Difficulty and ePow Algorithm Update

난이도 조정(Difficult Adjustment) 과 ePow 알고리즘의 문제점을 개선한 HDAC 1.05.0 버전을 배포합니다.

본 버전은 합의 알고리즘 규칙 (consensus rules) 을 변경하는 것으로 HDAC 을 운영하는 전체 full node에 대한 업그레이드가 이루어 져야 합니다.

HDAC 과 관련된 Explorer, Wallet, DApp 등의 동작에 영향을 주는 부분이 없으므로 이에 대한 업그레이드는 불필요합니다.

난이도 조정 (Difficulty Adjustment)

HDAC 의 난이도 조정은 Bitcoin의 난이도 조정 주기의 문제점을 보완하고자 480 blocks 으로 조정하였고 이는 시간으로 분류하면 24시간 정도의 주기를 가지도록 설계 되었습니다.

하지만 낮은 난이도에서의 hash 공격과 높은 난이도에서 거래 지연 현상이 반복되는 등 네트웍 환경에 유연하게 적응하지 못하는 문제를 노출하게 되어 이에 대한 개선 작업을 진행 하였습니다.

HDAC 코어 개발진은 수많은 Bitcoin계열의 코어에서 채용되고 있는 난이도 조정 방식에 대한 분석 및 적용 검토를 진행하였으며 다양한 상황에 대한 시뮬레이션을 통해서 HDAC 에 좀더 최적화 된 형태로 적용 하고자 하였습니다.

기존 480 블록을 주기로 변경되는 난이도를 매 블록마다 변경될 수 있도록 하였으며 블록 생성 시간은 기존과 동일한 180초에 수렴될 수 있도록 하였습니다.

이전 블록들에 대한 블록 생성 시간의 간격과 해시비율(Hash Rate)은 난이도 결정을 위한 중요한 요소로 작용합니다.

이에 대한 표본 입력 값으로 480개의 블록을 기준으로 했을 때 난이도 변경 폭이 다소 미미하였으며 30개 이하의 블록을 기준으로 했을 때는 변화 폭이 너무 크고 변별력이 다소 떨어지는 문제가 있었기 때문에 다양한 상황을 가정한 시뮬레이션을 통해 적정 수준으로 판단되는 60개 블록을 기준으로 난이도가 계산 될 수 있도록 했습니다.

# 난이도 조정 동작 방식

* 이전 블록 60개를 표본으로 블록간의 생성 시간과 해시비율을 추출하여 다음 블록의 난이도를 결정하는 데 적용한다.
* 낮은 난이도에서 높은 해시 비율을 보일 때 난이도가 상승 할 수 있도록 조정한다.
* 높은 난이도에서 낮은 해시 비율을 보일 때 난이도가 하락 할 수 있도록 조정한다.
* 난이도 조정은 평균 블록 생성 시간이 180초에 수렴할 수 있도록 조정하며 이에 대한 기준 블록의 개수는 60 블록이다.
* 높은 난이도에서 과도하게 낮은 해시 비율로 인해 블록 생성 주기가 10분 ~ 1시간 이상 오랜 기간 길어지지 않도록 60블록 외에 최근 6개 블록의 평균 블록 생성 시간을 함께 고려하여 해시 비율에 맞는 난이도가 빠르게 유도 될 수 있도록 한다.

# 예상 되는 문제점

매 블록마다 난이도를 조정하기 때문에 매 블록마다 적용되는 난이도의 변화 폭이 일정 하지 않을 수 있으며 높은 해시비율에서는 480개 블록을 기준으로 하는 것 보다 높은 난이도로 수렴될 수도 있고 반대의 경우로 480개 블록을 기준으로 하는 것 보다 낮은 난이도로 수렴 될 수 있기 때문에 해시비율의 최고점과 최저점이 크지 않아야 좀더 이상적인 결과를 가져 올 수 있습니다.

또한 제한된 환경에서 시뮬레이션이 이루어 졌기 때문에 실제 네트웍에 적용 시 예상 되었던 수치 범위를 벗어 날 수 있기 때문에 이에 대한 데이터 수집 및 지속 검토를 통해 좀더 발전 된 형태의 개선안이 만들어 질 수 있도록 할 예정입니다.

# 향후 개선 방향

낮은 난이도에서 빠른 블록 생성 시간을 노리는 해시 공격에 대해서 완벽히 방어 하는 것은 현재의 POW 동작 방식에서는 근본적으로 어려움이 있지만 평균적인 블록 생성 주기인 180초를 유지하기 위한 알고리즘 개선 작업은 꾸준히 검토 예정입니다.

ePow Consensus Algorithm

# 기존 버전 문제점

특정 마이너의 독점 채굴을 방지하고자 적용되었으며 현재 블록 height 기준으로 480개 이전 블록 동안 채굴한 마이너의 수(보상 주소 기준)가 몇 개인지를 확인하여 그에 맞는 윈도우 사이즈(WZ)를 계산하고 WZ 값에 따라 연속 채굴이 불가능하도록 하여 전체 마이너에게 최소한의 공평한 기회가 부여되도록 설계 되었습니다.

현재 방식대로 유지될 경우 문제점은 현재는 WZ값이 1을 유지하고 있으나 블록 height가 커지거나 마이너 수가 많아지게 되면 향후 HDAC의 난이도와 상관없이 WZ 값이 상승하게 되어 채굴의 속도가 느려질 수 있고 난이도에 따른 hash 공격에 유연하게 대처하기가 어렵습니다.

난이도가 낮은 구간에서는 일부 마이너의 50% 이상 독점 채굴을 막을 수가 없고 난이도가 높은 구간에서는 블록 생성 시간이 1시간 이상(Blackout) 걸릴 수도 있습니다.

# 변경된 ePow 동작 방식( 채굴 독점 방지 )

* New 블록과 현재 블록의 생성 시간 간의 차이(TimeDiff)와 최근 10개 블록에서의 마이너 수와 마이너의 채굴량(MinerRate)을 기준으로 동작합니다.
* TimeDiff 값이 3분 이하일 경우 MinerRate 및 마이너의 채굴 타임 간격을 보고 결정

특정 마이너가 과반 독점하지 못하도록 하고 블록 타임을 3분에 수렴하도록 함

* TimeDiff가 12분 보다 클 경우 MinerRate 및 연속 채굴량을 보고 결정
* 기존의 blackout 시간은 1시간에서 48분으로 변경 ( 12분 x 4 )
* WZ 값은 이전 120블록을 기준으로 합니다.

120블록의 블록 생성 시간이 기준 시간(3분\*120블록)보다 작은 경우 채굴 마이너 수에 따라 WZ는 0, 1, 2 등으로 유동적으로 변화하며 블록 생성 시간이 기준시간보다 2배이상 클 경우 채굴 마이너 수에 따라 WZ는 0, 1 등으로 유동적으로 변화합니다.

# 예상 되는 문제점

난이도가 낮다고 판단되는 구간에서 높은 해시로 인해 수초, 수십초 마다 블록이 생성되는 경우에 블록 생성 시간이 지연되도록 하였지만 제한된 환경에서의 시뮬레이션 결과 이기 때문에 실제 네트워크 환경에서 동작 시 예상 범위를 넘어설 수도 있으므로 이에 대한 데이터 수집과 분석을 통하여 추가 개선 사항을 찾도록 할 계획입니다.

WZ 값이 블록 생성 시간과 채굴 마이너 수에 따라 유동적으로 변하게 되어 있지만 이로 인해 마이너 입장에서는 블록 생성을 해도 거부되는 경우가 이전보다는 빈번하게 발생할 수도 있어 이 또한 실제 네트워크 환경에서 예상 범위를 벗어날 수도 있습니다.

추가 데이터 수집과 분석으로 필요시 추가 개선사항을 검토할 계획입니다.

# 향후 개선 방향

변경된 난이도 계산 방식과 WZ, ePoW를 연계하여 낮은 난이도에서 해시 공격 및 높은 난이도에서의 해시 이탈 시에도 평균 블록 타임이 3분에 수렴 가능하도록 알고리즘을 꾸준히 검토할 예정입니다.