 2개의 Chain을 가지고 있으며, 이 중 Longest Chain을 Main Chain으로 유지하고 있다.
- Main Branch가 Longest가 아님을 알게 된 순간, Side Branch를 Main으로 변경하고 이에 대한 LevelDB 업데이트가 이루어진다.

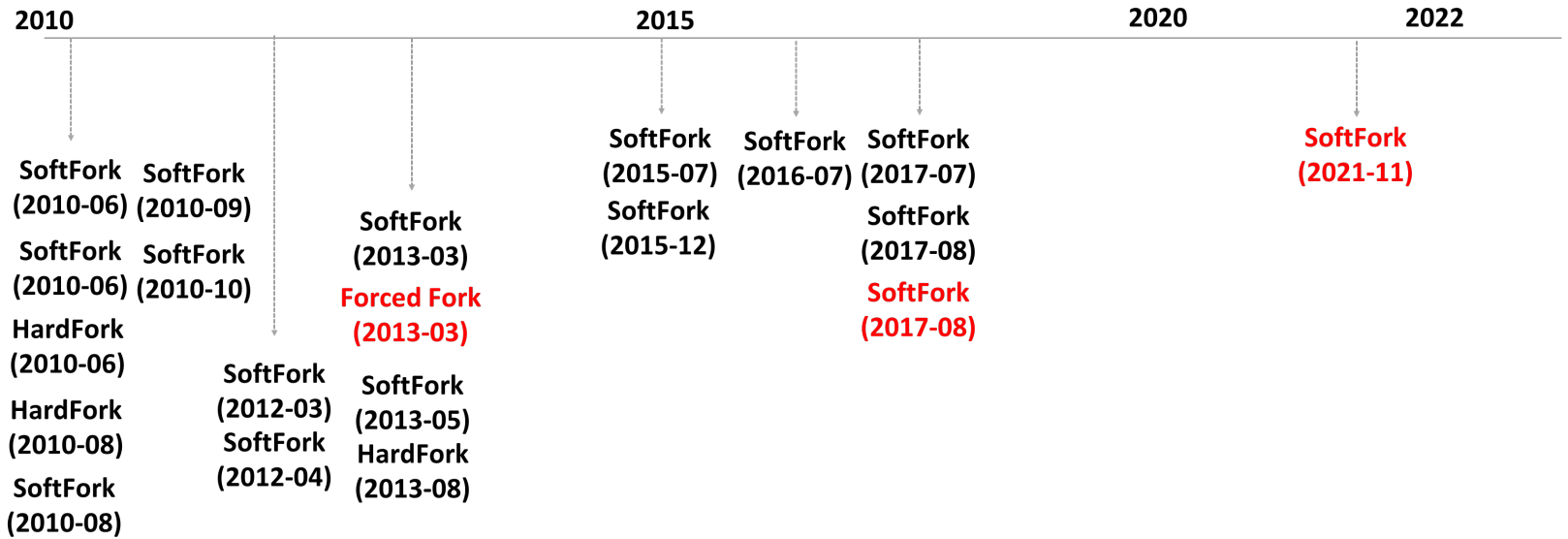


Bitcoin Software Upgrade

- Bitcoin Software의 Upgrade는 사용자가 본인이 사용하고 있는 프로그램을 신규 버전으로 재설치 하면된다.
- 이렇게 Software의 Upgrade가 필요한 경우를 Fork라고 부르고, Soft Fork 와 Hard Fork로 구분한다.
- Soft Fork는 모든 사용자가 Node Upgrade를 하지 않아도 진행이 된다.
- Hard Fork는 모든 사용자가 Node Upgrade를 해야 하고, 하지 않는 경우 네트워크에서 분리된다.



Bitcoin Fork History

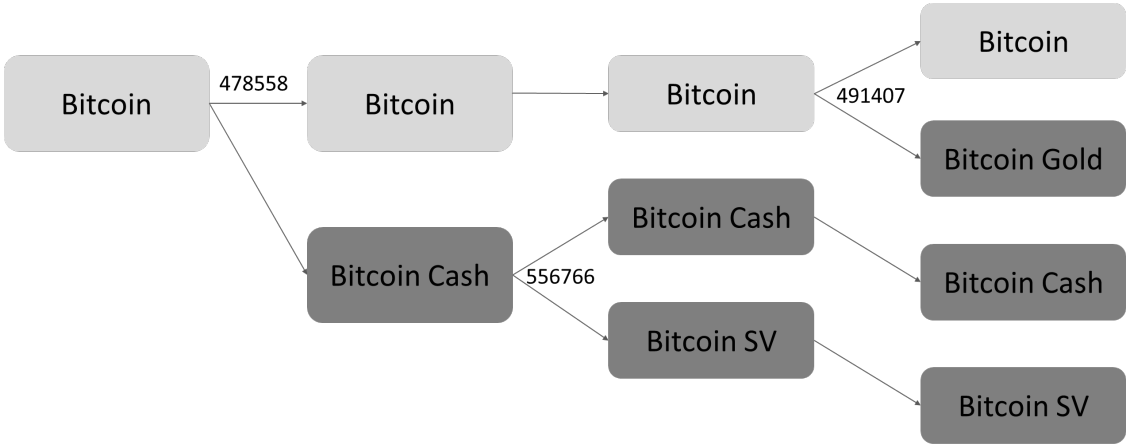


Soft Fork - Segwit

- Segwit은 Bitcoin의 블록 사이즈로 인한 처리 성능을 제한을 해소하고, Transaction Malleability 문제를 해결하는 방안으로 제시
- Soft Fork이기 때문에, 기존 Node가 업그레이드 하지 않아도 Segwit Transaction 처리가능
- 대표적인 ASIC 채굴자들이 반대하면서 Network Fork 분리가 발생하게 됨.

Bitcoin Hard Fork 발생원인

- Hard Fork는 네트워크 분리가 발생한다. 하지만 특정 기능을 제외한 대부분은 동일하다.(주소형태 등)
- 탈중앙화된 블록체인의 특성 상 새로운 업그레이드에 찬성하는 쪽과 반대한 쪽이 나뉘게 된다.
- Hard Fork 후에는 기존에 연결된 Node 상에서 서로 인정하는 Block이 달라지게 되고, 자연스럽게 각 네트워크 참가하는 노드에 따라 네트워크 분리가 발생



Hard Fork - Bitcoin Cash(Bitcoin ABC)

- Bitcoin Cash와 Bitcoin이 분리되게 된 원인은 새로운 Segwit 업그레이드가 기존 ASIC에서는 사용이 불가능하기 때문이다.
- 채굴자 측에서는 블록 사이즈 문제는 블록 크기 증가(8MB)로 가능하다고 하였다.
- 개발진 측에서는 Segwit 적용이 블록체인 확장성 문제를 해결 가능하다고 하였다.
- 478559 번째 블록 부터 Bitcoin Cash가 BTC(Bitcoin) 거래를 거부하기 시작하며 네트워크 분리가 시작
- 네트워크 분리로 인해서 Bitcoin Network Hash Rate의 30% 정도가 사라졌다.
- Craig Wright(크레이그 라이트)는 Bitcoin Cash에서 2018년 8월 Bitcoin Cash의 Atomic Swap 업데이트에 반대하며 Bitcoin SV(128MB)로 Hard Fork를 진행하였다.