

Programação Web3 e Blockchain

Fontes do Livro

Os fontes que você viu neste livro estão disponíveis para baixar neste link: <https://www.luiztools.com.br/livro-web3-fontes/>

Referências do Capítulo 1

How to Time-Stamp a Digital Document

Artigo original dos pesquisadores da Xerox que originou a tecnologia blockchain.

https://link.springer.com/content/pdf/10.1007/3-540-38424-3_32.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

Artigo original de Satoshi Nakamoto que originou o Bitcoin.

<https://bitcoin.org/bitcoin.pdf>

LuizTools: Playlist Blockchain

Esta playlist começa com uma série de vídeos que mostra de maneira prática estes conceitos iniciais de blockchain utilizando a linguagem JS para os exemplos.

<https://www.youtube.com/watch?v=niU3SWU5FTE&list=PLsGmTzb4NxK0hRfnjfcg0f9rc0lleY28O>

Introdução à Criptografia

Série de artigos explicando os fundamentos da criptografia incluindo hash e chaves assimétricas que usamos muito na blockchain.

<https://www.luiztools.com.br/post/introducao-a-criptografia/>

Blockchain Demo

Site do professor Anders Brownworth do MIT onde você consegue simular diversas características de uma blockchain.

<https://andersbrownworth.com/blockchain/hash>

Referências do Capítulo 2

Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.

Whitepaper original sobre a Ethereum, escrito por Vitalik Buterin, fundador da Ethereum.

[https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum Whitepaper - Buterin 2014.pdf](https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum%20Whitepaper%20-%20Buterin%202014.pdf)

Understanding the Ethereum Blockchain Protocol

Palestra de Vitalik Buterin, durante a DevCon 2015.

<https://www.youtube.com/watch?v=gjwr-7PgpN8>

Ethereum for Dummies

Palestra de Gavin Wood, co-fundador da Ethereum, durante a DevCon 2015.

https://www.youtube.com/watch?v=U_LK0t_qaPo

Remix

IDE Web para desenvolvimento de smart contracts em Solidity.

<https://remix.ethereum.org>

SolidityLang.org

Site oficial da linguagem de programação Solidity.

<https://www.soliditylang.org>

Referências do Capítulo 3

MetaMask

Site oficial para instalação da MetaMask.

<https://metamask.io>

Faucets para Sepolia

Lista oficial de faucets para testnet Sepolia.

<https://ethereum.org/pt/developers/docs/networks/#sepolia>

Sepolia EtherScan

Explorador de blocos da testnet Sepolia.

<https://sepolia.etherscan.io>

Deploy do Professor

Página do meu BookDatabase.sol com deploy feito na Sepolia.

<https://sepolia.etherscan.io/address/0x8dd78c50505f86d29b48a27e0396ef4f65c36057>

EVM Opcodes

Lista completa de opcodes da EVM para consulta caso seja um aficionado por programação de baixo nível.

<https://ethereum.org/pt-br/developers/docs/evm/opcodes/>

Ethereum Gás Tracker.

Página do explorador de blocos onde pode verificar o custo atual do gás na rede (mainnet).

<https://etherscan.io/gastracker>

Eth Converter

Página que faz as conversões entre as escalas Ether, Gwei e wei facilmente.

<https://eth-converter.com/>

Referências do Capítulo 4

Os Bastidores da Internet no Brasil

Livro que conta a história do surgimento da Internet e da web no Brasil (inclui vídeo).

<https://www.luiztools.com.br/post/os-bastidores-da-internet-no-brasil-resenha/>

Ebook Frontend para Iniciantes

Ebook gratuito que ensina frontend web 1.0 do completo zero.

<https://www.luiztools.com.br/post/materiais/front-end-para-iniciantes/>

Playlist Frontend para Iniciantes

Playlist no canal LuizTools que ensina frontend web 1.0 do completo zero.

<https://www.youtube.com/watch?v=w4Ts2sVxB08&list=PLsGmTzb4NxK2sGY3KqKmg1UTxNTcPPK1Z>

Node.js

Site oficial para download e instalação do Node.js.

<https://www.nodejs.org>

Visual Studio Code

Site oficial para download e instalação do Visual Studio Code.

<https://code.visualstudio.com>

ReactJS para Iniciantes

Série de tutoriais no blog (incluindo vídeos) para aprender ReactJS do completo zero.

<https://www.luiztools.com.br/post/tutorial-de-react-js-para-iniciantes/>

EthersJS

Página oficial da biblioteca de web3 que estamos usando no livro.

<https://www.npmjs.com/package/ethers>

Async-Await

Vídeo explicando em detalhes a programação assíncrona em JS.

<https://www.youtube.com/watch?v=CevNqJwjlik>

Referências do Capítulo 5

EIP-1

Primeira Ethereum Improvement Proposal que define o padrão a ser seguido por todas EIPs e ERCs a partir dela.

<https://eips.ethereum.org/EIPS/eip-1>

Padrão ERC-20

Documentação completa do padrão que estamos estudando.

<https://eips.ethereum.org/EIPS/eip-20>

Remix

Ferramenta online para codificação de smart contracts.

<https://remix.ethereum.org>

Checks-Effects-Interactions

Mais sobre o padrão de desenvolvimento seguro que mencionei.

<https://detectors.auditbase.com/checks-effects-interactions>

LuizCoin na Sepolia

Exemplo de deploy da LuizCoin na rede Sepolia Testnet.

<https://sepolia.etherscan.io/address/0x9e08687b0546122689ddea81b784f1ca41166652>

Reentrancy Attack

Mais sobre este popular e devastador ataque que pode zerar os fundos de smart contracts rapidamente.

<https://www.luiztools.com.br/post/reentrancy-attack-em-smart-contracts-solidity/>

Variáveis msg e block

Mais sobre as propriedades dessas variáveis globais da EVM.

<https://docs.soliditylang.org/en/latest/units-and-global-variables.html>

FaucetERC20 na Sepolia

Exemplo de deploy do FaucetERC20 na rede Sepolia Testnet, já verificado.

<https://sepolia.etherscan.io/address/0x7baef326dbd7cc9173d39c7b4652ef60d8138bf4>

Bootstrap

Página de download da biblioteca de estilos Bootstrap.

<https://getbootstrap.com/docs/5.3/getting-started/download/>

Referências do Capítulo 6

O Guia Jurídico da Tokenização

Livro do meu aluno, professor, advogado e programador, Fernando Lopes, sobre aspectos jurídicos da tokenização.

<https://lopesezorro.com/o-guia-juridico/>

Bored Ape Yacht Club

Talvez a coleção NFT mais famosa no mundo mainstream por causa das celebridades que compraram unidades.

<https://boredapeyachtclub.com/>

Crypto Punks

Outra coleção NFT muito famosa, mas mais underground.

<https://cryptopunks.app/>

Axie Infinity

Mais famoso crypto game competitivo da atualidade.

<https://axieinfinity.com/>

OpenSea

Maior marketplace de NFTs do mundo.

<https://opensea.io/>

ERC-721: Non-Fungible Tokens Standard

Documento oficial descrevendo o padrão mais famoso para NFTs.

<https://eips.ethereum.org/EIPS/eip-721>

ERC-165: Standard Interface Detection

documento oficial descrevendo o padrão para identificação de interfaces de contratos.

<https://eips.ethereum.org/EIPS/eip-165>

O que é IPFS?

Vídeo no meu canal explicando sobre e ensinando a subir um nó.

<https://www.youtube.com/watch?v=yhbnSMTyGDk>

Pinata

Site de uma empresa de armazenamento IPFS.

<https://pinata.cloud/>

Deploy MyNFTCollection.sol

Endereço da minha coleção com deploy feito na Sepolia.

<https://sepolia.etherscan.io/address/0x29192156887812feead48c668d403b7074e6e039>

Referências do Capítulo 7

IERC20 da Openzeppelin

Interface que segue o padrão ERC-20.

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC20/IERC20.sol>

ERC20 da OpenZeppelin

Implementação abstrata do padrão ERC-20 para facilitar a construção de novos tokens.

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC20/ERC20.sol>

Ownable da OpenZeppelin

Implementação abstrata para controle administrativo em funções de contratos.

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/access/Ownable.sol>

Wrapped Ether (WETH)

Contrato de Wrapped Token famoso, pareado 1:1 com o ETH, para você olhar os fontes e funcionamento.

<https://etherscan.io/token/0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2>

Binance-Peg BTC Token (BTCB)

Contrato de Peggy Token famoso da Binance, pareado 1:1 com o BTC, para você olhar os fontes e funcionamento.

<https://bscscan.com/token/0x7130d2a12b99bcbfae4f2634d864a1ee1ce3ead9c>

Binance Proof of Reserves

Páginas com as provas de que a corretora Binance possui lastro para os saldos dos clientes, suas criptos, etc.

<https://www.binance.com/en/proof-of-reserves>

Auditoria do USDT

Relatórios de auditoria financeira da stablecoin Tether, para conferência do lastro.

<https://tether.to/en/transparency/?tab=reports>

Auditoria do PAXG

Relatórios de auditoria das reservas de ouro da Paxos, para conferência do lastro.

<https://paxos.com/paxg-transparency/>

Caso Terra Luna

Entenda mais sobre a polêmica da stablecoin algorítmica que foi à falência.

<https://portaldobitcoin.uol.com.br/tudo-sobre/luna/>

Referências do Capítulo 8

O Risco do Private em Smart Contracts

Vídeo no canal LuizTools sobre o risco dos private states.

<https://www.youtube.com/watch?v=5isyH1taZDs>

Slither

Framework usado por atacantes para obter acesso a variáveis privadas.

<https://github.com/crytic/slither>

Access Control | OpenZeppelin

Implementação de controle de acesso da OpenZeppelin.

<https://docs.openzeppelin.com/contracts/5.x/access-control>

Reentrancy Attacks famosos

Abaixo estão os links de notícias relatando algumas ocorrências de reentrancy attacks famosos, citados na seção sobre este tipo de hacking.

<https://www.gemini.com/pt-br/cryptopedia/the-dao-hack-makerdao#section-origins-of-the-dao>

<https://quillhashteam.medium.com/burgerswap-flash-loan-attack-analysis-888b1911daef>

<https://www.zdnet.com/article/hackers-steal-25-million-worth-of-cryptocurrency-from-uniswap-and-lendf-me/>
<https://beosin.medium.com/a-sweet-blow-fb0a5e08657d>
<https://www.coindesk.com/business/2021/10/27/cream-finance-exploited-in-flash-loan-attack-worth-over-100m/>
<https://www.halborn.com/blog/post/explained-the-siren-protocol-hack-september-2021>

Tutorial Reentrancy Attack

Vídeo no canal LuizTools ensinando sobre esse ataque.

https://www.youtube.com/watch?v=mlCfzcn5_Mw

Reentrancy Guard | OpenZeppelin

Implementação de bloqueio de reentrada da OpenZeppelin.

<https://docs.openzeppelin.com/contracts/5.x/api/utils#ReentrancyGuard>

Tutorial Gas Griefing Attack

Vídeo no canal LuizTools ensinando sobre esse ataque.

<https://www.youtube.com/watch?v=ewGW68O2XR0>

Proteção contra Gas Griefing

Propostas da ConsenSys para se proteger de Gas Griefing Attack.

<https://swcregistry.io/docs/SWC-126/>

Outra proposta de proteção para Gas Griefing citada no livro.

<https://www.getsecureworld.com/blog/smart-contract-gas-griefing-attack-the-hidden-danger/>

Referências do Capítulo 9

Node.js

Site oficial para download do ambiente necessário ao HardHat.

<https://nodejs.org>

Visual Studio Code

Site oficial para download do editor de código VS Code.

<https://code.visualstudio.com>

Tutorial de Instalação

Vídeo no canal LuizTools ensinando a baixar e instalar as duas ferramentas acima.

<https://www.youtube.com/watch?v=iJ-BUhcZOSY>

HardHat

Site oficial do toolkit HardHat com a sua documentação completa.

<https://hardhat.org/>

Infura

Provedor de blockchain em nuvem com plano gratuito.

<https://infura.io>

API Key EtherScan

Página onde você cria chaves de API para automatizar a verificação de contratos no block explorer EtherScan.

<https://etherscan.io/myapikey>

OpenZeppelin Contracts

Página com o builder de contratos da OpenZeppelin.

<https://www.openzeppelin.com/solidity-contracts>

Complexidade de Algoritmos

Vídeo no canal LuizTools ensinando mais sobre Big O Notation.

<https://www.youtube.com/watch?v=LsViaR6fJv4>

Curtiu o Livro?

Aproveita e me segue nas redes sociais: <https://about.me/luiztools>

Conheça meus outros livros:

<https://www.luiztools.com.br/meus-livros>

Conheça meus cursos online:

<https://www.luiztools.com.br/meus-cursos>