

Introdução ao Blockchain

Além do Greeter

Agenda

- O que é Blockchain
- Ethereum
- Smart Contracts
- Ethereum Virtual Machine
- Gas
- Solidity
- Geth
- Rede Privada
- Contrato de registros
- Ethereum Wallet
- Truffle + Ganache
- GoBlockchain

- O que é Blockchain

O **Blockchain** é um dos principais elementos para transações peer-to-peer, é nele que ficam armazenadas as transações que ocorreram em toda a rede. Tecnicamente ele é o livro razão das transações, ou banco de dados descentralizado e distribuído.

Toda vez que uma transação é enviada, ela é validada por um consenso e armazenada em milhares de computadores pelo mundo, ou seja não existem servidores centrais ou intermediários.

O Bitcoin foi o primeiro projeto a utilizar esse mecanismo para armazenar informações distribuídas.

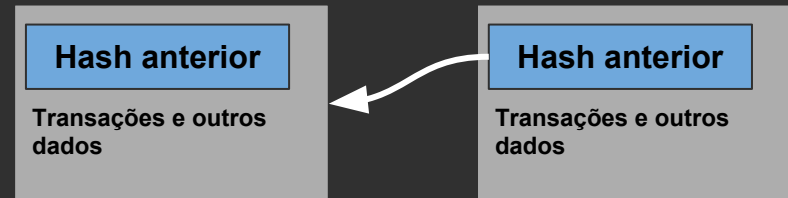
A estrutura básica de um Bloco é: Hash do bloco anterior, Nonce e Transações.

- Benefícios

- Segurança
- Confiança descentralizada
- Transparência
- Eficiência
- *Redução de custo
- Imutabilidade da informação
- Conciliação

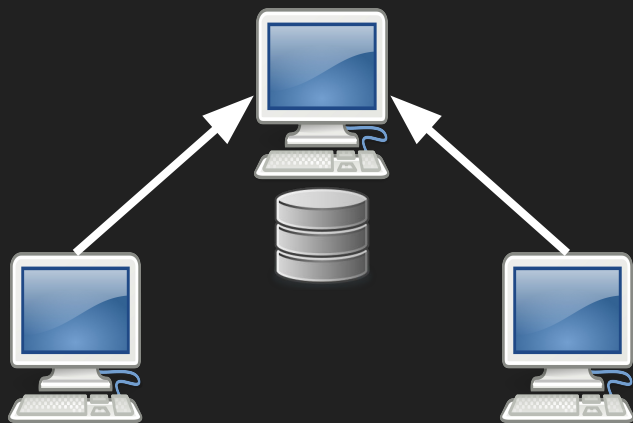
- Desafios

- Escalabilidade
- Legislação



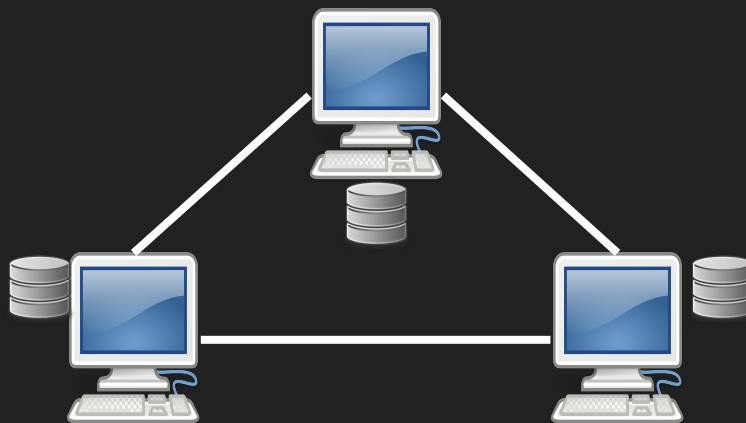
Rede Centralizada e Distribuída

Cópia dos dados em um único lugar



Centralizada

Todos participantes tem uma cópia dos dados



Distribuída

- Ethereum

É uma plataforma de código aberta baseada na tecnologia Blockchain.

O Ethereum foi construído a partir do código fonte do Bitcoin porém eles criaram uma camada chamada EVM que possibilitou que as transações tenham regras de negócios definidas, isso chamamos de Smart Contracts.

Dessa forma podemos criar aplicações descentralizadas, transparentes em uma rede distribuída.

A EVM é a máquina virtual que executa os Smart Contracts.

- Bitcoin e Ethereum estão em redes diferentes.
- O Ethereum vai rodar na sua máquina, isso significa que você é um nó da rede.
- Atualmente a maioria dos ICO's utilizam programas desenvolvidos em Ethereum.
- Hoje seu maior desafio é a escalabilidade e custo do GAS.
- Existem 3 ambientes disponíveis para você utilizar o Ethereum: Desenvolvimento, TestNet e MainNet

- Smart Contracts

Smart Contracts são os programas onde definimos as regras das nossas aplicações em Ethereum.

Imagina os Smart Contracts são a camada de back end da sua aplicação, você vai criar soluções autônomas, prova de fraudes humanas e sem intermediadores.

Importante:

- Executar o contrato tem custo(Gas);
- Faça muitos testes antes de ir para produção(mainnet);
- Os dados são gravados dentro do contrato, portanto quanto maior mais caro vai ficar com o tempo;
- Utilize variáveis adequadas para cada informação, assim você ter uma economia de Gas.

- Gas

Gas é o "combustível" que move a rede Ethereum, o valor do Gas é definido de acordo com o poder computacional necessário para validar a transação. Esse custo tem como vantagem motivar que as pessoas contribuam com a rede e desencoraja o uso de códigos ineficazes e maliciosos.

Importante

- Quanto mais complexo seu programa mais caro vai ser o Gas.
- Toda transação precisa ser enviada com Gas.
- Quanto menor a taxa oferecida mais demorado pode ser a execução da sua transação.
- O Gas é pago através de Ether, portanto você vai precisar ter Ether em sua carteira para compilar os programas em produção.

- Solidity

Solidity é a principal de linguagem de programação para os Smart Contracts da rede Ethereum.

Site:

<https://solidity.readthedocs.io/en/develop/>

- Geth

Geth é um dos softwares da rede Ethereum que permite que você se torne um nó da rede e tenha uma cópia do Blockchain. Ao instalar o Geth você pode acessar a rede de produção, as redes de homologação que são Ropsten, Kovan, Rinkeby e criar uma rede de desenvolvimento.

Download:

<https://geth.ethereum.org/downloads/>

Alguns comandos GETH

- `--rpc` permite a conexão o protocolo rpc
- `--rpcapi` permite quais são as apis que podem executar no nó
- `--datadir` define qual diretório deseja armazenar as informações e dados do nó
- `console` abre cliente javascript para execução de comandos
- `--dev` criar uma ambiente de desenvolvimento
- `Geth help` lista todos parâmetros

Ethereum Wallet

Vamos configurar

- Download
- Apontar para nosso nó privado
- Criar conta
- Enviar ether entre contas
- Compilar e executar contrato

Registros de nomes

Garante a unicidade de nomes
de tokens

<https://gist.github.com/falehenrique/2e2585ba3216729336bdd042a449793>

Ganache

- Simule de forma simples um cliente Ethereum para executar testes de forma mais rápida
- [Download](#)

ACCOUNTS	BLOCKS	TRANSACTIONS	LOGS
CURRENT BLOCK 0	GAS PRICE 2000000000	GAS LIMIT 6721975	NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING		
MNEMONIC candy maple cake sugar pudding cream honey rich smooth crumble sweet treat		HD PATH m/44'/60'/0'/0/account_index	
ADDRESS 0x627306090abaB3A6e1400e9345bC60c78a8BEf57	BALANCE 100.00 ETH	TX COUNT 0	INDEX 0
ADDRESS 0xf17f52151EbEF6C7334FAD080c5704D77216b732	BALANCE 100.00 ETH	TX COUNT 0	INDEX 1
ADDRESS 0xC5fdF4076b8F3A5357c5E395ab970B5B54098FeF	BALANCE 100.00 ETH	TX COUNT 0	INDEX 2
ADDRESS 0x821aEa9a577a9b44299B9c15c88cf3087F3b5544	BALANCE 100.00 ETH	TX COUNT 0	INDEX 3

CURRENT BLOCK 4	GAS PRICE 20000000000	GAS LIMIT 6721975	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING		
TX HASH 0x836c1cd1e859050f268972931eda11da000c12cbc249fc9d23b9f7936b1532ff							CONTRACT CALL
FROM ADDRESS 0x627306090abab3a6e1400e9345bc60c78a8bef57				TO CONTRACT ADDRESS 0x8cdaF0cd259887258bc13a92c0a6da92698644c0		GAS USED 26981	VALUE 0
TX HASH 0x5b81a682f2eeb1a6046f44cab9d7dfae2ec6bcc997d53eeaf2b7e77539d67541							CONTRACT CREATION
FROM ADDRESS 0x627306090abab3a6e1400e9345bc60c78a8bef57				CREATED CONTRACT ADDRESS 0x345ca3e014aaF5dca488057592ee47305d9b3e10		GAS USED 1746677	VALUE 0

Truffle

- Framework de desenvolvimento de contratos
- Automatiza o processo de deploy e testes na rede Ethereum
- Permite testes com Mocha e Chai
- Simula um ambiente para testes locais

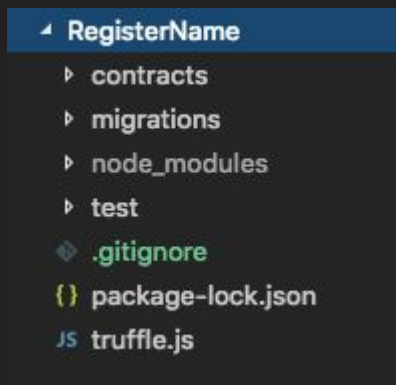
- Verificar se node esta instalado
- `node --version`
- `npm install -g truffle`
- Digite truffle

```
Commands:
init      Initialize new and empty Ethereum project
compile   Compile contract source files
migrate    Run migrations to deploy contracts
deploy     (alias for migrate)
build     Execute build pipeline (if configuration present)
test      Run JavaScript and Solidity tests
debug     Interactively debug any transaction on the blockchain (experimental)
opcode    Print the compiled opcodes for a given contract
console   Run a console with contract abstractions and commands available
develop   Open a console with a local development blockchain
create    Helper to create new contracts, migrations and tests
install   Install a package from the Ethereum Package Registry
publish   Publish a package to the Ethereum Package Registry
networks  Show addresses for deployed contracts on each network
watch     Watch filesystem for changes and rebuild the project automatically
serve     Serve the build directory on localhost and watch for changes
exec      Execute a JS module within this Truffle environment
unbox     Download a Truffle Box, a pre-built Truffle project
version   Show version number and exit
```

See more at <http://truffleframework.com/docs>

Truffle - Projeto

- `mkdir RegisterName && cd RegisterName`
- `truffle init`
- [Download do projeto](#)



- `contracts` contém os arquivos solidity, é aqui que ele vai buscar durante a migração
- `migrations` contém os arquivos com os scripts de deploy
- `test` contém os scripts de tests criados em mocha e chai
- `truffle.js` contém as configurações utilizada durante o processo de compilação e deploy

Truffle - Comandos

- truffle compile - gera os arquivos abi e bytecode dos contratos
- truffle migrate - realiza o deploy do build gerado na rede
- truffle test - executa os scripts de testes
- truffle console - disponibiliza um CLI para interações com os contratos

truffle.js

```
module.exports = {  
  networks: {  
    development: {  
      host: "127.0.0.1",  
      port: 7545,  
      network_id: "*"  
    }  
  }  
}
```

truffle console

```
[truffle(development)> Migrations.contractName  
'Migrations']
```

GoBlockchain

- Plataforma de ensino descentralizada
- Iniciativa para criar conteúdo relevante e contribuir conhecimento em Blockchain
- Queremos aprender, ensinar e validar as redes distribuidas



GoBlockchain

GoBlockchain

Identidade

Conta Corrente

Reputação

Certificados

Eventos

Pagamentos

Colaboradores



Obrigado

Vamos aprender e construir juntos

<http://goblockchain.io>