# [케블리] #3. Filecoin (파일코인) - P2P 드랍박스 시대 도래할까?

## Kblock 공식 리서치팀, 케블리


안녕하세요 케블리 입니다. 케블리는 '전세계의 블록체인 비즈니스를 함께 찾고 공부해 나눈다'는 KBlock의 목표에서 '나눈다'를 본격적으로 실천합니다.

---

### #3. Filecoin(파일코인) - P2P 드랍박스 시대 도래할까?


코인 투자자나 일반인 입장에서 바라볼 때, 수많은 알트코인들 중에서 획기적인 코인을 가려내는 작업이 마냥 쉽지만은 않습니다. 무엇보다 투자자들을 우롱하는 스캠 코인들이 너무 많죠. 그래서 앞으로 저의 역할을 '좀 더 합리적이고 획기적인 암호화폐'를 넓고 얕게 소개하는 일에 초점을 맞출까합니다 : )

## Filecoin

얼마 전 Telegram이 ICO 역사상 최대 자금 조달액 기록을 경신했죠 :) 그런데 Telegram 등장 전까지 부동의 ICO 규모 1위가 있었으니, 바로 오늘 소개해드릴 Filecoin 입니다 ! Filecoin의 ICO에 참여하기위해서는 연봉 20만달러 이상 (또는 배우자 포함 30만달러 이상) 또는 1백만 달러 이상의 자산을 증명해야 했습니다. 오늘은 이 Filecoin이 무엇인지 간단히 알아보겠습니다.

사실 Filecoin을 이해하기 위해서는 IPFS(InterPlanetary File System)를 먼저 간단히 알아야 합니다. IPFS는 전 세계 컴퓨터의 파일 표준 및 시스템을 연결시키려는 분산형 P2P 파일 표준입니다. IPFS 형태의 파일 저장을 장려하기 위해서, IPFS의 개발팀이 Filecoin이라는 탈중앙화 저장소 네트워크를 만들어낸 것이죠. 따라서 IPFS 형태의 파일 표준만

맞춘다면, 용량 제공자(Filecoin에서의 마이너)의 유휴 데이터 용량을 활용할 수 있게 됩니다. 이때 그 반대급부로 마이너에게 지불하게 되는 것이 'Filecoin'이라는 코인인데요. 이렇게 되면 암호화폐를 지불하고 활용하게 되는 일종의 시장, 또는 공유 경제 모델이 형성됩니다. 실제로 시장에 나오는 몇몇 코인들은 IPFS와 연결된 방식으로 등장하더군요. IPFS에 대해 잘 설명된 스팀잇 포스팅과 위키피디아 링크를 공유합니다.

https://steemit.com/kr/@scottnaddle/ipfs

IPFS wikipedia

Filecoin이란 클라우드 저장소를 알고리즘 시장으로 이끌어낸 탈중앙화 방식의 스토리지 네트워크이다. 이 알고리즘 시장은 프로토콜 토큰 'Filecoin'을 활용한 블록체인 위에서 형성되는데, 채굴자들은 자신들의 저장소를 클라이언트들에게 제공함으로써 이 토큰을 얻게 된다.

위 설명이 백서의 초록에서 볼 수 있는 Filecoin의 간단한 개념인데, 쉽게 생각하면 Filecoin은 IPFS 파일 표준을 기반으로 만들어진 '분산형 P2P 드랍박스' 정도로 이해될 것 같습니다. 한 개인이 컴퓨터 용량의 일정 부분을 타인에게 할당하면 코인을 얻게 되는 구조이지요.

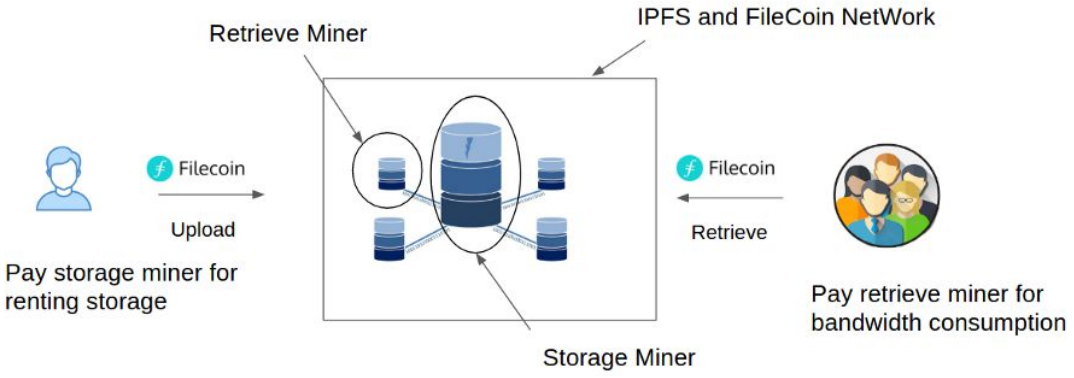
암호화폐에서는 항상 dApp에서 활용되는 토큰과 코인을 구분해야 하는데, Filecoin의 경우 토큰에 대한 별도의 설명은 나와있지 않은 것으로 보아 코인이 직접적으로 유통되는 것 같습니다.

## 특징

이제 Filecoin의 특징을 알아보겠습니다. Filecoin의 구성요소들을 제대로 이해하려면 컴퓨터 과학적 사고방식과 함수에 대한 배경지식이 있어야 하지만, 너무 디테일하게 들어가면 어려워질 수가 있기 때문에 넓고 얕게 소개드리는 것에 초점을 맞추겠습니다. 제가 소개할 특징은 크게 2가지로, 'DSN(Decentralized Storage Network)'이라는 네트워크와 Filecoin만의 독특한 '합의 알고리즘' 입니다.

## DSN

Filecoin 백서에는 DSN이라는 용어가 심심치 않게 등장합니다. DSN이란 Filecoin이 활용되는 네트워크 자체를 의미하는데, 직역하면 '탈중앙화 저장소 네트워크'가 됩니다. 사용자들은 DSN 상에서 데이터 용량을 제공하는 마이너들에게 보상을 지불합니다. 이 때, 채굴자들은 그들의 서비스 제공이 올바르게 이루어졌다고 '감사(Audit)'를 받는 경우에만 이 보상을 받을 수 있고요. 제가 이해한 바로는 DSN은 결국 개인의 유휴 데이터 용량을 거래하는, 일종의 모바일/디지털 시장과 비슷한 것 같습니다.




언뜻 보면 뭔가 복잡해 보이는데, 이런 네트워크가 구동되기 위해서는 역시 블록체인 내부의 합의 방식이 이슈가 됩니다. 바로 다음 항목에서 간략히 설명드리겠습니다.

## 합의 알고리즘(Consensus) 방식

블록체인에서는 합의 알고리즘이 어떻게 짜여지냐에 따라 블록체인 서비스나 비즈니스 모델이 변동합니다. 일종의 뼈대같은 구조라고 생각하는데요. Filecoin이 제공하는 DSN이라는 것도 구성원들의 자발적 합의에 의해 돌아가게끔 하는 독특한 합의 알고리즘이 있는데, 복제 증명이라는 방식과 시공간 증명이라는 방식입니다.

- 복제 증명 (PoRep : Proof-of-Replication)

복제 증명은 PoS 방식의 또 다른 종류인데, 복제 증명 방식은 특정 서버가 데이터를 저장함에 있어 고유한 물리적 저장소임을 입증하는 역할을 한다. 이 서버 내에서 특정 데이터는 두 번씩 복제되기 어렵고, 중복된 복제는 제거(deduplicate)된다. 이 구조는 클라우드 저장소, 또는 DSN 셋팅에 유용하게 활용되는데, 이런 구조 내에서는 복제의 적절한 레벨을 입증하는 것이 중요해지거나 해당 서비스를 동일한 유저에게 중복해서 팔게 될 수도 있다. PoRep는 각 사본이 독립적으로(중복되지 않고) 저장됨을 입증할 수 있다.

복제 증명의 개념을 보자면 마치 비트코인에서 작업 증명(Proof-of-Work) 방식이 떠오릅니다. 작업 증명 방식에서는 이중 지불(Double Spending)의 가능성을 배제하게 되는데요. 예컨대 잔고에 100원이 있을 때 200원을 결제할 수 없듯이, 복제 증명에서는 100 MB 라는 저장소에 200 MB를 이중 복제할 수 없게(Deduplicate) 됩니다.

- 시공간 증명 (PoSt : Proof of Spacetime)

시공간 증명 방식은 유저에게 특정 서버가 spacetime(어느 정도 사용된 스토리지를 의미) 자원을 이미 소비했음을 입증한다. 시공간 증명 방식은 공간 증명 방식(Proof-of-Space)이 시간이 지나면서 여러번 확인된 '결과물'로 볼 수 있다. 유용한 시공간 증명방식이라면, 스토리지 서비스가 활용 가능해짐에 따라 작업 증명(PoW) 방식을 대체할 수

있다. 시공간 증명 방식은 연속적인 복제 증명 방식(PoRep)과 함께 활용될 수 있다.
공간증명에 대한 부연 설명 (원문) : *Proof-of-Space* schemes allow a user to outsource the storage of data D to a server P and then repeatedly check if P is still storing D.
리서치하면서 가장 이해하기 까다로웠던 개념이 바로 이 '시공간 증명'이라는 방식이었습니다. 이 세상엔 정말 다양한 컨센서스 방식이 있음을 깨달았던 리서치 과정이었던 것 같네요.. 그래도 쉽게 풀어보자면, 이 시공간(spacetime) 증명 방식이라는 것은 기존의 공간 증명 방식(Proof-of-Space)에서 좀 더 나아간 개념이라고 생각하시면 됩니다. spacetime은 공간 증명 방식 내에서 이미 꽤 사용된 스토리지를 의미한다고 합니다.
작업증명 방식을 대체할 수 있다는 말은 아마도 작업 증명에서의 채굴 과정에서 파생되는 데이터 저장의 비효율성을 타겟팅한 것 같네요.
글을 쓰면서도 약간 추상적인 느낌을 지울 수 없어서, 시공간 증명 방식을 파생시키는 공간 증명 방식(Proof-of-Space)에 대해 조금 더 구체적으로 설명된 링크를 첨부합니다.
https://en.wikipedia.org/wiki/Proof-of-space

---

## Conclusion

여기까지가 Filecoin에 대한 간단한 소개였습니다. Filecoin에서의 스마트 컨트랙트 등 더 소개하고 싶은 내용들이 많지만, 한 주제를 디테일하게 뜯어보기엔 포스팅 길이를 너무 길게 할 수는 없을 것 같아 이번 포스팅에서는 간략한 소개에 그쳐야 할 것 같습니다. 개인적으로 Filecoin의 구동 방식에 대해 자세히 논하지 못한 것이 약간 아쉽긴 하네요. 리서치팀에서 맡은 첫번째 포스팅인지라 많이 미숙하지만

앞으로 더 구체적이고 쉬운 방식으로 다양한 알트코인을 소개드리도록 하겠습니다. 다음 시간에는 암호화폐의 '가치 안정화'를 위해 고안된 Stable Coin에 대해 알아보도록 하겠습니다 :)