Marcos Oliveira

Tópicos Avançados de Banco de Dados

Professora: Lorena Pereira da Ponte Pierre

Ciência da Computação

Universidade Vale do Acaraú - UVA

Fevereiro de 2018

DataChain: Uma Ferramenta para Assegurar a Propriedade e Imutabilidade de Documentos Digitais

Gabriel O. Mendanha [1], Lívia A. Cruz [1], Regis P. Magalhães[1]

[1]Universidade Federal do Ceará – Campus de Quixadá
Quixadá – CE – Brasil

gabrielmendanha@alu.ufc.br, {livia.almada,regismagalhaes}@ufc.br

Resumo. *Após a criação da criptomoeda Bitcoin, com o estudo e pesquisa da tecnologia que a tornou possível, a blockchain, viu-se a possibilidade de utiliza-lá para outros casos de uso não relacionados a transações financeiras ou dinheiro digital. Motivado por uma realidade que pessoas facilmente adulteram, copiam e corrompem informações digitais, este trabalho apresenta uma prova de conceito utilizando a blockchain, tirando proveito das características de imutabilidade e propriedade dos dados. Voltado para documentos digitais, o presente trabalho também abre uma gama de casos de uso e possibilidades para uma variedade de consumidores que desejam uma maneira de provar a autenticidade e posse de documentos, assim como transferí-los a outras pessoas.*

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Características do Blockchain

- **Lista encadeada de blocos**
- **Os blocos são identificados por sua função hash**

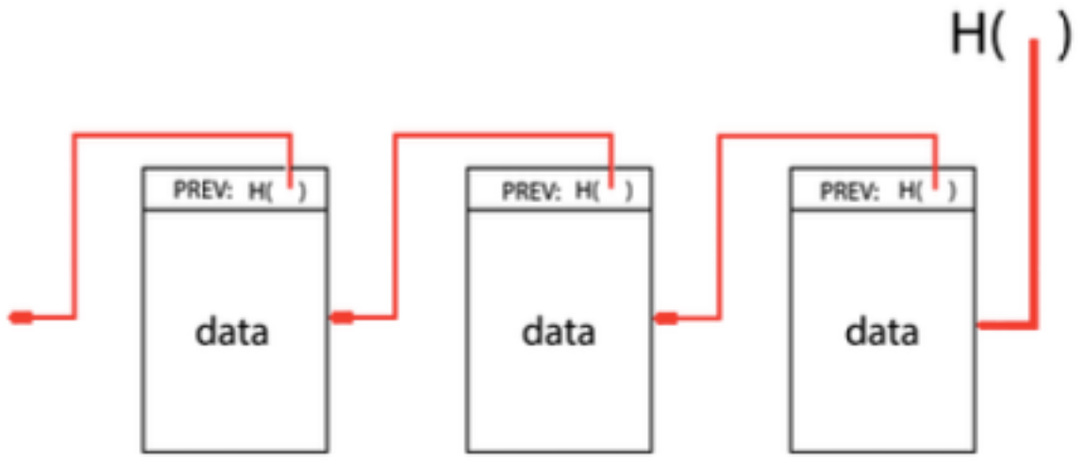
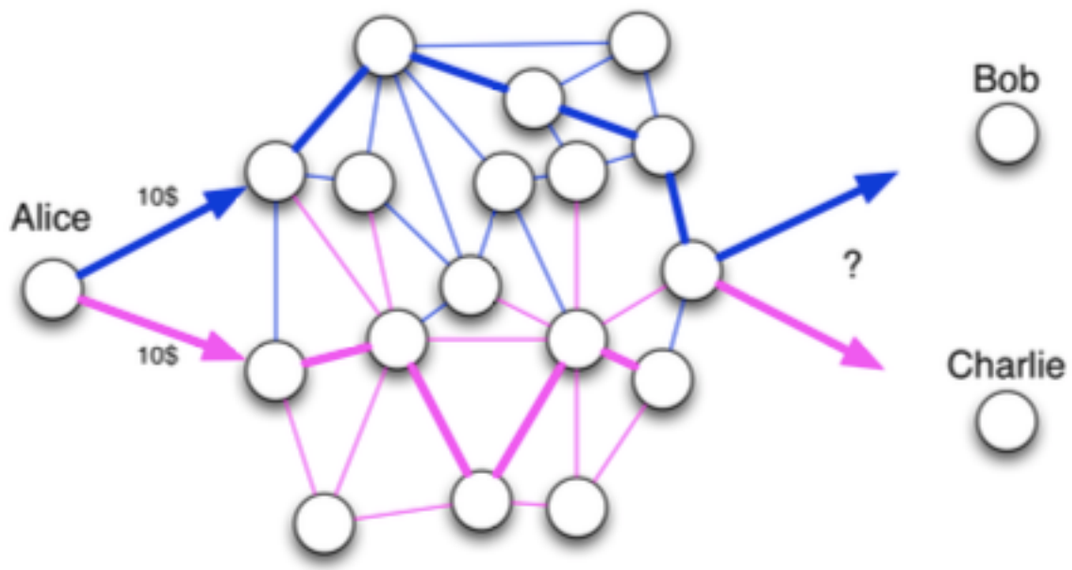
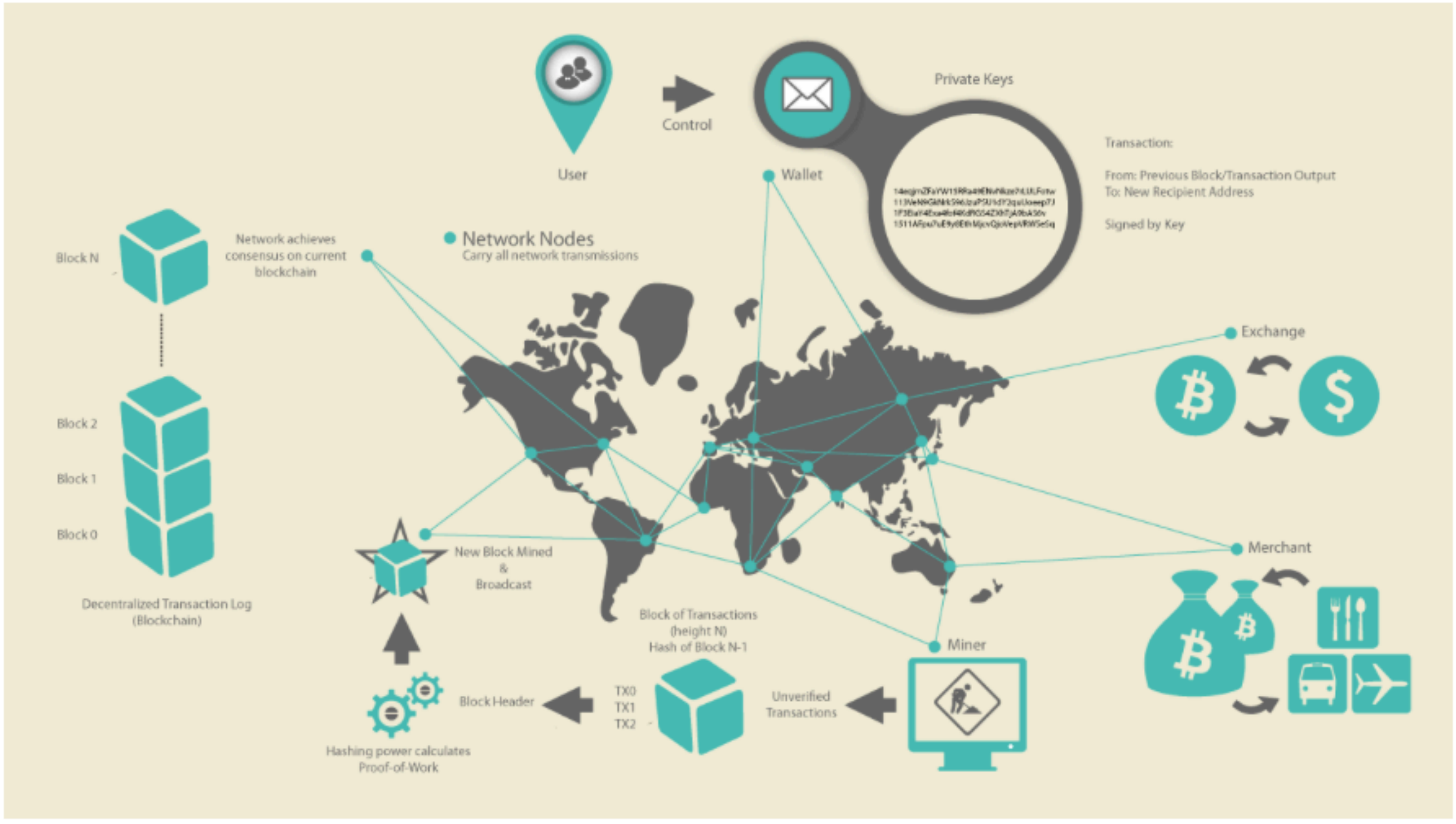


Figura 1. Estrutura da *blockchain*

Distribuição, Segurança e Integridade da Blockchain

- **O gerenciamento não é centralizado**
- **O controle é descentralizado e realizado por meio de um conjunto de nós numa rede *peer-to-peer*.**
- **Como o controle é descentralizado existe um algoritmo de resolução de conflitos**
- **Usa o sistema de criptografia assimétrica para garantir a assinatura de documentos e trasações**




User
Control
Private Keys
Wallet
Transaction:
From: Previous Block/Transaction Output
To: New Recipient Address
Signed by Key
Network Nodes
Carry all network transmissions
Network achieves consensus on current blockchain
Block N
Block 2
Block 1
Block 0
Decentralized Transaction Log (Blockchain)
Exchange
Merchant
New Block Mined & Broadcast
Block of Transactions (height N) Hash of Block N-1
Miner
Block Header
TX0
TX1
TX2
Unverified Transactions
Hashing power calculates Proof-of-Work

Sistema DataChain

- **Armazena documentos estabelece vínculo de posse;**
- **Permite a transferência do documentos usando um par de chaves criptográficas;**
- **Validação da posse do documentos pelos usuários que utilizam a plataforma;**
- **Público-alvo: autor de uma obra intelectual (artistas, compositores), homens de negócio para transferir ou provar a propriedade de terras, entidades que desejam combater fraudes em documentos sensíveis: documentos de identificação pessoal, prontuários médicos, diplomas;**

Arquitetura do DataChain

Componente do Datachain

- **BigchainDB**
  - ***Open Source*;**
  - **Descentralizado e Distribuídos;**
  - **Incorpora as características do *blockchain*;**
  - **Posse e transferência de ativos digitais são garantidas por meio de chaves públicas e privadas.**
- **IPFS (*InterPlanetary File System*)**
  - **Implementa o modelo *peer-to-peer;***
  - **Objetiva conectar vários dispositvos os mesmo sistema de arquivos;**
  - **Modelo de armazenamento endereçado pelo conteúdo;**
  - **Nós não confiáveis; Nós não tem uma hierarquia e se conectam para para transferir arquivos;**
  - **Gera *hash* único e imutável para cada documento;**

Arquitetura do DataChain

- **Uso BigchainDB e IPFS em conjunto;**
  - **Não há necessidade de armazenamento do arquivo no banco de dados;**
  - **Sem as limitações de dados do BD;**
  - **Não há necessidade conversões;**
  - **Melhor desempenho;**

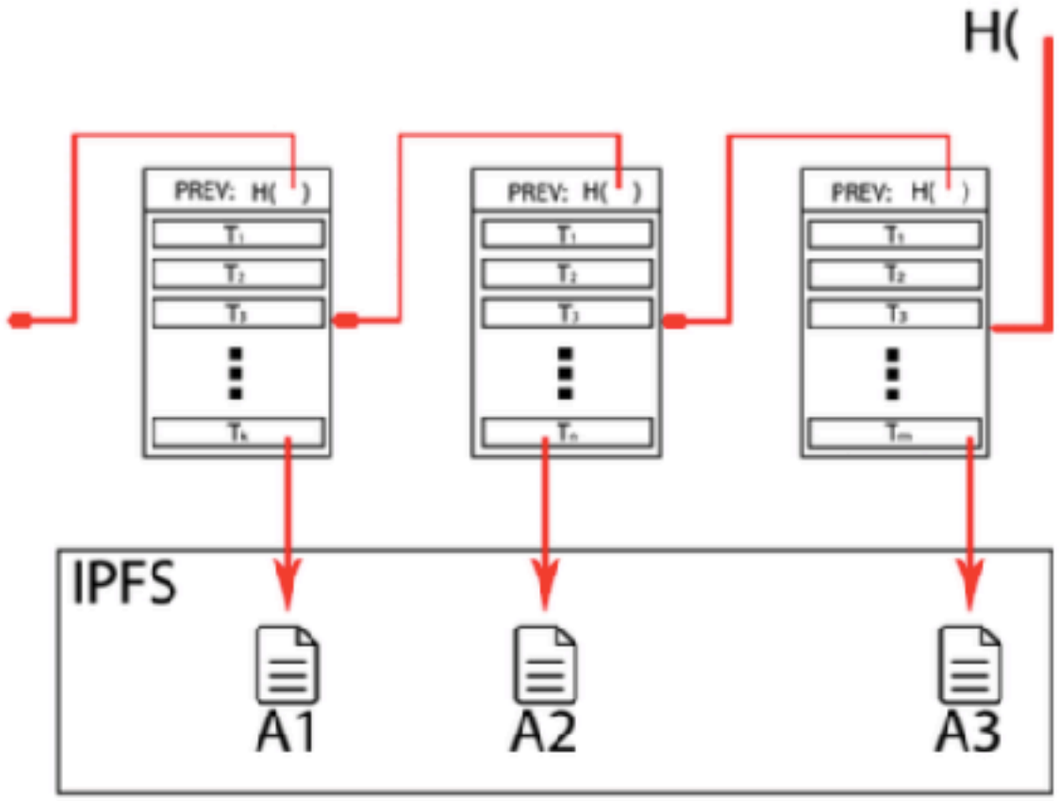
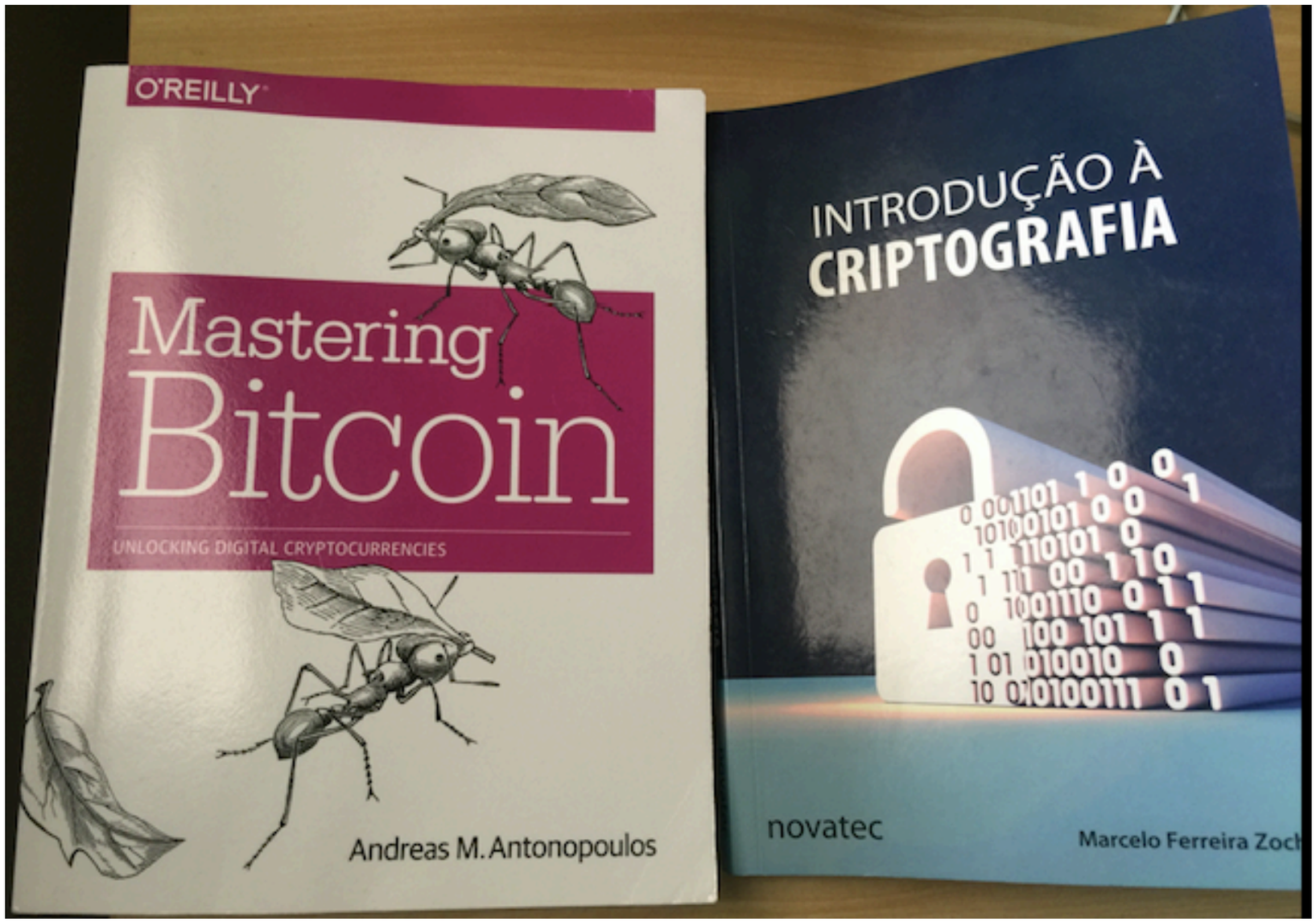
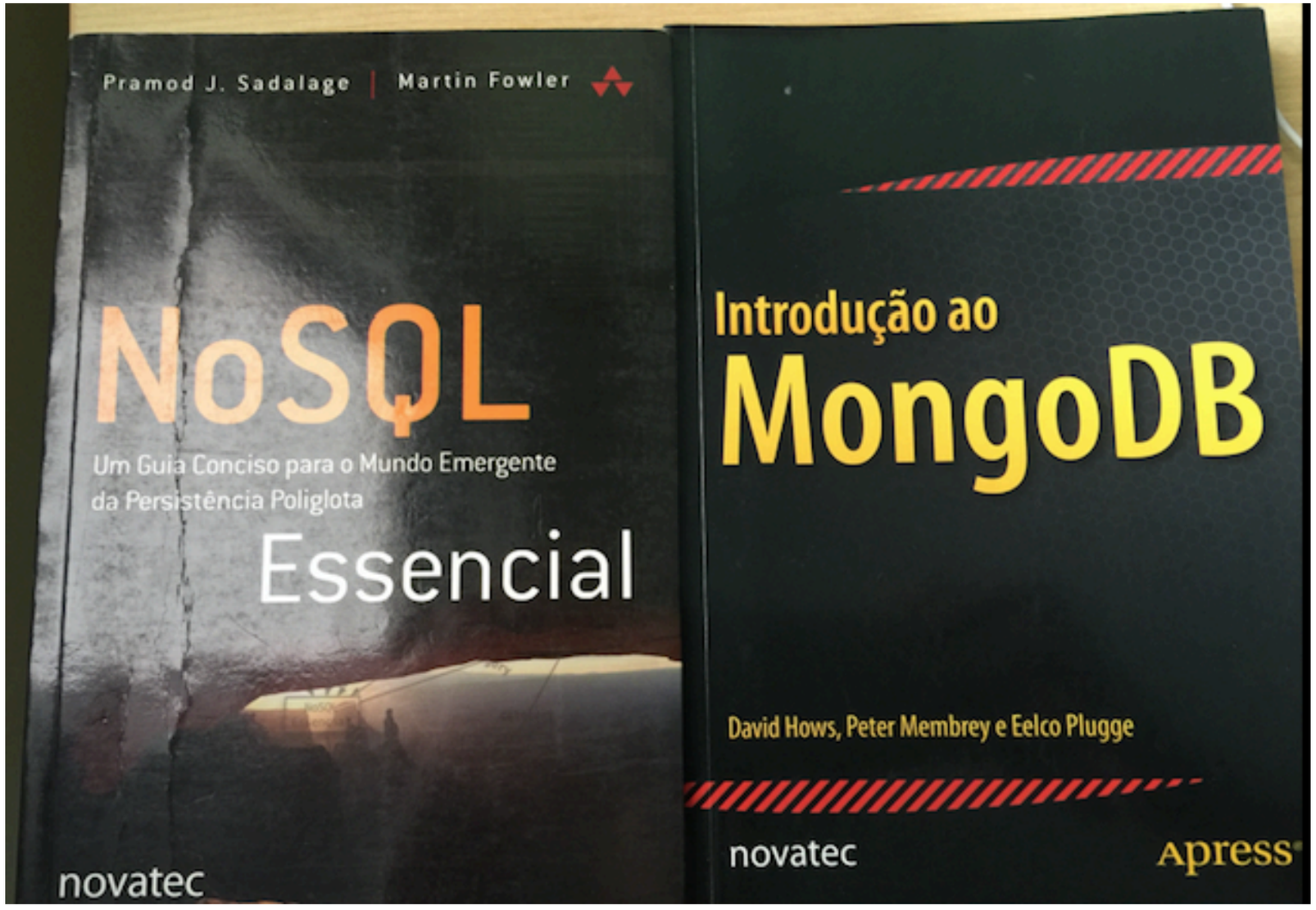


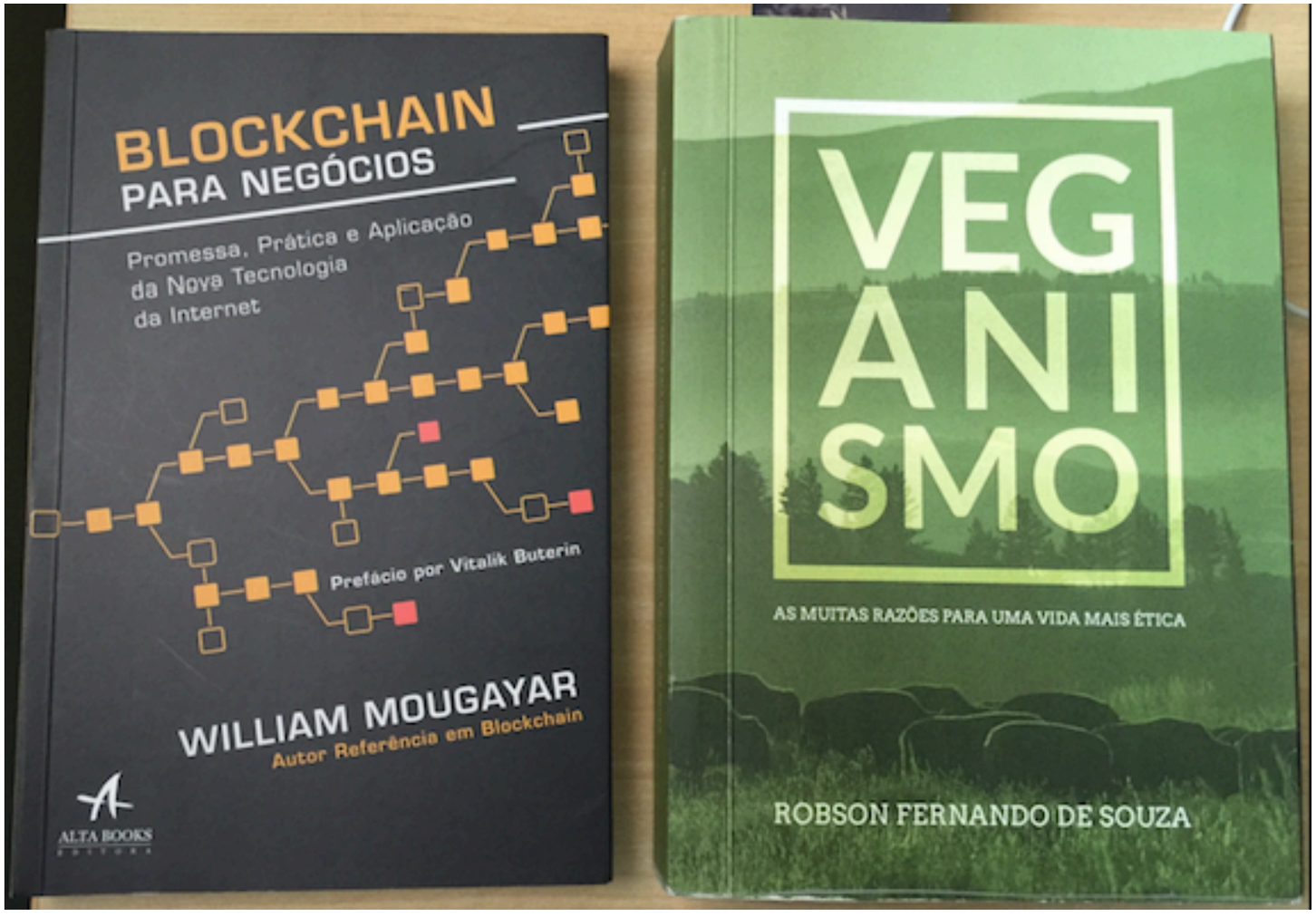
Figura 3. Integração entre a *blockchain* e o IPFS

Referências:

- **Artigo: https://goo.gl/cXfbYS**
- **White Paper BlockChain: https://bitcoin.org/bitcoin.pdf**
- **Livro Mastering Bitcoin: https://github.com/bitcoinbook**
- **BigchainDB white paper: https://www.bigchaindb.com/whitepaper/**
- **IPFS white paper: https://goo.gl/QfSWc2**
- **Melhor artigo sobre blockchain que já li: https://goo.gl/6v6yfp**


O'REILLY
Mastering
Bitcoin
UNLOCKING DIGITAL CRYPTOCURRENCIES
Andreas M. Antonopoulos
INTRODUÇÃO À
CRIPTOGRAFIA
novatec
Marcelo Ferreira Zoc


Pramod J. Sadalage | Martin Fowler
NoSQL
Um Guia Conciso para o Mundo Emergente
da Persistência Poliglota
Essencial
novatec
Introdução ao
MongoDB
David Hows, Peter Membrey e Eelco Plugge
novatec
Apress


BLOCKCHAIN
PARA NEGÓCIOS
Promessa, Prática e Aplicação
da Nova Tecnologia
da Internet
Prefácio por Vitalik Buterin
WILLIAM MOUGAYAR
Autor Referência em Blockchain
ALTA BOOKS
VEG
ANI
SMO
AS MUITAS RAZÕES PARA UMA VIDA MAIS ÉTICA
ROBSON FERNANDO DE SOUZA