# Criptografia no Blockchain


**Danilo Gazzoli Resende**

 danilo.gazoli@gmail.com

 /in/daniloresende/

 /danilogazzoli


Disciplina: Introdução à Criptografia

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

# Motivação

- O primeiro trabalho em uma cadeia de blocos criptograficamente segura foi descrito em 1991 por Stuart Haber e W. Scott Stornetta.
- 2008: Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System
- O comércio na Internet tem dependido quase exclusivamente de instituições financeiras que servem como terceiros confiáveis para processar pagamentos eletrônicos
- O custo da mediação aumenta os custos de transação
- O que é necessário é um sistema de pagamento eletrônico baseado em prova criptográfica em vez de confiança, permitindo a quaisquer duas partes dispostas a transacionar diretamente uma com a outra sem a necessidade de um terceiro confiável
- Transações que são computacionalmente impraticáveis de reverter protegeriam os vendedores de fraudes e mecanismos rotineiros de disputa poderiam ser facilmente implementados para proteger os compradores.

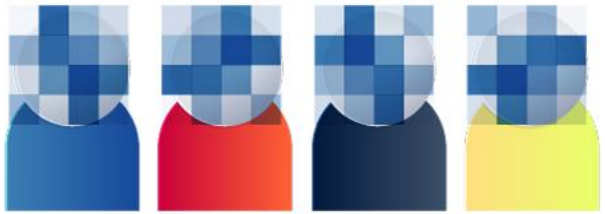
# O que é o Blockchain

- O blockchain (cadeia de blocos) é um registro público de transações de Bitcoin em uma ordem cronológica. A cadeia de blocos é compartilhada entre todos os usuários de Bitcoin. É usado para verificar a permanência de transações de Bitcoin e evitar o problema de “double spending”.
- Double spending: se um usuário malicioso tenta gastar suas bitcoins em dois recepientes diferentes ao mesmo tempo.
- Servidor distribuído peer-to-peer para gerar prova computacional da ordem cronológica das transações

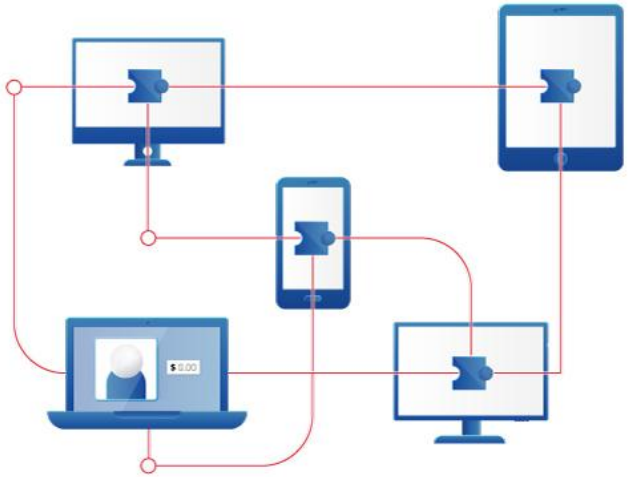
# O que é o Blockchain

The blockchain is **a database of information.**

This information is not stored in a single place, but **across a variety of data servers that participate in the network**, this is what is meant by "decentralised", there is no central point.



Identities are kept **completely private**, through the cryptography, however all transactions that happen on the blockchain are open to viewing by anyone at any time for always.

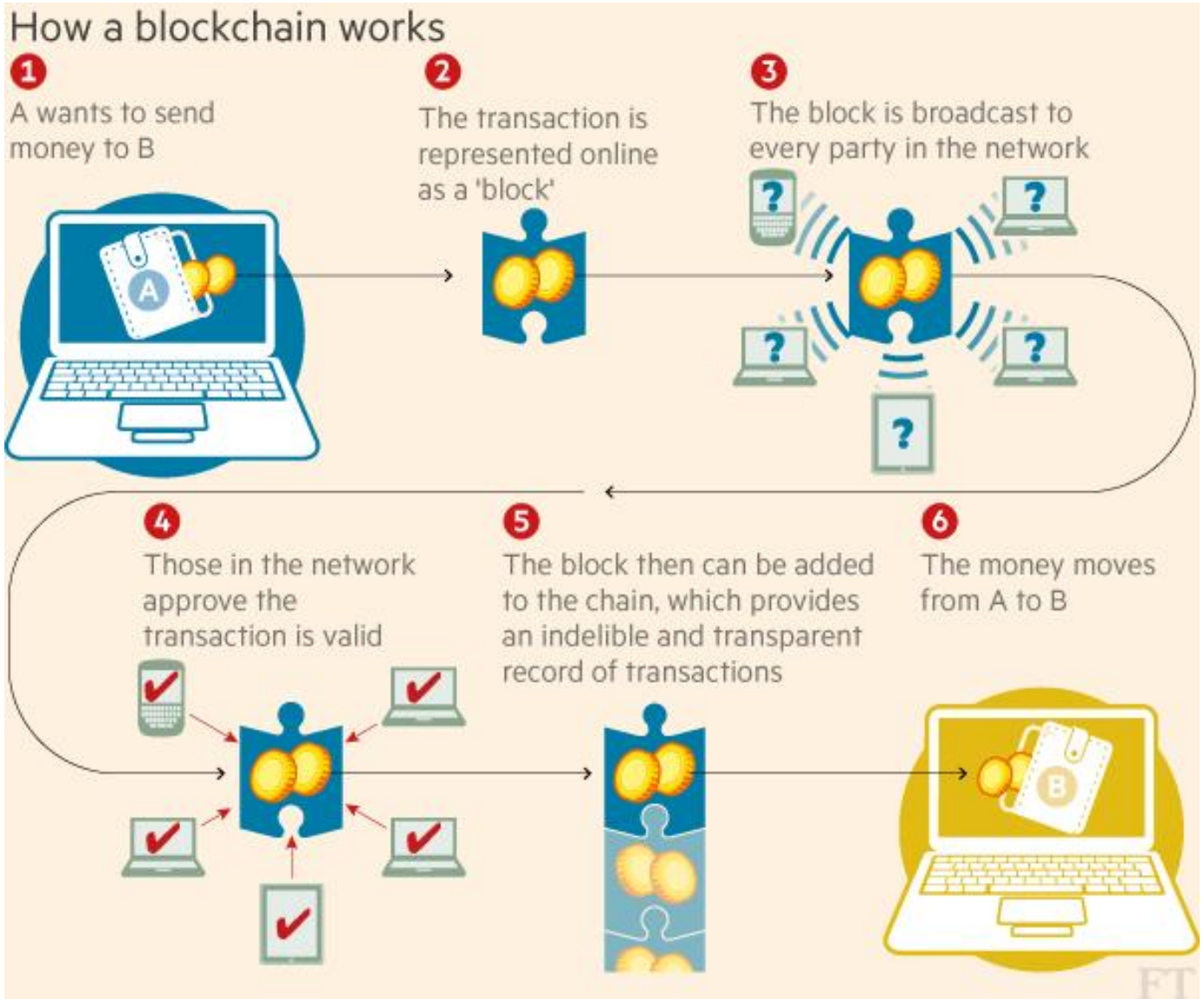


**Trust in the blockchain** is enough to transact with anyone

Every record that's written on a blockchain is secured by a unique cryptographic key, making the blockchain and its information **immutable**.

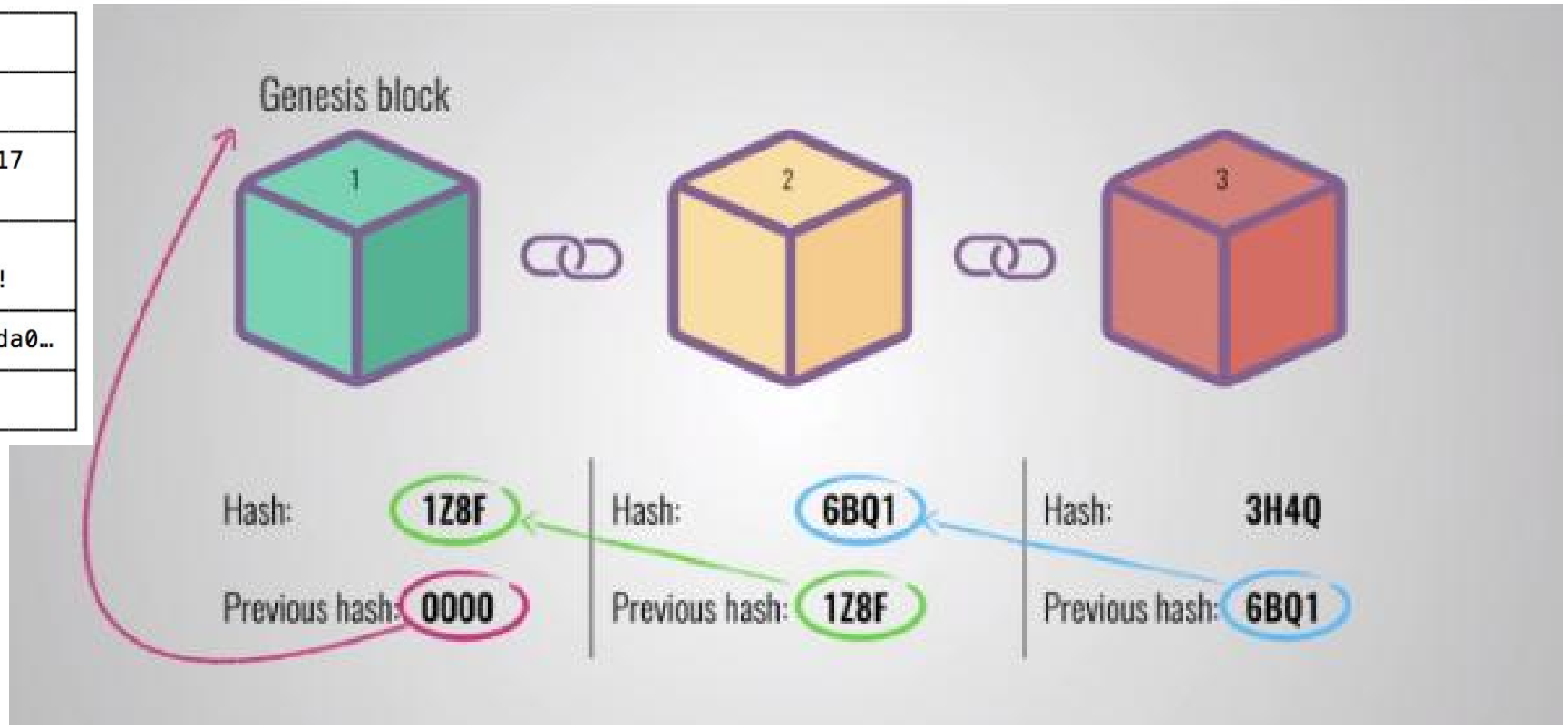
Lisk

# Como funciona o Blockchain



# Porquê uma cadeia?

| Genesis Block | |
|---|---|
| Previous Hash | 0 |
| Timestamp | Thu, 27 Jul 2017 02:30:00 GMT |
| Data | Welcome to Blockchain CLI! |
| Hash | 0000018035a828da0… |
| Nonce | 56551 |

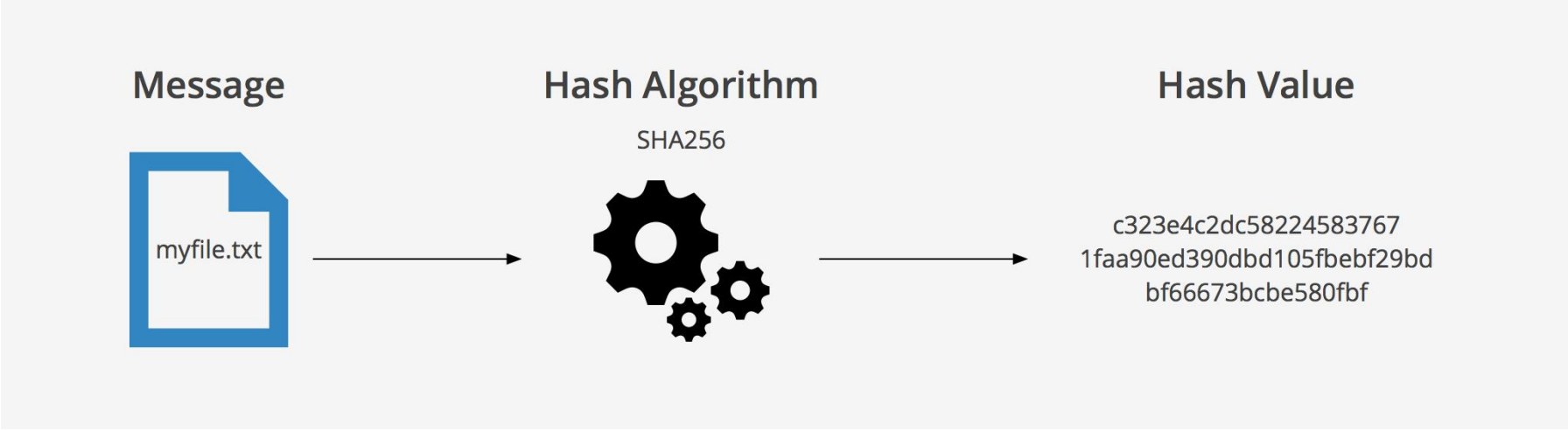



Cada registro escrito no blockchain é assegurado por uma única chave criptográfica. Quando um novo bloco é adicionado à cadeia, tudo do bloco anterior, inclusivo sua chave, é colocado na fórmula para gerar a chave do segundo registro. Esta interação cria independência. Quando um terceiro bloco é criado, os conteúdos e chaves dos dois primeiros blocos são colocados na fórmula para resultar na chave do terceiro registro. Esta dependência encadeia todos os registros.

# Block Hashing

- Hashing é o processo de obter uma entrada de qualquer tamanho e convertê-la para uma saída de comprimento fixo através de um algoritmo matemático.

- Bitcoin usa SHA-256



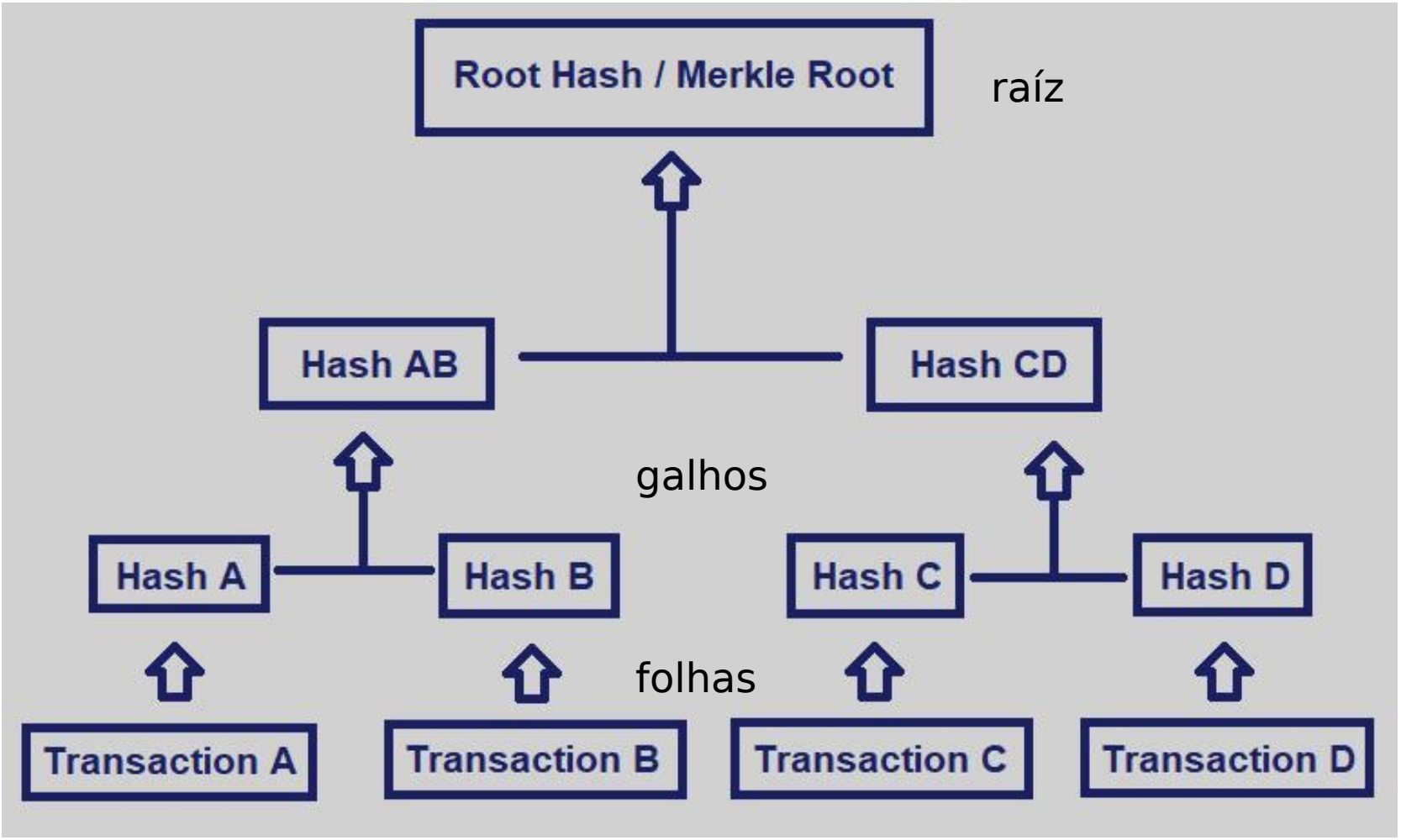
# Funcionamento da Árvore de Merkle

- Uma árvore de Merkle sumariza todas as transações em um bloco ao produzir um "fingerprint" digital de todo o conjunto de transações, o que possibilita um usuário verificar se a transação está ou não incluída em um bloco.

- Árvores de Merkle são criadas repetidamente ao fazer o "hashing" de pares de nós até que haja somente um hash (Root).

- Cada nó folha é um hash de dados transacionais e cada nó não folha é um hash dos hashes anteriores.

# Hash Tree ou Merkle Tree



# Benefícios da Árvore de Merkle

- 1. Fornece um meio de provar a integridade e validade de um dado
- 2. Requerem pouco espaço de disco/memória visto que as provas são computacionalmente fáceis e rápidas
- 3. Suas provas e gerenciamento exigem somente pequenas porções de informação para serem transmitidas pela rede

# Referências


- Nakamoto S. *Bitcoin: a peer-to-peer electronic cash system*. Disponível em: <http://bitcoin.org/bitcoin.pdf>. Acesso em 01 jun. 2019.
- Ray, S. *Merkle Trees*. Disponível em: <https://hackernoon.com/merkle-trees-181cb4bc30b4>. Acesso em 01 jun. 2019.
- *Essentials of Blockchain Cryptography*. Disponível em: <https://blog.bankex.org/essentials-of-blockchain-cryptography-c60180f14b7f>. Acesso em 01 jun. 2019.
- *Blockchain Basics*. Disponível em: <https://lisk.io/academy/blockchain-basics>. Acesso em 01 jun. 2019.
- *O QUE É A TECNOLOGIA BLOCKCHAIN?.* Disponível em: <http://datascienceacademy.com.br/blog/o-que-e-a-tecnologia-blockchain/>. Acesso em 01 jun. 2019.