FIAP ON

BLOCKCHAIN ADVANCED

WEB 3.0

HENRIQUE POYATOS

7

LISTA DE FIGURAS

SUMÁRIO

7 WEB 3.0

7.1. Armazenamento descentralizado

A proliferação de aplicações bem-sucedidas utilizando *blockchain* foi apenas o começo de novos modelos descentralizados. Vários profissionais começaram a se perguntar: “Que outros modelos centralizados poderiam ser descentralizados? ” e uma destas respostas foi o **armazenamento**.

As informações presentes na Internet geralmente estão centralizadas, armazenadas em grandes *datacenters* pertencentes à grandes corporações: Amazon (com seu AWS), Microsoft (Azure), Oracle, Google e outras gigantes do mercado.

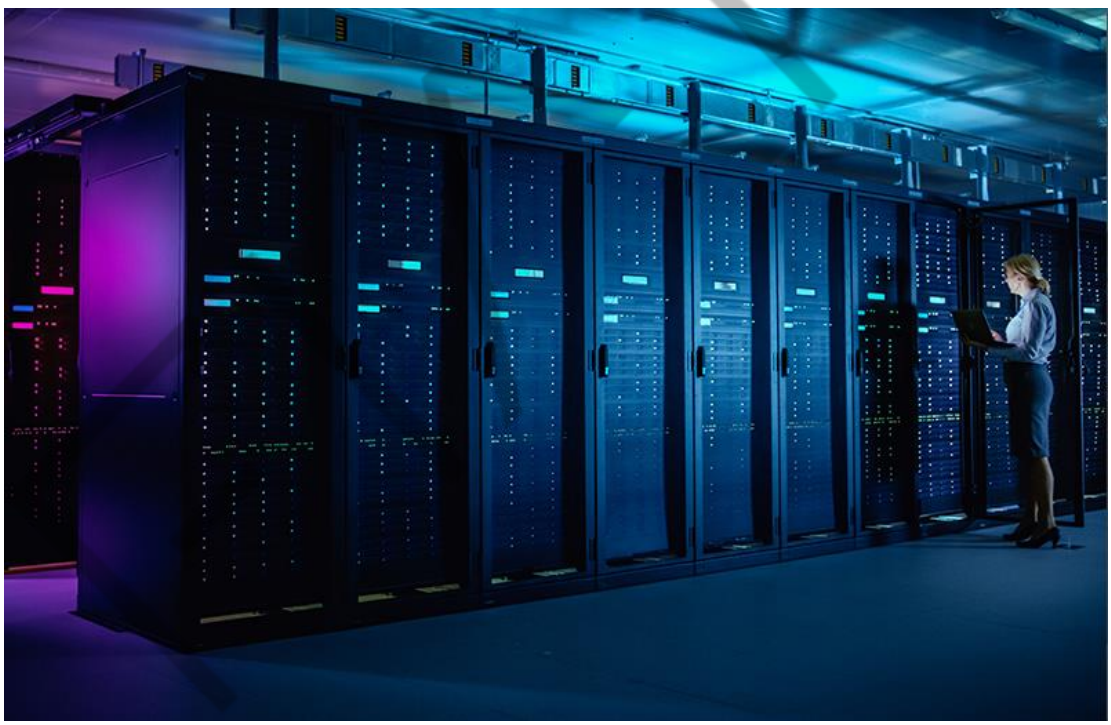

Figura 7.1 – Grande datacenter armazenamento grandes quantidades de informação
Fonte: Shutterstock (2020)

Um dos problemas do armazenamento centralizado é a **disponibilidade**: o que acontece quando um destes *datacenters* que concentra as informações de um *website* tem uma falha técnica e o serviço sai do ar? Um grande prejuízo, certamente. Segundo Tweney (2013), a Amazon.com, o site de comércio eletrônico mais frequentado do mundo saiu do ar por aproximadamente 40 minutos em agosto daquele ano, e estima-se que a empresa teve um prejuízo de quase 5 milhões em dólares em vendas não

realizadas. Em menos de uma hora! Consegue imaginar o prejuízo que aconteceria nos dias de hoje?

Além disso, o armazenamento centralizado possui outro grande problema: ele pode ser **censurado**. O fato de um determinado conteúdo estar concentrado em poucos servidores torna mais simples para governos bloquearam acesso à conteúdos indesejados. Em abril de 2017, o governo da Turquia mandou bloquear o acesso do país inteiro à Wikipédia, alegando que a enciclopédia on-line havia se recusado a tirar do ar conteúdos que alegavam que o governo turco estava patrocinando grupos terroristas como o ISIS e Al-Qaeda, e o *website* permanece bloqueado no país, dois anos depois. Desde 2014, a Turquia restringiu acesso inúmeras vezes a plataformas como Twitter, Facebook, Instagram, YouTube e WhatsApp por compartilhar informações não favoráveis ao país (OSTERLUND, 2018; SCF, 2019).

Figura 7.2 – Protesto contra a censura da Internet em Istambul
Fonte: Shutterstock (2020)

Por que utilizar um modelo centralizado, então? A principal razão é a alta expectativa que temos ao acessar a internet: queremos conteúdo rápido, em alta qualidade e com baixa latência, e em datacenters centralizados as empresas

conseguem um maior controle que como cumprir tais expectativas. Não havia outra alternativa... até agora.

O modelo de **armazenamento descentralizado** é formado por uma rede ponto-a-ponto (P2P) em que seus membros fornecem espaço em disco e compõem juntos uma memória compartilhada global.

Para entendermos como os serviços de armazenamento descentralizado funcionam, precisamos primeiramente entender como o centralizado funciona. Quando queremos baixar uma imagem (como o logo do FIAP ON) precisamos fornecer para o navegador *web* seu endereçamento exato, como "https://www.fiap.com.br/wp-content/themes/fiap2016/images/fiap/vitrines/online/logo.png". A requisição é traduzida para o endereço de IP (graças ao serviço de DNS), que solicita à um serviço *web* disponível no servidor (geralmente um servidor Apache HTTP Server) pelo arquivo logo.png, no subdiretório indicado. Se, por acaso, o servidor web presente neste endereço IP estiver indisponível, o *download* simplesmente não acontecerá, **mesmo que dezenas de pessoas tenham acessado este endereço e tenham feito cópias exatas do arquivo**. Este modelo em questão é conhecido como endereçamento baseado em localização (*Location based addressing*).

A proposta feita pelos serviços de armazenamento descentralizados é um endereçamento baseado em conteúdo (*Content based addressing*), e não em localização, assim sendo, o endereço não indica **onde** localizar o que queremos, mas **o que** nós queremos.

Cada arquivo hospedado de forma descentralizada recebe uma chave hexadecimal que o torna único na rede; quando quisermos acesso ao arquivo, basta solicitar aos nós que possui o arquivo que corresponde àquele *hash* identificador.

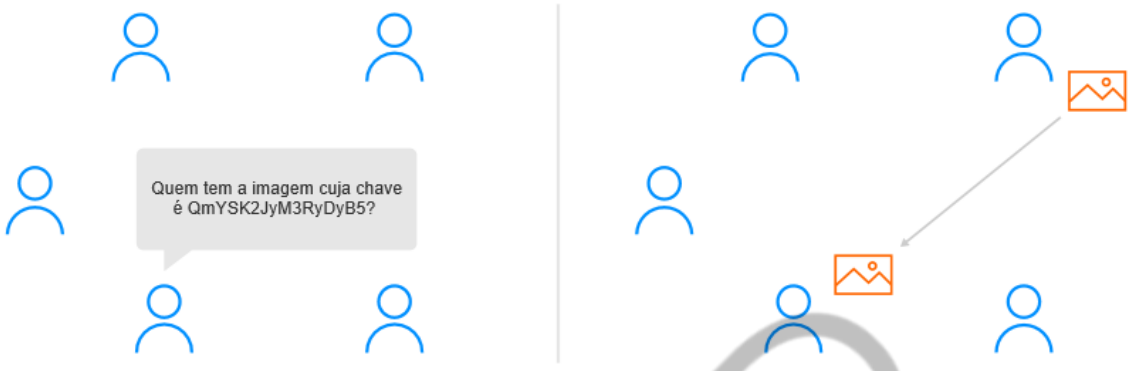

Figura 7.3 – Hash usado para identificar um arquivo
Fonte: Simply Explained (2020)

Entretanto, talvez você se pergunte: “Como terei certeza que o arquivo que estou recebendo é realmente sua versão original? Será que o nó que está me enviado não o adulterou de alguma forma?” e resposta para seu questionamento é o próprio *hash* em si, que acaba servindo como uma “assinatura digital”. Apenas a partir do arquivo original é possível gerar o *hash* em questão, pois um único bit “1” no lugar de um “0” **gerará um *hash* completamente diferente**. Sendo assim, assim que o arquivo é baixado, um *hash* para ele é gerado, os dois *hashes* são confrontados e estes devem ser exatamente iguais.

Além da segurança, o sistema a partir do *hashes* garante que o conteúdo é imutável, de forma similar a um *blockchain*. Em caso de arquivos que precisem ser alterados, os sistemas de armazenamento centralizado suportam versionamento, permitindo que os objetos sejam encadeados, assim os solicitantes terão acesso sempre à última versão do arquivo publicado.

7.1.1 InterPlanetary FileSystem (IPFS.io) + FIlECOIN (FILECOIN.IO)

O IPFS (***I**nter**P**lanetary **F**ile**S**ystem*) é uma destas soluções de armazenamento descentralizado, criado pela Protocol Labs inicialmente na linguagem Go e publicado no início de 2015. É possível instalá-lo em Windows, Mac OS X e Linux (incluindo o Raspbian, variação do Debian para o Rasperry Pi).

Figura 7.4 – Logo do IPFS
Fonte: Google Imagens (2020)

Para poder acessar o conteúdo em um navegador web, existem alguns nós que fazem o papel de *IPFS Gateways*, realizando a ponte do protocolo HTTP com os arquivos presentes no IPFS. Desta maneira, é possível hospedar websites inteiros utilizando o protocolo, descentralizado o serviço WWW.

Embora funcione muito bem, o sistema possuía um problema: Se todos os nós que possuem o arquivo estiverem *off-line*, o arquivo se torna indisponível. Para arquivos que estão publicados em um único nó, o risco se torna ainda maior (e convenhamos, não é muito diferente do modelo centralizado). Como promover a alta disponibilidade do arquivo, encorajando os nós à distribuí-lo?

Aqui entra o incentivo financeiro do **Filecoin**. Trata-se basicamente de um *blockchain* criado por cima do IPFS pela própria Protocol Labs para promover um verdadeiro mercado de armazenamento.

Digamos que você possua um espaço para armazenamento disponível. Você pode disponibilizá-lo para baixar e guardar arquivos de outros usuários, ganhando dinheiro no processo. O mecanismo de recompensa da rede o encorajará a manter os arquivos pelo maior tempo possível e, segundo Benet e colaboradores (2017), o sistema utiliza um modelo chamado *Proof of Replication* (PoRep), uma variação do *Proof of Storage*, para garantir que os arquivos foram de fato replicados. Pela replicação, os nós são recompensados com Filecoins (FIL), uma criptomoeda criada para tal que pode ser comercializada em *exchanges*, tornando-se Ethers (ETH) ou Tethers (USDT), e consequentemente uma moeda fiduciária como o real.

Quanto à requisitos de instalação, o Filecoin exige pelo menos 8GB RAM do equipamento (provavelmente por tarefas referentes a validação dos blocos), inviabilizando sua instalação em equipamento de baixo custo, como o Raspberry Pi. Já o IPFS sem o Filecoin pode ser instalado neste tipo de equipamento com resultados interessantes.

Figura 7.5 – Logo do Filecoin
Fonte: Google Imagens (2020)

O ICO (*Initial Coin Offer*) do Filecoin aconteceu entre Agosto e Setembro de 2017 e levantou 257 milhões de dólares, tornando-se o recordista em ICO's até então (HIGGINS, 2017). No início de 2019, a Multicoin, Coinbase Ventures, BlueYard Capital e Collaborative Fund investiram mais 1 milhão e meio de dólares no IPFS (DALE, 2019).

7.1.2 Sia (Sia.Tech)

O projeto SAI começou em 2013 no HackMIT e foi lançado oficialmente em 2015. Assim como o IPFS + Filecoin, o objetivo é alavancar a capacidade subutilizada de disco rígido espalhada pelo mundo e criar um mercado de armazenamento de dados mais eficiente e mais barato para as soluções atuais. Diferentemente da *dobradinha* "IPFS + Filecoin", o SIA é uma solução integrada e usa a criptomoeda Siacoin (SC) para recompensar os nós que hospedam os arquivos. Trata-se de uma criptomoeda da maior aceitação do que o Filecoin, comercializada em mais de uma dezena de *exchanges* no mundo, incluindo gigantes como a Binance, Bittrex, Huobi Global e Poloniex.

O algoritmo de consenso de seu blockchain é *Proof of Work* (PoW), utilizando seus próprios ASIC para a mineração, e utilizam mecanismos semelhantes a contratos inteligentes (chamados de *File Contracts*) para regras e requisitos de armazenamento. Seu algoritmo de *Proof of Storage* é utilizado para proteger e validar provas e contratos de arquivos na rede (TERADO, 2018). Ao dividir os papéis entre nós validadores e nós de armazenamento, possibilitam a instalação da infraestrutura de hospedagem em *hardwares* mais modestos: existem tutoriais que ensinam a instalação do SIA Daemon em Raspberry Pi usando Gentoo Linux OS 64 bits (PINODE, s.d.).

Figura 7.6 – Logo do SIA
Fonte: Google Imagens (2020)

Segundo SIA.TECH (2019), a capacidade de armazenamento da rede chega a 2 petabytes de dados espalhados em 319 nós. Em 2019, o SAI recebeu 3,25 milhões de dólares em uma rodada de investimentos da Bain Capital Ventures.

Existem aplicações que utilizando o SAI como *backend*, como o FileBase(.com), uma solução de cloud compatível com o Amazon AWS S3 e o Goobox(.io), uma espécie de *personal cloud* semelhante ao Dropbox.

7.1.3 Swarm (IPFS)

O SWARM é outro protocolo dedicado ao armazenamento descentralizado que faz parte da plataforma Ethereum, fazendo parte da tríade da web centralizada: O Ethereum para o poder de computação descentralizado, o Whisper para mensageria e o Swarm para armazenamento descentralizado (TERADO, 2018).

O desenvolvimento está um pouco atrasado no desenvolvimento se comparado às soluções anteriores, mas é uma solução que se beneficia do privilégio de poder se integrar diretamente com a rede Ethereum. Ao instalar o GETH (conforme visto em

um capítulo anterior) para o Ethereum, o Swarm já está disponível para hospedagem os arquivos.

Figura 7.7 – Logo do Swarm
Fonte: Google Imagens (2020)

7.2. Ethereum Name Service (ENS)

Inegavelmente, a Internet não seria o que é hoje sem o serviço de nomes de domínio (***D**omain **N**ame **S**ystem*, DNS). É este serviço que é responsável por traduzir endereços fáceis de decorar (como fiap.com.br) em endereços IP (*Internet Protocol*) que são efetivamente os endereços de rede que o protocolo de rede Ethernet utilizava para localizar os *hosts* de uma rede.

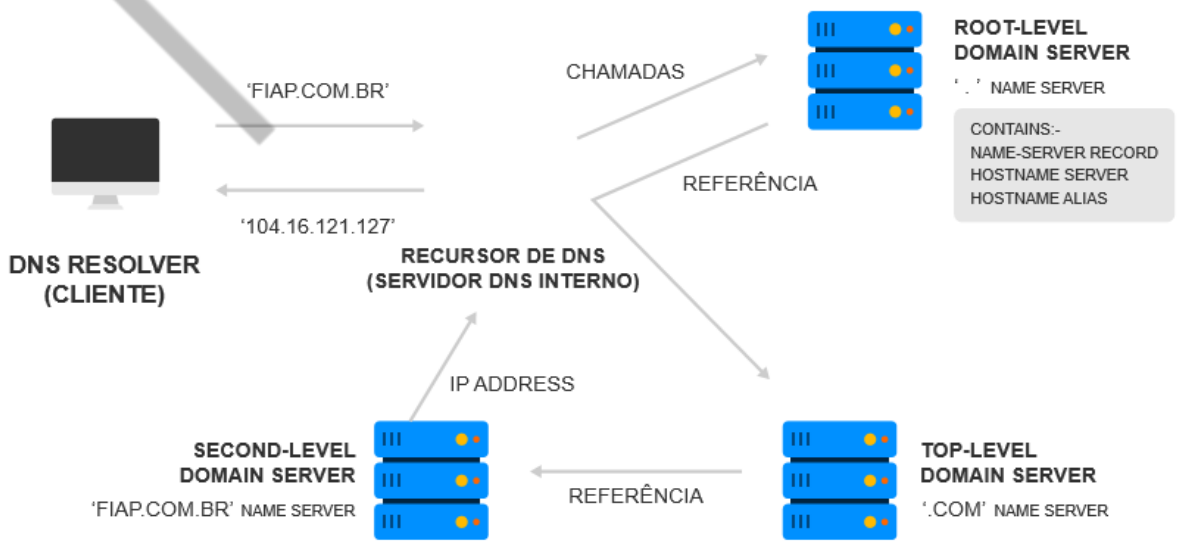

Figura 7.8 – Funcionamento do serviço DNS
Fonte: FreeCodeCamp, adaptado por FIAP (2020)

Embora sejam necessários vários servidores para resolver um nome de domínio (conforme Figura “Funcionamento do serviço DNS”), o sistema funciona com um banco de dados distribuído espalhado por vários servidores organizados hierarquicamente. Assim sendo, o processo depende de servidores que fazem o papel de recursores DNS que, na prática, centralizam as requisições das máquinas clientes (somos nós!). Por esta razão, o servidor de DNS se torna vulnerável a ataques cibernéticos do tipo *spoofing* ou negação de serviço distribuído (*Distributed Denial-of-Service*, DDoS) (IMPERVA, s.d.; CLOUDFLARE, s.d.)

Como alternativa ao serviço de DNS, o projeto Ethereum propôs o ***Ethereum Name Service*** **(ENS)**, testado inicialmente na rede de testes Ropsten, o ENS foi lançado na *mainnet* do projeto em maio de 2017.

Endereços fáceis de se lembrar (finalizados com a extensão .eth) são resolvidos em endereços de carteiras ou *smart contracts* da plataforma Ethereum, substituindo os longos e imemoriáveis *hashes* usados como identificador único, fundamental para uma adoção em grande escala no futuro.

Os endereços .ETH resolvidos pelo ENS também podem representar os *hashes* usados de arquivos presentes no armazenamento compartilhado do IFPS ou Swarm. Como arquivos HTML, CSS, JS, imagens e outros podem ser facilmente armazenados nestes serviços, na prática, é possível hospedar uma página de Internet de forma totalmente descentralizada, hospedagem e domínio.

Domínios terminados em .ETH possuem apenas um problema: eles exigem a instalação de um *plugin* no navegador que chamar o *ENS Registry* que, por sua vez, chama o *Resolver*, responsáveis pelo processo de resolução de endereço (vide Figura “Funcionamento do serviço ENS”). O *plugin* **ENS Gateway: .Eth Domain Browser for Ethereum para Google Chrome** (https://chrome.google.com/webstore/detail/ens-gateway-eth-domain-br/jkaiofboahfpipgijdgdmbdldlgcipgo?hl=en) faz este papel, embora outros *plugins* como a carteira de criptomoedas Metamask (http://metamask.io/), também possam desempenhar este papel.

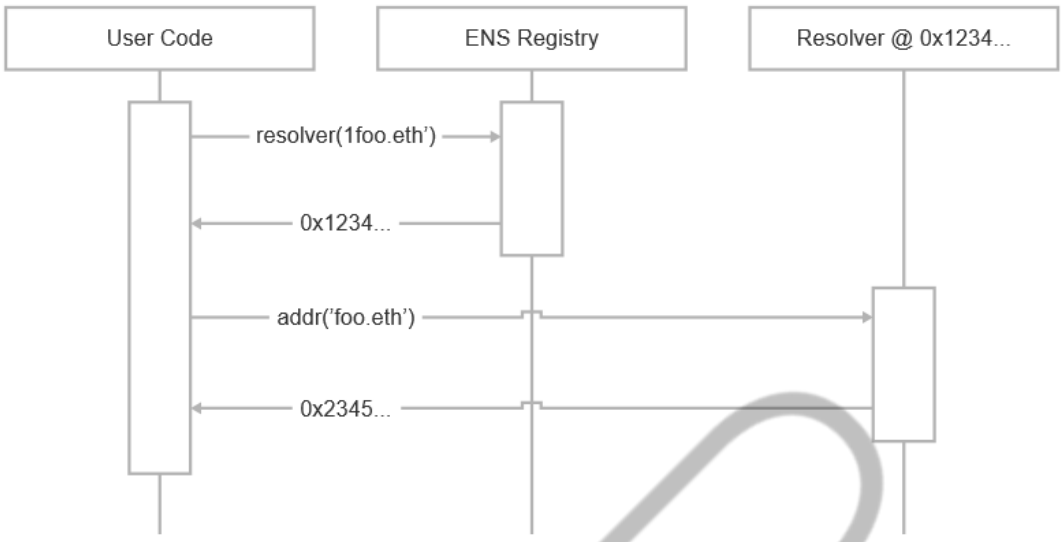

Figura 7.9 – Funcionamento do serviço ENS
Fonte: Ethereum Name Service (s.d.)

Apesar do empecilho envolvendo o *plugin*, em abril de 2019 os registros ENS chegaram a marca de 300 mil endereços .ETH registrados (KIM, 2019). Para registrar um é bem simples: basta acessar https://manager.ens.domains/ com um navegador web com uma carteira de criptomoedas embutida (a combinação usual é o Google Chrome com o *plugin* Metamask ou o navegador BRAVE) e pagar o equivalente a cinco dólares em ethers por ano pelo domínio.

O pessoal do *Ethereum Name Service* apresentou várias novidades em 2019: a criação de domínios finalizados em .XYZ que integram o serviço DNS com o ENS usando DNSSEC, dispensando a necessidade de *plug-ins* de resolução. A integração acontece de forma não-permissionada (permissionless), e smart contracts provam a posse do domínio ao serviço DNS e se encarregam de fazer a resolução aos moldes do ENS. Para conseguir este domínio, basta registrar o domínio .XYZ no ***Permanent Registrar*** do ENS (https://manager.ens.domains/) e também no serviço DNS, em qualquer servidor de hospedagem que disponibilize o serviço, integrando-os com DNSSEC após uma breve configuração.

E, por fim, um novo domínio (de extensão .LUXE) que realiza integração nativa endereço DNS-ENS! Para este tipo de domínio, basta registrá-lo no DNS e este é automaticamente disponibilizado no ENS. Para tal, basta acessar https://join.luxe/, conhecer as empresas que comercializam o domínio. A grande vantagem do .LUXE é permitir uma hospedagem web descentralizada (usando IPFS ou Swarm) mas, ao mesmo tempo, permite serviços de DNS tradicionais como servidor de e-mails.

CONCLUSÃO

Os desdobramentos da Web 3.0 têm o potencial de transformar profundamente a Internet como conhecemos. O sucesso do *Blockchain* do Bitcoin possibilitou a vários especialistas em tecnologia a repensar modelos centralizados e propôs alternativas descentralizadas viáveis.

Novas propostas estão surgindo, como o OrbitDB, um banco noSQL que funciona acima do IPFS (BULAT, 2018). Tais alternativas podem promover uma nova Internet com menos monopólios e mais privacidade e democracia.

REFERÊNCIAS

BENET, Juan; DALRYMPLE, David; GRECO, Nicola. **Proof of Replication.** 2017. Disponível em: <https://filecoin.io/proof-of-replication.pdf>. Acesso em: 22 jul. 2020.

BULAT, Ross. **OrbitDB: Deploying the Distributed IPFS Database in the Browser.** 2018. Disponível em: <https://medium.com/@rossbulat/orbitdb-deploying-the-distributed-ipfs-database-with-react-79afa1a7fabb>. Acesso em: 22 jul. 2020.

CLOUDFLARE. **What is a DNS Flood? | DNS Flood DDoS Attack.** Disponível em: < https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/>. Acesso em: 22 jul. 2020.

DALE, Brady. **Multicoin, Coinbase Ventures Invest $1.5 Million in 'Decentralized Flickr'.** 2019. Disponível em: <https://www.coindesk.com/multicoin-coinbase-ventures-invest-1-5-million-in-decentralized-flickr>. Acesso em: 22 jul. 2020.

ETHEREUM NAME SERVICE. **Introduction**. Disponível em: <https://docs.ens.domains/>. Acesso em: 22 jul. 2020.

FREECODECAMP. **An introduction to HTTP: Domain Name System servers**. 2018. Disponível em: <https://www.freecodecamp.org/news/an-introduction-to-http-domain-name-system-servers-b3e7060eca98/>. Acesso em: 22 jul. 2020.

HIGGINS, Stan. **$257 Million**: Filecoin Breaks All-Time Record for ICO Funding. 2017. Disponível em: < https://www.coindesk.com/257-million-filecoin-breaks-time-record-ico-funding>. Acesso em: 22 jul. 2020.

IMPERVA. **What is domain name system (DNS) spoofing.** Disponível em: <https://www.imperva.com/learn/application-security/dns-spoofing/>. Acesso em: 22 jul. 2020.

INOUE, Makoto. **Step by step guide of "How to claim your DNS domain on ENS".** 2018. Disponível em: < https://medium.com/the-ethereum-name-service/step-by-step-guide-of-how-to-claim-your-dns-domain-on-ens-60a2d2dcbe6e>. Acesso em: 22 jul. 2020.

JOHNSON, Nick. **EIP 137.** 2016. Disponível em: <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-137.md>. Acesso em: 22 jul. 2020.

JOHNSON, Nick. **ENS Is Upgrading — Here's What You Need to Do.** 2019. Disponível em: <https://medium.com/the-ethereum-name-service/ens-is-upgrading-heres-what-you-need-to-do-f26423339fcf>. Acesso em: 22 jul. 2020.

JOHNSON, Nick. **ENS Root Change Will Allow Easy Integration of More Than 1300 DNS TLDs.** 2019. Disponível em: <https://medium.com/the-ethereum-name-service/upcoming-changes-to-the-ens-root-a1b78fd52b38>. Acesso em: 22 jul. 2020.

JOHNSON, Nick. **Introducing .luxe on ENS.** 2018. Disponível em: <https://medium.com/@weka/introducing-luxe-on-ens-35a9ee2383ce>. Acesso em: 22 jul. 2020.

KIM, Christine. **The Ethereum Name Service Is Turning Nearly 300,000 .ETH Domains Into NFTs.** 2019. Disponível em: <https://www.coindesk.com/the-ethereum-name-service-is-turning-nearly-300000-eth-domains-into-nfts>. Acesso em: 22 jul. 2020.

MAURELIAN, J.; JOHNSON, N; DE SANDE, A. V. **EIP 162.** 2016. Disponível em: <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-162.md>. Acesso em: 22 jul. 2020.

MMX. **Join. luxe Website.** 2018. Disponível em: <https://join.luxe/>. Acesso em: 22 jul. 2020.

OSTERLUND, Paul Benjamin. **Turkey marks one year without Wikipedia.** 2018. Disponível em: <https://www.theverge.com/2018/4/30/17302142/wikipedia-ban-turkey-one-year-anniversary>. Acesso em: 22 jul. 2020.

PINODE. **4 x 2.5" HDD RAID5 RASPBERRY PI SIA HOSTING (low-Intermediate level build)**. Disponível em: < https://www.pinode.co.uk/sia-host-raspberry-pi.html>. Acesso em: 22 jul. 2020.

PPIO. **What Is Decentralized Storage?** 2019. Disponível em: <https://medium.com/@ppio/what-is-decentralized-storage-9c4b761942e2>. Acesso em: 22 jul. 2020.

TERADO, Tom. **What is Decentralized Storage? (IPFS, FileCoin, Sia, Storj & Swarm).** 2018. Disponível em: <https://medium.com/bitfwd/what-is-decentralised-storage-ipfs-filecoin-sia-storj-swarm-5509e476995f>. Acesso em: 22 jul. 2020.

TWENEY, Dylan. **Amazon website goes down for 40 minutes, costing the company $5 million.** 2013. Disponível em: <https://venturebeat.com/2013/08/19/amazon-website-down/>. Acesso em: 22 jul. 2020.

SCF. **Turkey marks second year without Wikipedia.** 2019. Disponível em: <https://stockholmcf.org/turkey-marks-second-year-without-wikipedia/>. Acesso em: 22 jul. 2020.

SIA.TECH. **Sia Official Site.** 2019. Disponível em: <http://sia.tech/>. Acesso em: 22 jul. 2020.

SIMPLY EXPLAINED. **IPFS: Interplanetary file storage! 2018**. Disponível em: <https://www.youtube.com/watch?v=5Uj6uR3fp-U>. Acesso em: 22 jul. 2020.

ZAGO, Matteo. **Why the Web 3.0 Matters and you should know about it.** 2018. Disponível em: <https://medium.com/@matteozago/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949>. Acesso em: 22 jul. 2020.