

Um evento com propósito

# Embarcadero Conference 2020 Online

## TODOS CONECTADOS



Um evento com propósito  
**Embarcadero Conference**  
**2020 Online**

# INTEGRANDO-SE À BLOCKCHAIN DA ETHEREUM

Mario Guedes | [mario@arrayof.io](mailto:mario@arrayof.io)



# Agenda

O objetivo da apresentação é o de apresentar os conceitos iniciais da Blockchain da Ethereum.

- Contexto atual
- Quando surgiu, o que é e para que é Blockchain?
- Oportunidades de negócio
- O que é a Ethereum?
- Principais conceitos envolvidos
- Convite para desenvolvermos um:  
**Cofre de Senhas Descentralizado**
- 👉 **Não falaremos de investimento em ETH ou BitCoin**  
*Sou daqueles que compra na alta e vende na baixa* 🙄

# Avaliação da palestra

- Ao final da palestra, deixe sua avaliação:
- <https://forms.gle/mueNWCySr86RMv7R7>



## Contexto atual

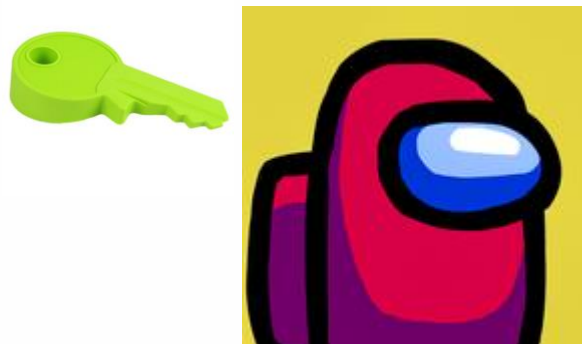
- Vivemos no pior momento em termos de confiança  
Política, Financeira, Social, Empresarial ...
- Abrimos mão da nossa privacidade em troca do pertencimento ao mundo digital
- Tempos de LGPD e direito ao esquecimento
- Cada vez menos, porém maiores, intermediários:  
Bancos, empresas de tecnologia (redes sociais), governos
- Hiper conectividade, GPS, hardware mais barato, redes mais rápidas

- Em 2008 uma entidade auto denominada Satoshi Nakamoto produziu um white paper com um proposta: Um **Sistema Financeiro Eletrônico Ponto a Ponto** [5]
- O objetivo, grosso modo, é o de eliminar **intermediários**.
- Pilares:
  - Trocas diretas
  - Validação descentralizada
  - Necessidade de consenso
  - Eliminar “gasto duplo”
  - Desconfiança – todos os participantes “sabem de tudo”
  - Projeto de código aberto – auditabilidade
  - Criptografia em todas as fases
  - As informações gravadas são imutáveis
  - Não existe um “cadastro de usuários” mas sim endereços
- Sistema global em produção desde 2009 sem interrupção
- 🧐 <https://blocks.wizb.it/>

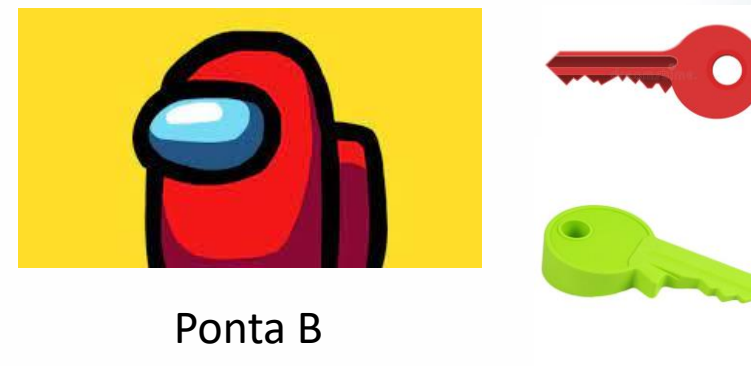
# Chaves assimétricas

- É um instrumento que permite o tráfego de mensagens criptografadas.
- Temos um par de chaves:
  - Chave pública
  - Chave privada.
- A chave pública é *derivada* da chave privada.
- O dono da chave privada compartilha com terceiros a chave pública.
- O terceiro usa a **chave pública** para criptografar uma mensagem.
- Mas somente o dono da chave privada consegue descriptografar, usando a **chave privada**.

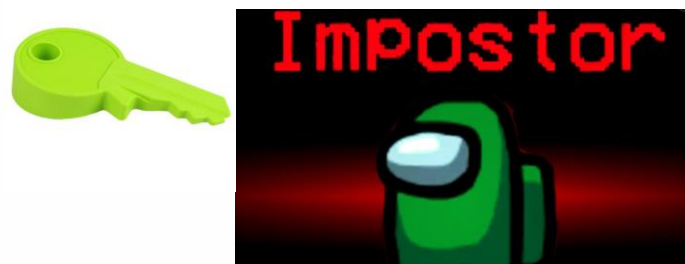
# Um pouco de criptografia assimétrica



Ponta A



Ponta B



Ponta C



# Hash criptográfico

- Algoritmo de hash
- Garante **autenticidade** de uma informação  
Texto, JPEG, PDF, Word, MP4, PPT, .pas, .gdb ...
- Gera uma representação alfanumérica com um mesmo tamanho
- Uma ligeira alteração do conteúdo gera uma representação totalmente diferente
- Existem vários algoritmos:  
md5, sha-1, sha-2, sha-256 e etc

# O que é Blockchain?

*“Banco de dados descentralizado mantido através de consenso e uma rede de participantes.”*

- Protocolo da Confiança
- Fortemente baseado em **criptografia** em todas as fases: transmissão, validação, armazenamento, etc.
- Vários nós de uma rede executam um *cluster* blockchain
- Ele nos oferece TRANSPARÊNCIA e IMUTABILIDADE

# Cadeia de Blocos

- Todos os conceitos são magistralmente demonstrados no projeto: <https://andersbrownworth.com/blockchain/>



# Tipos de blockchain

- **Pública:** Os dados são acessíveis a qualquer um que queira inspecionar as transações. A blockchain do BitCoin foi a primeira neste sentido.
- **Privada:** Tanto a rede quanto os dados são de acesso restrito.
- **Permissionada:** É o mais interessante para o mundo corporativo pois os participantes devem ser convidados a participar da rede. Logo a participação não é anônima.
- **Não Permissionada:** Os participantes se associam livremente e geram as transações de forma anônima.
- **Ethereum:** É uma rede blockchain pública e não permissionada
- **Hyperledger Fabric:** É um ferramental que nos permite criar uma rede permissionada tanto pública quanto privada. É mantida pela IBM e Linux Foundation e aderente ao mundo corporativo.





- “A Ethereum é uma plataforma global de código aberto para aplicativos descentralizados.”
- Foi idealizada em 2013 e implementada em 2015 por **Vitalik Buterin**
- O grande diferencial da blockchain da Ethereum é o de executar códigos arbitrários, os conhecidos Smart Contracts.
- <https://ethereum.org/pt-br/>
- <https://ethereum.foundation/>
- <https://etherscan.io/>
- <https://remix.ethereum.org/>
- <https://studio.ethereum.org/>





## Quem sustenta a blockchain da Ethereum?

- A motivação de alguém manter uma máquina na rede Ethereum é a **recompensa** em ETH.
- São os **mineradores**. Têm por objetivo fechar um bloco.
- E cada transação paga uma taxa ao minerador
- **PoW – Prova de Trabalho**  
Vence aquele que primeiro gerar um hash válido para o bloco atual
- **PoS – Prova de Participação**  
Vence aquele que possui melhor posição em moeda

# Proof of Work: Prova de trabalho

- Demanda alta carga de processamento
- O nó da rede tem que vencer ao desafio proposto pela rede que, em outras palavras, consiste em gerar um hash criptográfico aderente às regras impostas pela rede.
- Para isto o nó tem que modificar constantemente o Nonce.
- Em algum momento o nó apresenta o resultado aos outros nós da rede.
- Os outros nós da rede validam o resultado proposto, acatando ou não o bloco como fechado.
- Quando 50% + 1 da rede acatar o resultado este nó ganha a recompensa e toda a rede entende que o bloco está resolvido.

# Conceitos gerais

- **Transação**

*É um evento que altera o estado de uma informação associada à uma blockchain.*

- **DAO – Organização Autônoma Descentralizada**

*“Organização cujas regras são geridas por smart contracts, que são executados e validados por uma blockchain.” [1]*

- **Wallet**

*"Carteira", basicamente, é um gerenciador de chaves criptográficas. É o mecanismo que permite gerar, assinar e enviar transações em uma rede blockchain.*

- **Moeda**

*É a representação monetária da blockchain, que é comercializada no mundo “real”*



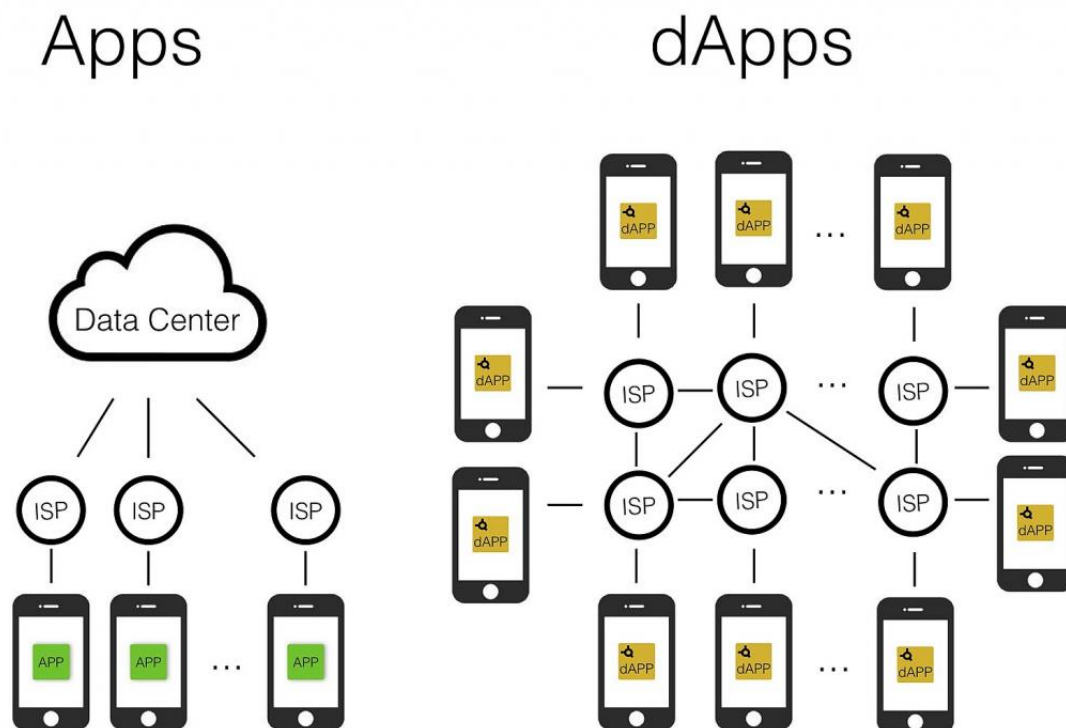
# Smart Contracts

*Contrato: “É um acordo de vontades entre duas ou mais partes.”*

- É o seu código com a sua regra de negócio
- A Ethereum suporta duas linguagens: Solidity e Vyper
- **É “Contract”?**  
*Não. É apenas a execução de um contrato.*
- **É “Smart”?**  
*Não pois não há inteligência artificial envolvida. Executa apenas o que foi programado.*
- Pode fazer o papel de “escrow” entre duas partes. [3]
- O conceito foi idealizado por Nick Szabo, um dos precursores do BitCoin

# DApp – **A**pplicação **D**escentralizada

- Um passo a frente do *serverless*
- Usar uma blockchain pode ou não eliminar a necessidade de um servidor centralizado
- É aqui que o Delphi entra: desenvolve-se uma aplicação descentralizado



# Oportunidades de negócio

- Soluções de rastreamento:  
*da matéria prima ao consumidor chegando à logística reversa*
- Soluções jurídicas, contábeis, bancárias, eleitorais, cartorárias, patentes
- Soluções voltadas para gestão pública
- Soluções voltadas para *smart cities*
- Soluções de prevenção à fraude
- Soluções de marketing e engajamento (como por exemplo programas de fidelidade)
- Soluções de registros sensíveis, como vacina
- Em uma palavra: **Desintermediação**
- Exemplo de uma empresa brasileira fundamentada em blockchain: **OriginalMy**  
<https://originalmy.com/>  
Soluções voltadas à identificação, privacidade, coleta de provas digitais entre outras nesta linha de atuação.  
🤖 Detalhe: Fica situado na **Estônia**, país mais digital do mundo  
<https://olhardigital.com.br/video/startup-brasileira-faz-sucesso-na-estonia/95543>

# Usando no Delphi

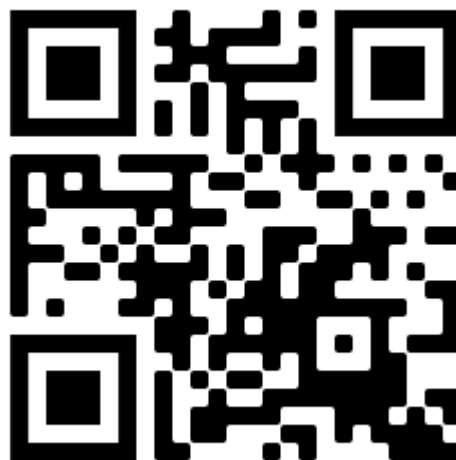


- O Embarcadero MVP holandês **Stefan van As** desenvolveu uma biblioteca que facilita a interface com a rede blockchain da Ethereum: **Delphereum**
- Esta biblioteca é citada na página da Ethereum Foudation, ou seja, tem credibilidade.
- **Stefan van As:** <https://stackoverflow.com/story/svanas>
- **Biblioteca Delphereum:** <https://github.com/svanas/delphereum>
- **Artigos do Stefan no Medium:** <https://medium.com/@svanas>
- A comunicação com a rede Ethereum é sobre um protocolo RPC
- Também temos a opção de contratarmos *providers* que intermediam a comunicação com os nodes da rede Ethereum.
- Isso facilita pois usa-se um protocolo mais amigável, como REST/JSON.
- Um exemplo é o Infuria: <https://infura.io/>



## Continuaremos esta palestra no YouTube

- Por ser um assunto denso priorizei fazer uma alinhamento geral
- Iniciaremos uma **série de vídeos** sobre **Blockchain** da **Ethereum** no nosso canal
- Nesta série iremos desenvolver um cofre de senhas para guarda-las diretamente na blockchain da Ethereum



[http://bit.ly/cofre\\_senhas](http://bit.ly/cofre_senhas)

# O que será o nosso Cofre de Senhas?

- Existem vários gerenciadores de senha no mercado: LastPass, 1Password e etc
- Isso nos permite usar senhas exclusivas e longas nos diversos sites e aplicativos
- Mas algo incomoda: tem uma empresa por trás e nossas senhas estão em algum servidor por aí

*Mesmo que a empresa diga que não tem a minha chave mestra, como saber se não tem mesmo? Aqui estamos falando de falta de confiança.*



- Vamos então desenvolver uma aplicação que atua como wallet e armazena as nossas senhas na blockchain acionando um smart contract para tal.
- Será uma **DApp** pois não haverá um servidor centralizado.
- 🖱️ Iniciaremos na primeira semana de Novembro: [http://bit.ly/cofre\\_senhas](http://bit.ly/cofre_senhas)

## Conclusão e links

- **Blockchain** é uma tecnologia nova com muitos desafios pela frente
- Mas já está passando pelo filtro do tempo e veio para ficar
- Observe que focamos na rede blockchain da **Ethereum**.
- Existe diversas outras redes: BitCoin, Ripple, Corda, RSK, Stellar, ...
- E pode-se montar uma privada e customizada usando a tecnologia **Hyperledger**
- **Ethereum Foudation:** <https://ethereum.org/pt-br/>  
*Apresentação da proposta de valor, material introdutório, cases entre outros recursos.*
- **Enterprise Ethereum Alliance:**  
<https://entethalliance.org/>  
*Organização que fomenta o uso da Ethereum pelo mundo corporativo. É sustentado por grandes empresas além da participação de outros atores da sociedade civil.*
- **Lista de ferramentas de desenvolvimento:**  
<https://github.com/ConsenSys/ethereum-developer-tools-list#smart-contract-languages>
- **Fórum de discussão oficial:**  
<https://ethereum.stackexchange.com/>



**Mario Guedes**  
[mario@arrayof.io](mailto:mario@arrayof.io)

 Desenvolvedor na TEx Tecnologia  
 Instrutor e Consultor pela ArrayOf.io

 Em todas as redes: @jmarioguedes

<https://jobs.solides.com/textecnologia>



**EU GOSTO DO DELPHI**

Mantido pela ArrayOf.io



OBRIGADO

 **embarcadero**



# Referências

- [1] [https://pt.wikipedia.org/wiki/Organiza%C3%A7%C3%A3o\\_aut%C3%B4noma\\_descentralizada](https://pt.wikipedia.org/wiki/Organiza%C3%A7%C3%A3o_aut%C3%B4noma_descentralizada)
- [2] <https://trailhead.salesforce.com/pt-BR/content/learn/modules/blockchain-basics/blockchain-network-types>
- [3] <https://www.dicionariofinanceiro.com/escrow/>
- [4] <https://blockchainacademy.com.br/>
- [5] <https://cointimes.com.br/whitepaper-do-bitcoin-traduzido/>