

INTER PLANETARNI PODATKOVNI SUSTAV - IMPLEMENTACIJA I PRIMJENE

INTER PLANETARY FILE SYSTEM - IMPLEMENTATION AND APPLICATIONS

Mario Kamenjak¹, Gordan Davidović²

¹Tehničko veleučilište u Zagrebu, Zagreb, Hrvatska, Student

²Tehničko veleučilište u Zagrebu, Zagreb, Hrvatska

Sažetak

IPFS je peer to peer distribuirani podatkovni sustav kojemu je cilj spojiti sva računala u jedan podatkovni sustav. Da bi to ostvario koristi koncepte uzete iz Git-a i Bittorrenta. U poglavlju implementacije IPFS-a će se razjasniti korištene funkcionalnosti IPFS-a, neke podatkovne strukture i korištene druge tehnologije. U poglavlju problematike današnjeg weba će se razjasniti detaljno neki problemi koje IPFS pokušava riješiti, i način kako ih rješava. U poglavlju primjene se objašnjava kako IPFS instalirati na razne platforme, ali isto tako se pokazuju određena već postojeća programska rješenja za IPFS. Ovaj rad analizira implementaciju IPFS-a, objašnjava probleme koje IPFS svojom primjenom nastoji prevladati. Pregledava već postojeće aplikacije koje koriste IPFS i predlaže smjerove za daljnje radove i istraživanja.

Ključne riječi: *IPFS, Web, Internet, peer to peer, protokol*

Abstract

IPFS is a distributed file system which has a goal to connect all computers into one file system. To achieve that it is using concepts taken from Git and Bittorrent. In the IPFS implementation section it will be talked about how IPFS functions, which data structures it uses and which other technologies it uses. In the problematics of today's web section some problems will be shown that IPFS is trying to fix, and how it fixes them. In the application section it will be shown how to install IPFS on different platforms and some already existing IPFS programs will be shown.

This paper analyzes the IPFS implementation, it explains the problems that IPFS is trying to solve with its own application. It looks at already existing applications that use IPFS and it suggests directions for future papers and research.

Keywords: *IPFS, Web, Internet, peer to peer, protocol*

1. Uvod

1. Introduction

Bilo je mnogo pokušaja u konstruiranju globalnog distribuiranog podatkovnog sustava. Neki su bili uspješni, a neki neuspješni. Jedan od uspješnijih akademskih pokušaja je Andrew file system (AFS). Izvan akademije su najveći uspjeh imali sustavi orijentirani prema dijeljenju velikih datoteka poput BitTorrenta, KazaA, Napstera i sl. Međutim nijedan od istih nije dizajniran kao infrastruktura na koju se može nadograđivati. Iako postoje slučajevi uspješnog prenamjenjivanja, iz njih nije nastao podatkovni sustav opće namjene sa globalnom i decentraliziranom namjenom. Do sada je u industriji Hypertext Transfer protokol (HTTP) uglavnom bio zadovoljavajuć zato jer je premještanje malih datoteka jednostavno i jeftino. Međutim dolazimo u eru video streamanja visokih i super visokih definicija, eru petabytea podataka, 'big data' analiza unutar više organizacija, verzioniranja i sprječavanja slučajnog gubljenja podataka. Bez prihvaćanja novijih tehnika distribucije podataka, korištenje HTTP u te svrhe stvara velike troškove korisnicima Internet Service Provider (ISP) usluga i veliko opterećenje na infrastrukturu.

Veliki izvor ideja za IPFS je bio Git sustav kontrole verzioniranja koji omogućuje efikasnu distribuciju podataka, međutim za distribuirane podatkovne sustave najkorisniji je koncept Merkle Dyrected Acyclic Grafa(DAG) podatkovnog modela proizašao iz Git-a koji omogućuje snažne strategije distribucije podataka. Središnja ideja IPFS-a je da modelira sve podatke kao dio istog Merkle DAG-a[1]. Također vezano za IPFS, na Internetu postoji velika opasnost da se radi odumiranja tehnologije dogodi tzv. 'Digitalno tamno doba'. Odumiranjem web tehnologija, postoji strah da bi mnoge stranice mogle postati nečitljive, ne samo odumiranjem web tehnologija nego i odumiranjem samih stranica. IPFS želi biti građevni blok budućeg permanentnog Interneta kojemu je cilj spriječiti odumiranje digitalnih podataka[2][3].

Drugi problem koji IPFS pokušava riješiti je problem nepotrebne višestruke distribucije velike količine podataka. Taj problem predstavlja veliko opterećenje na infrastrukturu ali i na propusnost mreže korisnika. Taj problem se idealno opisuje situacijom, ako je jedno računalo u Local Area Network (LAN) mreži preuzelo video sa Interneta, i drugo računalo u istoj LAN mreži želi skinuti isti video, zašto drugo računalo ne bi preuzelo video sa prvog računala umjesto da ga skida sa udaljenog servera[4]. IPFS iako je mlad protokol koji je prvi puta spomenut tek 2014, već sada ima mnoge aplikacije. Npr. već sada postoji dodatak za Firefox koji omogućuje pregledavanje interenta preko IPFS-a. Također postoji i eksperimentalni preglednik za IPFS, pa i IPFS tražilica[5].

Ovaj članak opisuje IPFS i njegovu implementaciju u drugom poglavlju, problematiku kojom se bavi u trećem poglavlju i u četvrtom poglavlju opisuje neke već postojeće IPFS aplikacije ali i pokazuje proces instalacije IPFS-a čitatelju.

2. Implementacija IPFS-a

2. IPFS implementation

IPFS uzima mnoge ideje od već postojećih tehnologija, prvenstveno git-a i bittorrenta, međutim one ne čine potpuni dizajn IPFS-a. Tu je još i IPNS koji je samo certificirajući, potpomaže

Domain Name System(DNS) sustavu i prevodi Uniform Resource Locator(URL) u ljudima čitljiva imena[1].

Distribuirane Hash Tablice(DHT) se koriste da bi se koordinirali i održavali metapodaci o peer to peer računalnim sustavima. IPFS koristi S/Kademlia DHT, koji je nadogradnja na Kademlia DHT. Kademlia DHT se također koristi u BitTorrent protokolu i može efikasno pretraživati velike računalne mreže.

U IPFS-u čvorovi se identificiraju sa hash-om javnog ključa koji je kreiran pomoću S/Kademlia. Čvorovi spremaju svoj javni i privatni ključ. Korisnici smiju pri svakom novom povezivanju kreirati novi identitet čvora, ali time gube generiranu statistiku u mreži. Pri prvom povezivanju čvorovi izmjenjuju javne ključeve i provjeravaju hash sa identitetom čvora. Ako je ova provjera negativna veza se gasi.

Mrežni podsustav IPFS-a se sastoji od:

- **Transporta:** Može koristiti bilo koji transportni protokol.
- **Pouzdanosti:** Nudi pouzdanost ako ju niži protokoli ne nude.
- **Povezivosti**
- **Integriteta:** Opcionalno provjerava integritet poruka.
- **Autenticiteta:** Opcionalno provjerava autentičnost poruka.

IPFS može koristiti bilo koju mrežu, on ne pretpostavlja pristup Internet Protokolu.

Čvorovima je potreban sustav usmjeravanja koji može pronaći druge elemente na mreži i elemente koji mogu poslužiti točno određene objekte. IPFS to ostvaruje koristeći Dynamic Sloppy Hash Table (DSHT) baziran na S/Kademlia i Coral. Male vrijednosti su spremljene direktno u DHT a velike su referencirane u DHT-u[1].

Unutar IPFS-a razmjena podataka se događa razmjenom blokova pomoću protokola inspiriranog BitTorrent-om, sa nazivom BitSwap. Za razliku od BitTorrenta, BitSwap nije ograničen na blokove u samo jednom torrentu. BitSwap radi kao stalno tržište gdje čvorovi mogu pronaći blokove podataka koji su im potrebni, a blokovi mogu doći i iz sasvim nepovezanih datoteka u podatkovnom sustavu.

Sustav također mora poticati čvorove na to da dijele podatke koje imaju, ali i da očuva rjeđe podatkovne blokove. To znači da će čvorovi češće spremati rjeđe podatkovne blokove u pred-memoriju. Poticanje na dijeljenje podataka se ostvaruje sa BitSwap kreditnim sustavom. Uspostavljaju se pouzdani i nepouzdan čvorovi što se tiče razmjene podataka. To onemogućuje Sybill napade, štiti uspješne veze i usporava loše veze dok se ne poprave.

DHT i BitSwap omogućuju IPFS-u da formira peer to peer sustav za spremanje i distribuciju blokova na brzi način. Povrh njih IPFS gradi Merkle DAG koji omogućuje:

- Adresiranje sadržaja
- Otpornost na neovlašteno manipuliranje
- Deduplikaciju

U IPFS-u putanje rade na isti način kao UNIX putanje i može se njima putovati sa string Application Programming Interfaceom(API). IPFS putanje se mogu montirati u postojeće podatkovne sustave bez konflikta. Drugi dio IPFS putanja se obično sastoji od hash rezultata objekata. IPFS klijentima je potrebno i nešto lokalnog spremišta sa kojeg su dostupni lokalni podaci objekata kojima upravlja IPFS. Za to može poslužiti tvrdi disk ili Random Access Memory(RAM).

Klijenti koji žele osigurati preživljavanje željenih podataka i objekata na IPFS-u to mogu ostvariti sa radnjom Object Pinning. To osigurava da će objekt ostati u lokalnoj memoriji čvora i može biti napravljeno rekurzivno čime bi se ta radnja obavila i nad djecom objekata. Upravo ova funkcionalnost IPFS obilježava kao permanentni web[1]. Podatkovni objekt commit reprezentira povijest verzija raznih objekata. Pomoću njega se mogu otkriti razlike između starijih i novijih verzija objekata. Tako dugo dok postoji jedan commit i svi objekti djeca tog commita, sve ranije verzije se mogu povratiti.

IPFS svoj podsustav za imena zove IPNS. On je ostvaren tako da je napravljen nepromjenjivi Merkle DAG. Time su objekti na određeni način u IPFS-u stalni. Adresiranje sadržaja korišteno u IPFS-u zahtijeva optimizaciju propusnosti, nepovjerljivo serviranje sadržaja, stalne poveznice i mogućnost kreiranja punih stalnih backupa objekta.

IPNS se sastoji od samo-certificirajućih imenskih prostora. Na IPNS se nadgrađuje i sustav za ljudima čitljiva imena, jer hash vrijednosti nisu lagano čitljive[1].

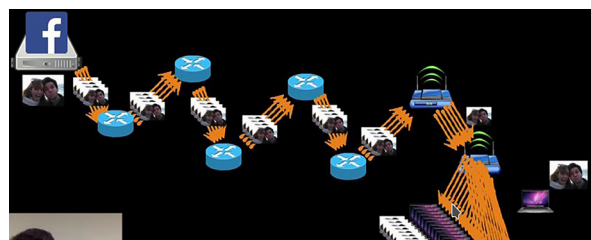
Postoje planovi za uvođenje sustava signaliziranja koji će biti povrh IPNS podsustava. Time će se omogućiti prenošenje dinamičkih web stranica i sadržaja preko IPFS-a. To će se ostvariti pomoću signaliziranja preko usmjerničkog podsustava i pomoću distribuiranog agenta[6].

3. Problematika današnjeg web-a

3. The problematics of today's web

Današnji HTTP protokol radi na drugačijim principima u odnosu na IPFS. Prvenstvena konceptualna razlika je u tome da http koristi lokacijsko adresiranje, za razliku od IPFS-a koji koristi sadržajno adresiranje[4].

Kod lokacijskog adresiranja svaki sadržaj dobiva adresu na osnovu svoje lokacije. Ako se taj sadržaj pomakne ili kopira na drugu lokaciju, HTTP sa lokacijskim adresiranjem ga tretira kao drugi sadržaj. To je uzrok velikog opterećenja na infrastrukturu ali i uzrok velike latencije. Uzrok latencije leži u činjenici da su poslužitelji koji nude podatke često fizički vrlo udaljeni od klijenta. Međutim postavlja se pitanje, ako je drugi klijent fizički vrlo blizu prvom klijentu već ranije preuzeo isti sadržaj sa web-a, zašto se ne bi smanjila latencija tako da prvi klijent preuzme taj isti sadržaj ali ne sa poslužitelja nego sa računala prvog klijenta.



Ilustracija 1: Mrežno opterećenje višestrukim skidanjem istog sadržaja[4]

Illustration 1: Network load of downloading the same content

IPFS sa svojim sadržajnim adresiranjem radi upravo to. Spaja klijente u jednakopravne peer-ove i kada više peer-ova ima traženi sadržaj, IPFS će uzeti sadržaj sa njih nekoliko najbližih. Time se smanjuje latencija i povećava brzina mreže uz smanjenje opterećenja na infrastrukturu.



Ilustracija 2: Centralizirani kolaborativni web servis[4]

Illustration 2: Centralized collaborative web service

Zatim postoji problem mrežnih grešaka rada u modernim kolaborativnim web aplikacijama. Većina aplikacija je trenutno napravljena na centraliziranoj server klijent arhitekturi. To znači da je za prekid rada dovoljan prekid veze bilo gdje na relaciji klijent-server. Čak i ako su svi klijenti povezani na istu LAN mrežu, ako je veza sa udaljenim poslužiteljem prekinuta, kolaboracija ne može nastaviti. IPFS bi sa svojom peer to peer distribuiranom arhitekturom omogućio distribuirane web aplikacije koje bi omogućile kolaborativni rad bez potrebe za centralnim poslužiteljem. Time bi se kolaboracija mogla nastaviti čak i uz određene smetnje u samoj mrežnoj infrastrukturi. Moglo bi se argumentirati da bi to sve zajedno, iako manje troši korisnikov bandwidth, više trošilo korisnikov tvrdi disk. Ali ispostavlja se da cijena tvrdih diskova brže pada od cijene propusnosti mreže[4].

Postoji još i problem tzv. digitalnog tamnog doba. Digitalno tamno doba je problem u kojem bi u bližoj budućnosti mnogi digitalni podaci mogli postati ili već jesu postali nedostupni. Najčešći razlog tome je taj da su tehnologije spremanja podataka zastarjele ili jednostavno nestajanje podataka[7].

Mnogi digitalni podaci već jesu izgubljeni, npr. 1990-ih su mnogi National Aeronautics and Space Administration (NASA) znanstvenici naišli na problem kada su njihovi zapisi iz 1960-ih i 1970-ih bili na medijima koji su bili ne čitljivi radi kvara na stroju za čitanje istih medija i radi toga da takav stroj više nije bio u prodaji. Za neke podatke su onda pokrenuli proces digitalne arheologije i reverznim inženjeringom su iščitavali podatke sa medija[8].

Mnogi podatci se kasnije mogu trajno sačuvati emulacijom tehnologije. Postavlja pitanje gdje će se trajno pohraniti emulatori. IPFS pokušava biti tehnologija na kojoj bi se emulatori mogli sigurno pohranjivati.



Ilustracija 3: Kapacitet diska i bandwidth[4]

Illustration 3: Disk capacity and bandwidth

Izuzev toga, sadržajno adresiranje koje predstavlja novi način adresiranja koje se koristi u IPFS-u, zajedno sa peer to peer arhitekturom želi spriječiti odumiranje poveznica, a time i odumiranje sadržaja tj. znanja i informacija pohranjenih na njima[4].

4. Primjene

4. Applications

Što se tiče implementacije web servisa i aplikacija na IPFS-u, dodatno istraživanje bi trebalo biti izvršeno oko toga kako implementirati neke već danas postojeće koncepte web servisa ali na distribuiranom IPFS-u. Npr. kako na IPFS-u implementirati dinamički sadržaj i druge servise poput npr. IPFS tražilica. Sve to ukazuje na to da je implementacija distribuiranih web servisa drugačija od tradicionalnih web servisa[6][9].

Sa druge strane servisi statičke prirode kao servisi za raspodjelu slikovnih i video datoteka već postoje[10][11].

4.1 Instalacija IPFS-a na Linux okruženju

4.1 Instalacija IPFS-a na Linux okruženju

Na Linux operacijskom sustavu se IPFS podrška može instalirati tako da se preuzme odgovarajući paket sa službene stranice. Zatim se taj paket treba raspakirati u novi direktorij. Treba se ući u novi direktorij i pokrenuti skriptu za instalaciju sa administratorovim privilegijama[12]:

```
sudo ./install.sh
```

Ili se nakon raspakiranja instalira sa naredbom:
`sudo mv go-ipfs/ipfs /usr/local/bin/ipfs`

Slijedeći korak je da se IPFS inicijalizira. U ovom koraku se kreira i IPFS repozitorij, sa naredbom:
`ipfs init`

Zadnji korak je spajanje na IPFS protokol. Spajanje na IPFS protokol se radi naredbom:
`ipfs daemon`

Nakon toga računalo je priključeno na IPFS. Provjera konekcije i lista spojenih čvorova se može dobiti sa naredbom:
`ipfs swarm peers`

4.2 Instalacija IPFS-a na Windows okruženju

4.2 Instalacija IPFS-a na Windows okruženju

IPFS se može instalirati i na Windows operacijskim sustavima. Da bi se IPFS instalirao na windowse prvo se mora preuzeti paket za windowse sa službenih stranica. Zatim se taj paket mora raspakirati.



```
zma@dunee-chan:~$ ipfs cat /ipfs/QmYwAPJz5CZsnA625s3kTznmetygpHdWEZ/90JWnFbdo/readme
Hello and Welcome to IPFS!

IPFS

If you're seeing this, you have successfully installed
IPFS and are now interfacing with the ipfs merkledag!

-----
Warning:
  This is alpha software. Use at your own discretion!
  Much is missing or lacking polish. There are bugs.
  Not yet secure. Read the security notes for more.
-----

Check out some of the other files in this directory:
./about
./help
./quick-start  <-- usage examples
./readme      <-- this file
./security-notes
```

Ilustracija 4: IPFS pozdravna poruka

Illustration 4: IPFS welcome message

IPFS.exe se treba kopirati u %PATH% direktorij Windowsa.

Slijedeći korak je inicijalizacija koju vršimo kroz command prompt naredbom:
`ipfs init`

Zadnji korak je spajanje na IPFS protokol. Spajanje na IPFS protokol se radi naredbom:
`ipfs daemon`

Nakon toga računalo je spojeno na IPFS.

Provjera konekcije i lista spojenih čvorova se može dobiti sa naredbom:
`ipfs swarm peers`

IPFS je testiran na oba operacijska sustava navedena u ovom poglavlju i na oba sustava je radio stabilno.

4.3 Aplikacije treće strane

4.3 Third party applications

IPFS search

IPFS search je eksperimentalna tražilica web stranica za IPFS. Koristi lunr.js za provođenje traženja i građenje indeksa traženja. Pretražuje naslove, tekst i URL od 11000 IPFS web stranica koje su uspješno pronađene scrape tehnikom.[5]

Akasha

Akasha je socijalna mreža slijedeće generacije pokretana sa Ethereum i IPFS projektima. Akasha je decentralizirana socijalna mreža sa ciljem imunosti na cenzuru i ciljem razošiljanja ljudskog znanja.[5]

OpenBazaar

OpenBazaar je Open source decentralizirana web trgovina. Za razliku od tradicionalnih web trgovina, gdje su web trgovine posrednik između kupca i dobavljača OpenBazaar povezuje kupca i dobavljača izravno bez posrednika. OpenBazaar isto uklanja kartičarske kuće iz novčanog posredstva tako da za valutu koristi BitCoin. Jedino gdje postoji oblik posredstva je u razrješavanju potencijalnih prijevара, gdje postoji treća strana i novčana transakcija je blokirana sve dok se barem dvije od tri strane ne slože oko razrješavanja. OpenBazaar koristi IPFS radi veće dostupnosti prodavačkih mjesta, da prodavači ne moraju stalno održavati vlastiti server[13].

5. Zaključak

5. Conclusion

U ovom članku je objašnjena implementacija IPFS-a. Opisano je kako IPFS preoblikuje web i pomoću kojih koncepata. Zatim se išlo u pitanje nekih od problematika koje IPFS rješava. U nastavku je pisano kako IPFS primijenit na različitim operacijskim sustavima u trenutnoj implementaciji, kao i neke web aplikacije napisane za IPFS.

Očekujemo da će se daljnja istraživanja provoditi oko toga kako razvijati distribuirane dinamičke web servise, jer iako postoje određene ideje oko razvitka istih, to je još uvijek jedno vrlo neistraženo područje.

Zaključno se može reći da IPFS ima vrlo zanimljiva rješenja za problematiku koju rješava. Iako je IPFS protokol tek u svojim počecima, već se kreiraju mnoge primjene za njega. IPFS ima potencijala da bude tehnologija koja će transformirati web i naš doživljaj istoga.

6. REFERENCE

6. REFERENCES

- [1] Benet J.; Cornell University; 14.07.2014; IPFS - Content Addressed, Versioned, P2P File System; ISSN arXiv:1407.3561v1
- [2] <https://www.wired.com/2016/06/inventors-Internet-trying-build-truly-permanent-web/> Finley K.; Wired; 20.06.2016; The Inventors of the Internet Are Trying to Build a Truly Permanent Web; Pristupljeno: 21.12.2016
- [3] <https://blog.neocities.org/blog/2015/09/08/its-time-for-the-distributed-web.html> Drake K.; Neocities; 08.09.2015; HTTP is obsolete. It's time for the distributed web; Pristupljeno: 21.12.2016
- [4] <https://www.youtube.com/watch?v=skMTdSEaCtA> Benet J.; Cornell University; 20.02.2015; IPFS Alpha | Why We Must Distribute The Web; Pristupljeno: 22.12.2016
- [5] <https://github.com/ipfs/awesome-ipfs> Github; Awesome-ipfs; Pristupljeno: 02.01.2017
- [6] <https://github.com/ipfs/faq/issues/28> Github; 10.09.2015; How can IPFS distribute dynamic content; Pristupljeno: 05.01.2017
- [7] Kuny T.; 27.08.1997; A digital dark ages? Challenges in the preservation of electronic information
- [8] <http://www.nytimes.com/1990/03/20/science/lost-on-earth-wealth-of-data-found-in-space.html> Blakeslee S.; The New York Times; 20.03.1990; Lost on Earth: Wealth of data found in space; Pristupljeno: 10.01.2017
- [9] <https://github.com/ipfs/archives/issues/8> Github; 29.08.2015; Search engine; Pristupljeno: 12.01.2017
- [10] <https://github.com/download13/ipfstube> Github; Ipfstube; Pristupljeno: 12.01.2017
- [11] <https://github.com/ipfspics/ipfspics-server> Github; Ipfspics-server; Pristupljeno: 19.01.2017
- [12] <https://ipfs.io/docs/install/> Ipfs.io; Install Go IPFS; Pristupljeno: 22.01.2017
- [13] <https://bitcoinmagazine.com/articles/openbazaar-integrating-interplanetary-file-system-to-help-keep-stores-open-longer-1460660998/> Torpey K.; Bitcoinmagazine; 14.04.2016; OpenBazaar Integrating InterPlanetary File System to Help Keep Stores Open Longer; Pristupljeno: 07.02.2017

AUTORI · AUTHORS

Mario Kamenjak - R: 25.1.1992, Koprivnica. 2014. godine je završio stručni studij Informatike, smjer organizacije i informatizacije ureda na Tehničkom veleučilištu u Zagrebu. 2016. godine je upisao specijalistički studij informatike, modul računarski sustavi na Tehničkom veleučilištu u Zagrebu.

Korespondencija

mkamenjak@tvz.hr

Gordan Davidović - nepromijenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 2, No. 1, 2014.

Korespondencija

gordan.davidovic@tvz.hr