Smart contracts
(ou contratos inteligentes)

PUC Minas

Aplicações Descentralizadas e Blockchain

Prof. Carlos Leonardo dos S. Mendes

O que são *smart contracts*

- ***Smart contracts*** foram inicialmente propostos em 1994 por **Nick Szabo**, um cientista da computação americano, que inventou uma moeda virtual em 1998 chamada “Bit Gold”.
- Szabo definiu um smart contract como **“um protocolo de transação computadorizado que executa os termos de um contrato”**.
- Objetivos gerais definidos por Szabo:
  - satisfazer as condições contratuais comuns (pagamento, ônus, cumprimento, etc.);
  - minimizar exceções maliciosas e acidentais;
  - minimizar a necessidade de intermediários confiáveis.

Fonte: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

O que são smart contracts

- Essa máquina executa automaticamente os termos do contrato de venda.

O que lhe faz confiar nela?

- A confiança é fundamental para qualquer sistema de trocas.
- No sistema monetário atual, desde o abandono do lastro em ouro, o valor das moedas se baseia em um sistema de garantias oferecido pelo Estado.
- De uma forma geral, qualquer troca no sistema capitalista tem um terceiro como garantidor, geralmente um órgao de Estado.
- A ausência de confiança é a regra!

A CONFIANÇA COMO ELEMENTO FUNDAMENTAL DO CAPITALISMO

A relação com blockchain

- A ideia de Nick Szabo **carecia de uma ambiente** que trouxesse **confiabilidade** para a execução dos contratos inteligentes.
- Vitalik Buterin, criador da plataforma Ethereum, percebeu que a **blockchain** era o ambiente que tornaria os *smart contracts* **reais**.
- A plataforma Ethereum foi a primeira tecnologia de blockchain a implementar uma **máquina virtual distribuída** para a execução de smart contracts: **Ethereum Virtual Machine**, ou EVM).
- *Smart contracts* podem ser escritos na plataforma Ethereum em uma **linguagem** chamada **Solidity**.
- Hoje, outras plataformas de blockchain executam *smart contracts*.

The code is the law

- *Smart contracts* são **regras escritas em código de programação**.
- Essas regras são **registradas** em uma rede de **blockchain**.
- *Smart contracts* são **auto-executáveis** se condições **auto-verificáveis** pré-programadas ocorrerem.

PUC Minas

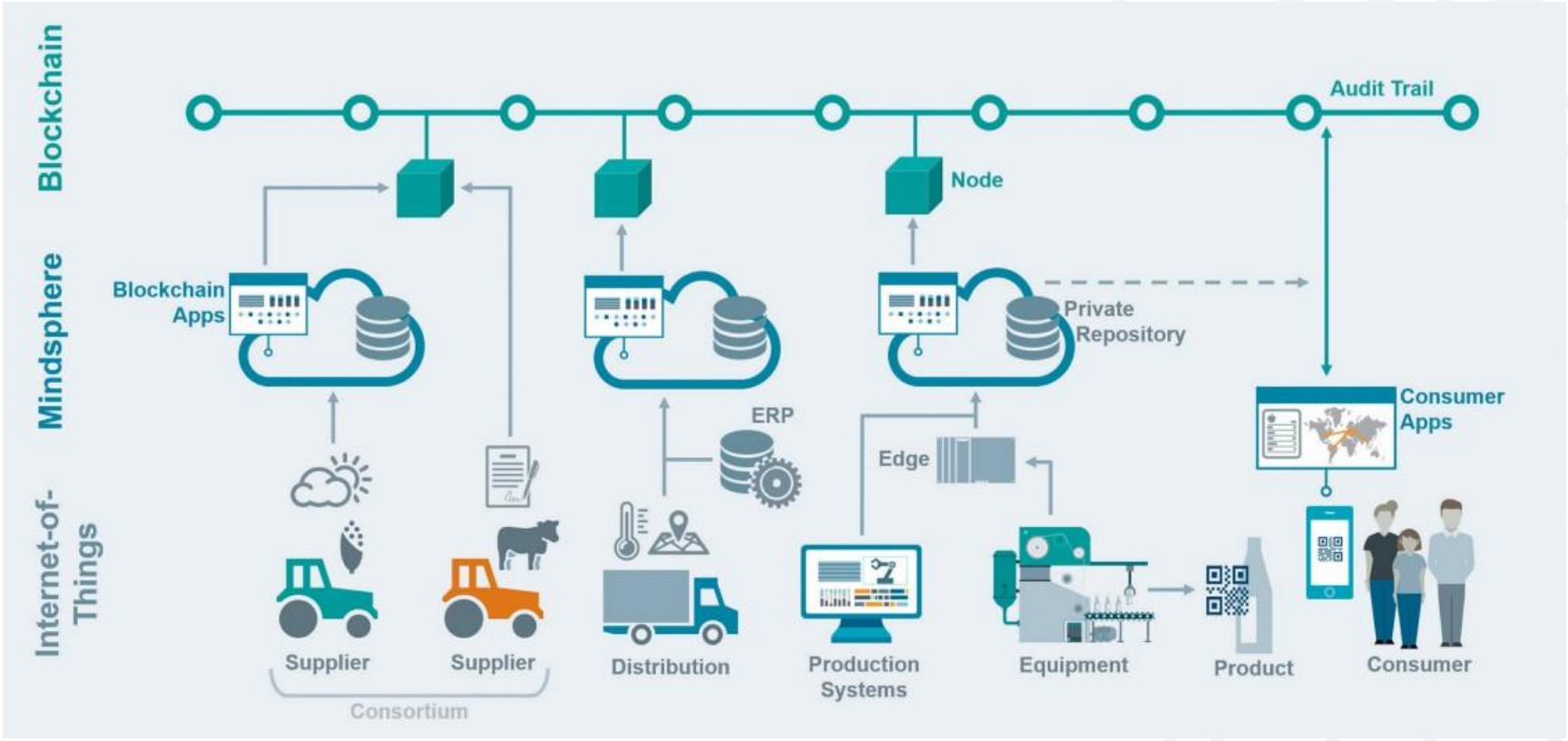
Principais características

- Distribuídos.
- Determinísticos.
- Autônomos.
- Imutáveis.
- Customizáveis.
- Não requerem confiança.
- Transparentes.

PUC Minas

Smart contracts: casos de uso

Wallmart: Rastreamento da cadeia de perecíveis

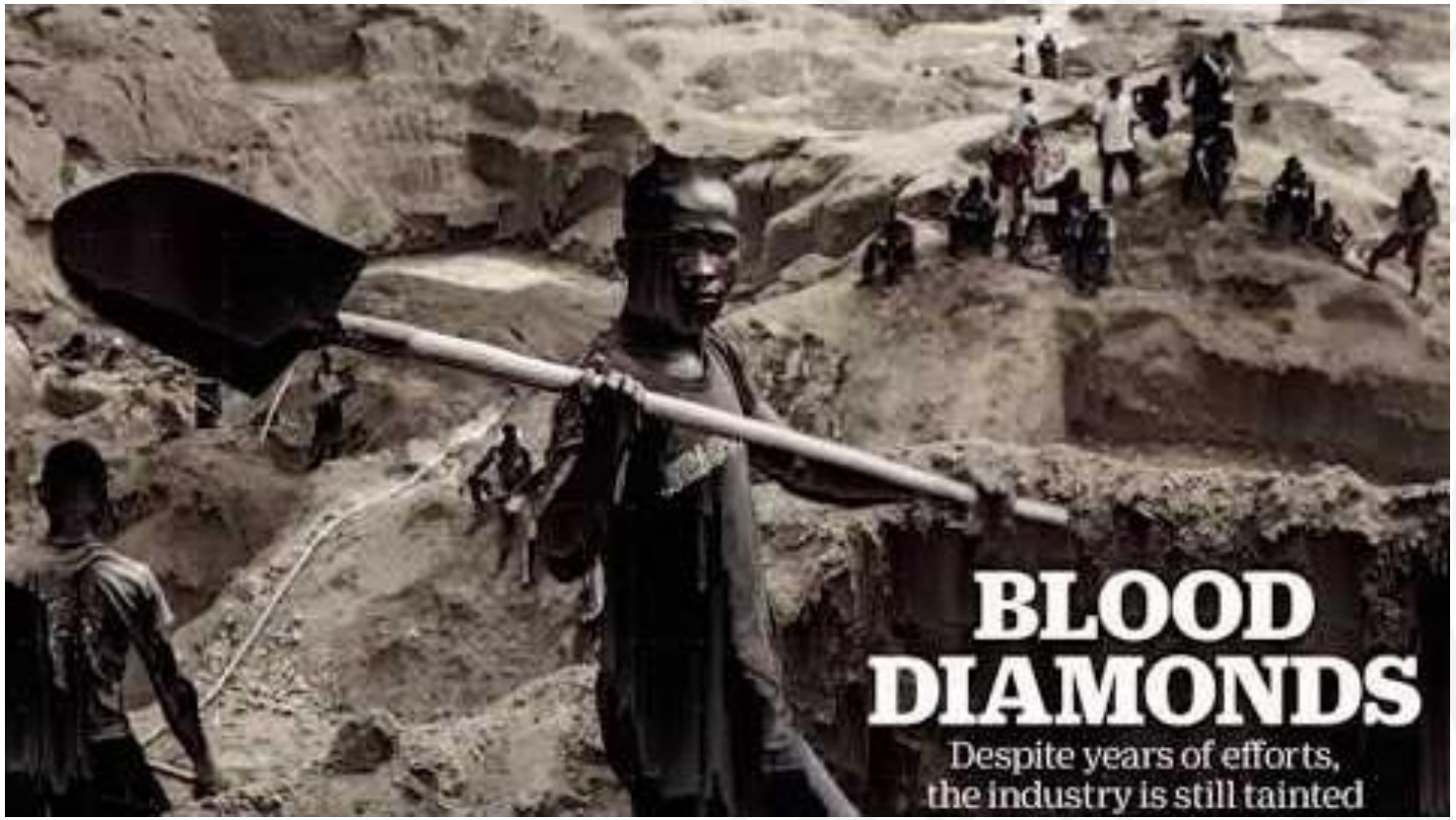


https://www.hyperledger.org/resources/publications/walmart-case-study

Smart contracts: casos de uso

"Diamantes de Sangue"

- O ciclo de vida da produção de diamantes originados na África do Sul foi registrada em blockchain.
- As operações, desde a extração, lapidação e produção de jóias, são registradas na blockchain e podem ser rastreadas.



https://youtu.be/pQoPRAajHT8

Aprenda a escrever smart contracts para Ethereum

- https://cryptozombies.io/pt/

PUC Minas