

중학생도 만드는 IPFS DAPP 튜토리얼

한우영
(GoldenTime Blockchain Developer)



안녕하세요! 이번에 중학생도 만드는 IPFS Dapp 튜토리얼 이라는 주제로 이야기하게된 한 우 영 입니다 :)

사실 여담으로 먼저 시작하자면, 제목을 조금 잘못정했어요... ㅎㅎ

20분정도인줄 모르고 진짜 튜토리얼형으로 해볼까 생각하다가 20분이라길래.. 살짝 전향해서 IPFS 소개 + 시연 정도로..진행을 할 예정입니다.

00. 발표자 소개



한우영 (@hanukoon)

010-9719-6521
hwymaster01@hanukoon.com

- 부산에서 온 자퇴생 -> 굳이 나이로 따지면 중3
- **GoldenTime BlockChain Developer**
- 대구대학교 정보보호영재교육원 6기 해킹추적과정
- **Blockpaper (전자 계약서 작성을 위한 이더리움 DAPP) 개발**
- **BlockChain(Klaytn) 기반의 IOT 펌웨어 보안 솔루션 개발**
- 기타등등..?
- Digital Forensic, Pwnable / Flask, Node, Blockchain, C#
- <https://github.com/cokia>



제 소개를 간단하게 하자면,
자퇴를 해서 굳이 나이로 따지면 중3인 학생입니다 :)
골든타임이란 스타트업에서 블록체인 개발을 담당하고 있고,
하고싶은게 무진장 많은 새내기 개발자 입니다 :)



한우영 (@hanukoon)

010-9719-6521
hwymaster01@hanukoon.com

하고싶은게 무진장 많은, 새내기 개발자(?)



제 소개를 간단하게 하자면,
자퇴를 해서 굳이 나이로 따지면 중3인 학생입니다 :)
골든타임이란 스타트업에서 블록체인 개발을 담당하고 있고,
하고싶은게 무진장 많은 새내기 개발자 입니다 :)

01. IPFS 란



ipfs 가 무엇일까요? Inter Planetary File System, 즉 행성간 파일시스템의 약자 입니다.

정확히 말하면, 비트토렌트보다 발전된 형태의 “탈 중앙화 분산저장 스토리지” 입니다.

01. IPFS 란

ZONE	EVM OPCODE	GAS/WORD	GAS/KB	GAS/MB
STACK	POP	2	64	65,536
	PUSHX	3	96	98,304
	DUPX	3	96	98,304
	SWAPX	3	96	98,304
MEMORY	CALLDATACOPY	3	98	2,195,456
	CODECOPY	3	98	2,195,456
	EXTCODECOPY	3	98	2,195,456
	MLOAD	3	96	98,304
	MSTORE	3	98	2,195,456
	MSTORE8	3	98	2,195,456
STORAGE	SLOAD	200	6,400	6,553,600
	SSTORE	20,000	640,000	655,360,000



ipfs 는 왜 필요하고, 이더리움과는 무슨 연관이있을까요?

일단. 이더리움에서 1GB의 파일을 저장할때, 들어가는 비용을 계산해보면 65억 가스가 드는데, 이더로 환산하면, 6이더 상당입니다.

요새 이더리움도 올라서 31만원대 인데, 그러면...1기가를 저장하기위해 200만원을.. 쓸수는 없으니, 그 대체재로 나온게 IPFS입니다.

01. IPFS 란

 이더리움 ETH/KRW ▼

315,550 KRW

671088640000

gwei ▼

=

671.08864 ETHER



ipfs 는 왜 필요하고, 이더리움과는 무슨 연관이있을까요?

일단. 이더리움에서 1GB의 파일을 저장할때, 들어가는 비용을 계산해보면 6710억 가스가 드는데, 이더로 환산하면, 671이더 상당입니다.

요새 이더리움도 올라서 31만원대 인데, 그러면...1기가를 저장하기위해 200만원을.. 쓸수는 없으니, 그 대체재로 나온게 IPFS입니다.

01. IPFS 란

671 * 315,550 =

211,734,050

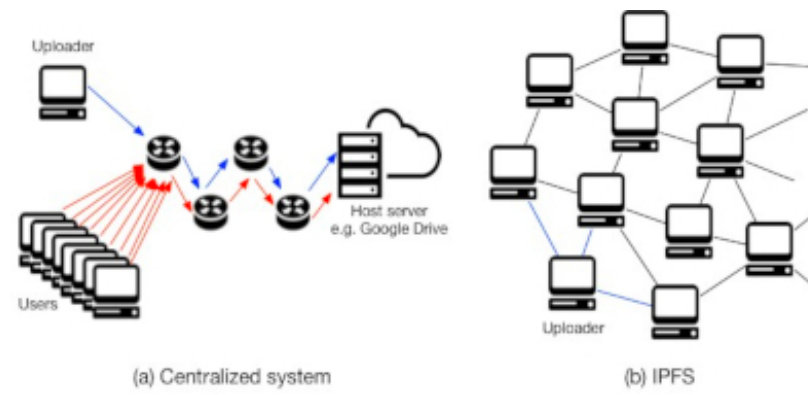


ipfs 는 왜 필요하고, 이더리움과는 무슨 연관이있을까요?

일단. 이더리움에서 1GB의 파일을 저장할때, 들어가는 비용을 계산해보면 6710억 가스가 드는데, 이더로 환산하면, 671이더 상당입니다.

요새 이더리움도 올라서 31만원대 인데, 그러면...1기가를 저장하기위해 200만원을.. 쓸수는 없으니, 그 대체재로 나온게 IPFS입니다.

01. IPFS 란

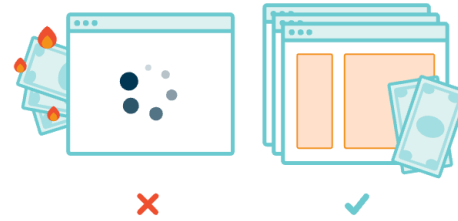


그러면, 우리가 사용하는 Centralized 시스템과, ipfs의 차이는 무엇일까요?

간단히 이야기하자면, ipfs는 탈 중앙화된 웹, http는 중앙화된 웹입니다.



01. IPFS 란



HTTP is inefficient and expensive

Luis Fonsi - Despacito

조회수 6,214,203,492회

Youtube HD (1080p25 = 8 Mbps)

300 MB



IPFS 특징 4가지가 있는데요 (http 와 차별점)

데스파시토 라는 유튜브 최다 뷰를 찍은 비디오를 예로 들었을때 250초 가량의 1080p 영상일때 용량이 300mb 정도 되는데, 62억 뷰로 계산할때, 1,864.26PB 라는 어마무시한 양의 데이터가 전송 된 것 입니다.

1,864,260,000(18억기가바이트 정도)인데, 1기가당 100원 정도가 든다고 가정하더라도, 1800억원이 파일 분배에 소모되었다는...

01. IPFS 란



Humanity's history is deleted daily

Not Found

The requested URL /figererg was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache/2.2.34 (Unix) mod_ssl/2.2.34 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 Server at www.YourURL.com Port 80

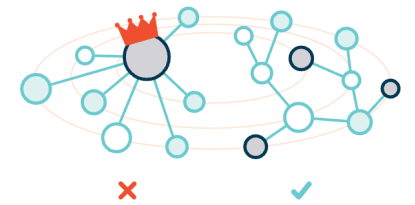


인류 역사는 꾸준히 사라지고, IPFS는 그것에 대한 대안이 될수있습니다.

밑에있는 사진처럼 구글링을 하다보면, 404 Not Found 가 뜨는 사이트가 꽤 많이 보입니다. 이런 자료들은, 서버가 죽었던지, 운영비가 없어서 망했던지 두경우가 많은데 http로 500년 뒤까지 역사를 전할 수 있을까요?

그런 해답을, IPFS가 제시하고 있습니다.

01. IPFS 란



The web's centralization limits opportunity



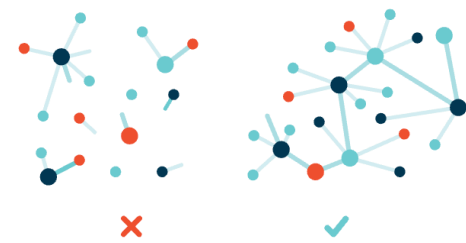
웹은 고도로 중앙화 되어있습니다.

소수의 서비스에 매우 의존하고 있고, NSA 혹은 우리나라의 국정원은 이제 몇 개의 서버만으로 우리를 철저하게 감시할 수 있습니다

또한 중앙화된 서버는 또한 DDoS공격이 성공할 경우 치명적인 결과를 더욱 큰 피해를 야기할 수 있습니다

그리고, Web이 분산화된다면, 큰 기관 하나 무너지더라도 수많은 데이터가 유실되는 경우를 방지할 수 있을 것입니다.

01. IPFS 란



Our apps are addicted to the backbone



웹의 백본 의존도는 너무 높습니다.

특정 서버의 데이터를 얻기 위해서는 반드시 그 서버와 연결되어 있어야 합니다. 인터넷 연결이 끊어지는 상황이 발생하면(예를 들어, 개발도상국의 통신선 미비, 자연재해로 인한 유실 등) 해당 서버에 접근할 수 없기 때문에 원하는 데이터를 얻을 수 없습니다.

예를 들면 최근에 KT 아현지사가 화재로 마비되었을때, 부산에 있던 저도 카드결제를 못했고, 스타벅스와 몇몇 금융권을 제외한 대부분의 곳에서 인터넷이 마비되었습니다.

01. IPFS 란

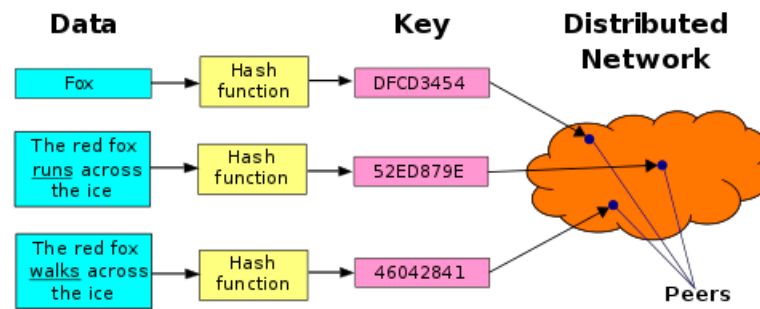
1. Distributed Hash Tables(DHT) - Routing

2. Bittorrent - File exchange



IPFS 를 구성하는 3가지 대표 요소입니다.

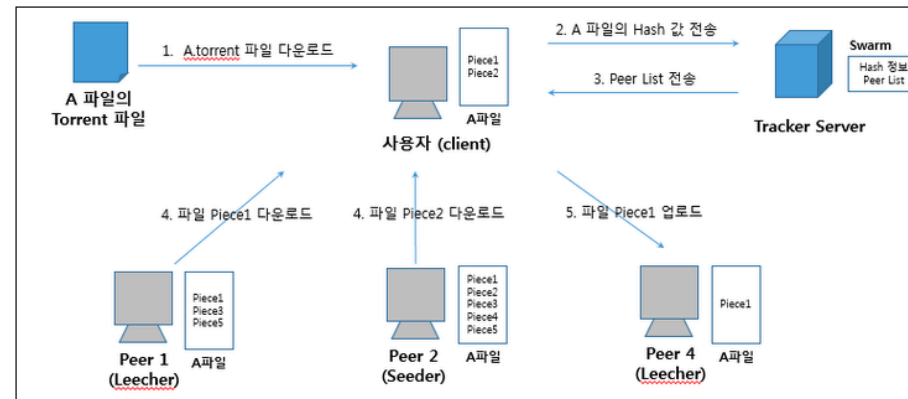
1. Distributed Hash Tables(DHT) - Routing



분산 해시 테이블(Distributed hash table, DHT) 기술은 네트워크에 참여한 노드들이 해시 테이블을 각자 관리하므로써 중앙화된 서버 없이 고도의 P2P 네트워크를 실현할 수 있게 만들어줍니다.

파이썬의 dictionary 와 비슷합니다.

2. Bittorrent - File exchange



비트토렌트는 꽤 유-명한 P2P 파일공유 기술인데요, Tracker Server 라는 DHT 역할을 하는 중앙화된 서버 와 클라이언트가 통신해 Peer 라는 다운로더 정보를 받고, 서로 필요한 조각을 부분부분 받는 방식입니다.

IPFS 에서는 비트토렌트에서 영감을 받아 비트스왑이라는 기술을 사용하는데, 노드들이 받기만 하려고하고 줄 생각이 없다면 문제가 되겠죠. 이를 해결하기 위해 BitSwap는 기본적으로 물물교환 시스템을 기반합니다. 무언가 받기 위해서는 무언가 주어야합니다. 줄수있는게 없는 노드가 있다면,그 노드는 열심히 일해서 굉장히 희귀한 파일블록이라도 얻어서 보유해놓아야 합니다- 이는 희귀한 파일블록들이 더욱 배포, 확산되는 효과를 낳습니다.

Tutorial

ipfs.cloudus.io
bit.ly/ethconipfs



링크가 두개 있는데요, 일단 첫번째 링크부터 한번 들어가 보겠습니다.

혹시 노트북으로 들어가보실분은 꼭 메타마스크를 먼저 언락하고 들어가주세요!!(롭스텐 네트워크 기반입니다)

두번째 링크는 IPFS 노드 설치 , 데몬 실행, 파일 업로드, 다운로드 를 하는 명령어들을 정리해놓은 문서입니다 :)

Tutorial

```
const IPFS = require('ipfs-api');  
/* infura 사용 */  
const ipfs = new IPFS({ host: 'ipfs.infura.io', port: 5001, protocol: 'https' });
```

```
await ipfs.add(this.state.buffer, (err, ipfsHash) => {  
  console.log(err, ipfsHash);  
  this.setState({ ipfsHash: ipfsHash[0].hash });  
});
```

```
ipfs.get(this.state.cid, (err, files) => {  
  files.forEach((file) => {  
    console.log(file.path)  
    this.createAndDownloadBlobFile(file.content, this.state.cid);  
  });  
});
```



아까 첫번째 링크에 있던 그 홈페이지의 일부 구성입니다.

제가 React.js 로 한 거의 첫번째 프로젝트라 Eth-ipfs 라는 프로젝트에서 틀을 따오고, 다운로드 기능을 추가하고 코드를 조금 다듬었습니다..

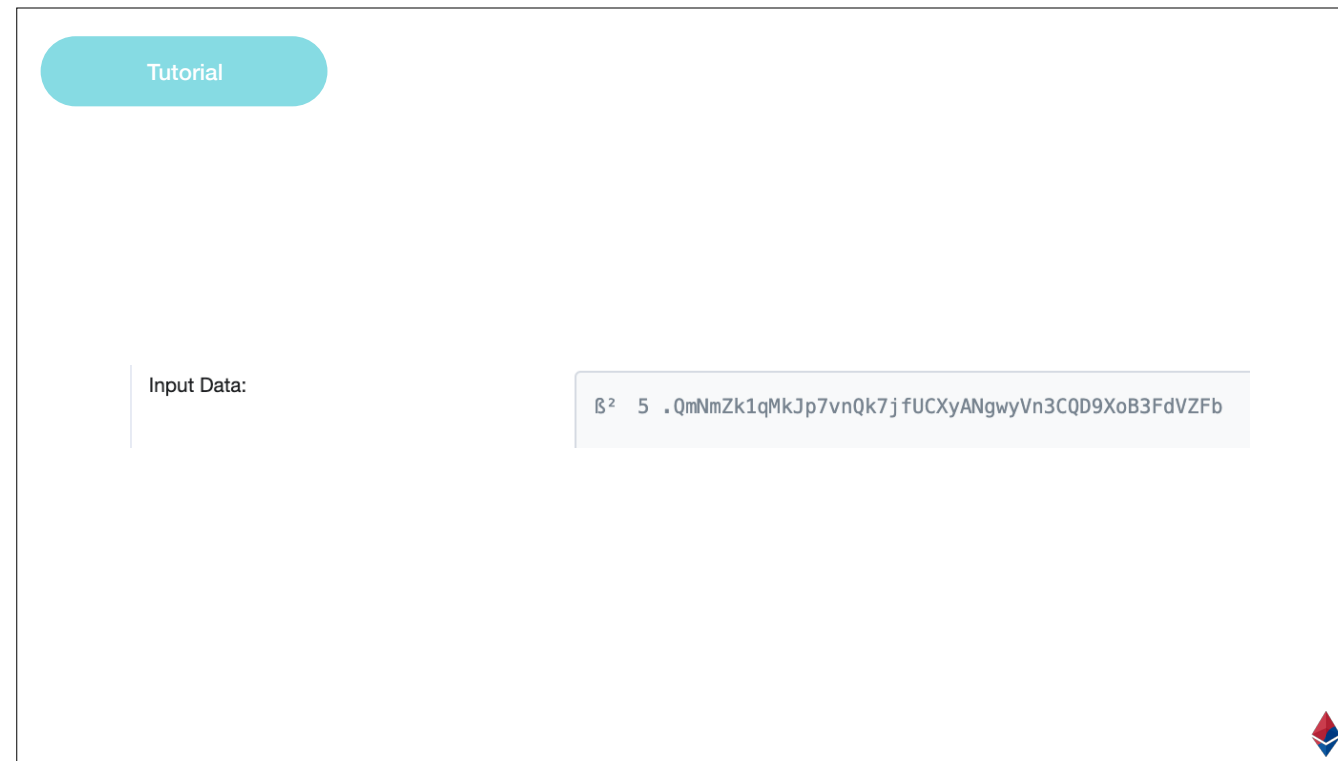
그중 일부만 캡처를 한것인데, JS에서 ifps-api를 불러오고, infura 라는 공용 노드를 사용해서, ipfs.add 라는 함수와, ipfs.get 이라는 함수로 string 형태로 파일 데이터를 가져오고, 그것을 파일로 재구성 했습니다.

Tutorial

```
contract Contract {  
    string ipfsHash;  
  
    function sendHash(string x) public {  
        ipfsHash = x;  
    }  
  
    function getHash() public view returns (string x) {  
        return ipfsHash;  
    }  
}
```



이부분은 이더리움 연동부분인데요, ipfs에 1기가의 파일을 올리든, 100기가의 파일을 올리든 Qm으로 시작하는 해시가 생기고, 그 해시만 이더리움에 저장한다면, 파일을 저렴한 가격에 보존할 수 있습니다.



이부분은 이더리움 연동부분인데요, ipfs에 1기가의 파일을 올리든, 100기가의 파일을 올리든 Qm으로 시작하는 해시가 생기고, 그 해시만 이더리움에 저장한다면, 파일을 저렴한 가격에 보존할 수 있습니다.

TXT

ipfs

dnslink=/ipfs/QmZpAMcBXmtKC7iCxe4aCTi1...

1.IPFS 는 ENS 같이 DNS 시스템이 없나요?

A: (ex: /ipns/ipfs.hanukoon.com)

```
h4nuko0n@MacBook-Pro-3 ~  
ipfs cat /ipns/ipfs.hanukoon.com
```



2.데이터 안정성 보장은 어떻게..?

A: Pin 기능을 활용!

```
h4nuko0n@MacBook-Pro-3 ~  
ipfs pin add /ipns/ipfs.hanukoon.com  
pinned QmZpAMcBXmtKC7iCxe4aCTi1MVDuV5x1cKpTFa9APq1nq2 recursively
```



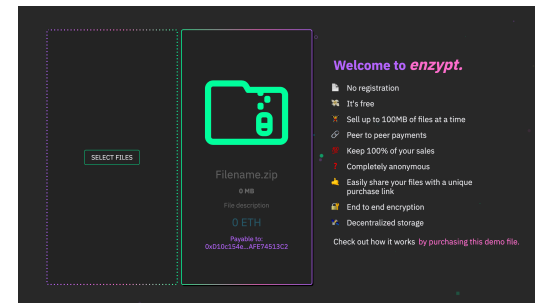
3. 왜 해시는 QM으로 시작하나요?

A : SHA256 + Base58-btc 로 인코딩..!



radicle^{alpha}

*A peer-to-peer stack for code
collaboration*



eternum

Welcome to Eternum

Eternum is an [IPFS](#) pinning service that aims to be simple and easy to use. It will host your IPFS files so you can be sure that they'll always be available, and it comes with an [API](#) that you can use in your applications.

The service costs [around](#) \$0.14 per gigabyte per month.

To sign up (or log in), just enter your email address below and click the link we send you:



IPFS를 활용한 몇가지 서비스 입니다.

감사합니다 :)



Q&A

hanu@cloudus.dev
010-9719-6521



Special Thanks to Daniel



감사합니다..!