



LIVRO RAZÃO

B

L	O	C	K
C	H	A	I

N

CADEIA DE BLOCOS



Fundamentos do Blockchain

Conceitos Primais do Blockchain

O Blockchain (cadeia de blocos imutáveis) ou Livro Razão (Ledger) que registra e processa informações ou documentos digitais (à prova de adulteração) é possível, grosso modo, devido a dez tecnologias computacionais:

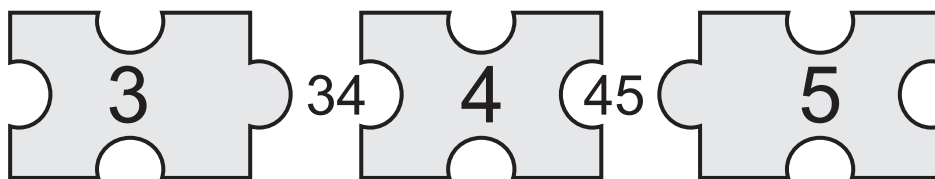
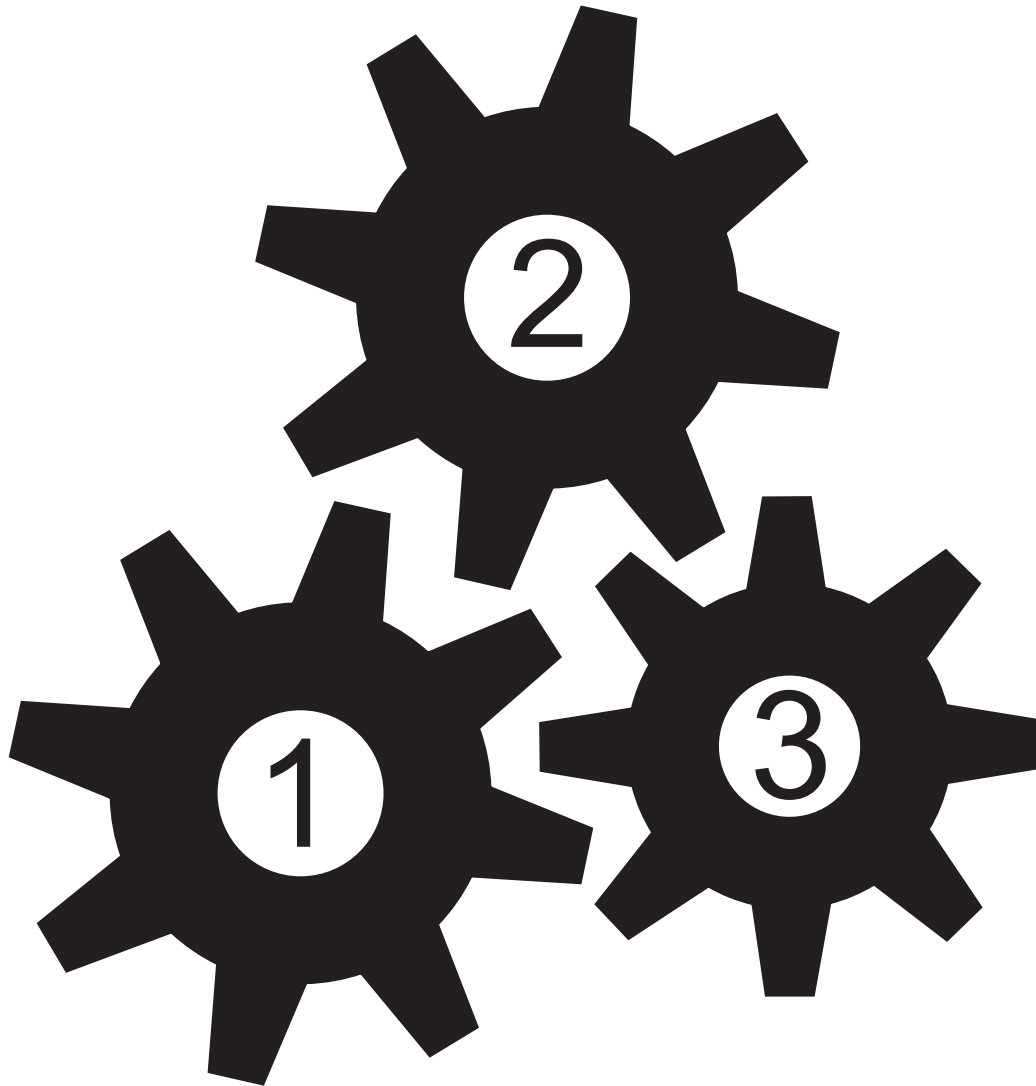
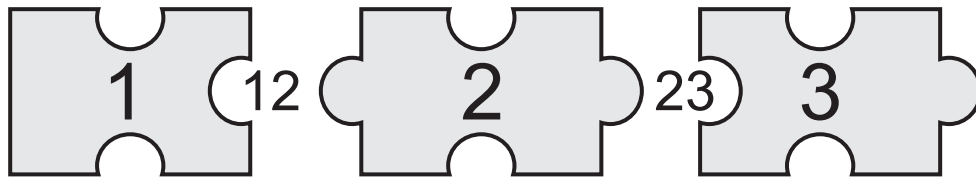
- 1.0 Blocos de Dados Interligados
- 2.0 Dados Distribuídos em Rede
- 3.0 Dados/Informações Criptografadas
- 4.0 Chave Criptográfica Pública
- 5.0 Smart Contract/Protocolo Efetivo
- 6.0 Ataque Percolativo / $50\% + 1$
- 7.0 Matemática de Consenso
- 8.0 Algoritmo Hash - 256
- 9.0 Livro-Razão Inviolável
- 10.0 Fork/Undecided Blockchain
- 11.0 Backen-as-a-Service

Os mineradores ou validadores desses documentos ganham pelo esforço computacional tokens/bitcoins, caso acertem o nonce (solução de um problema matemático)

Cadeia de Documentos Imutáveis



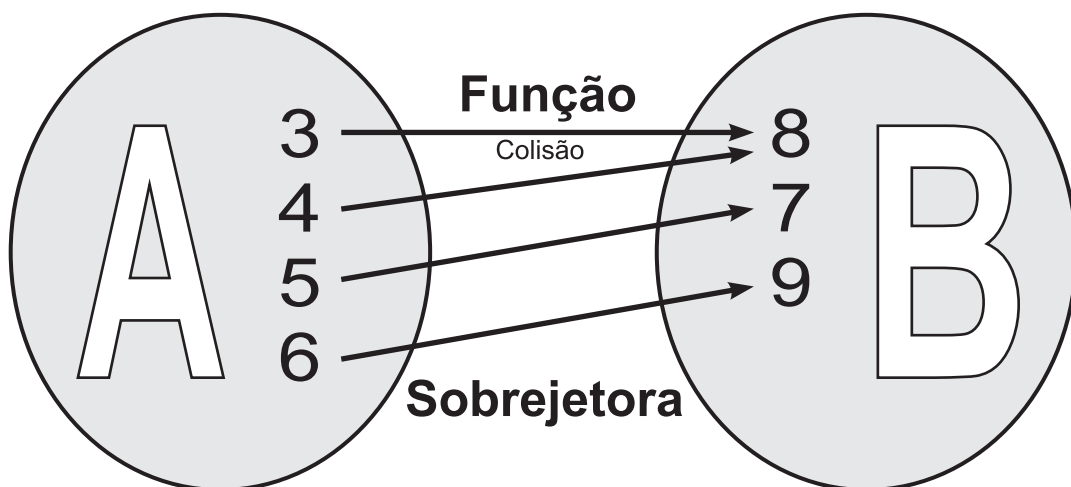
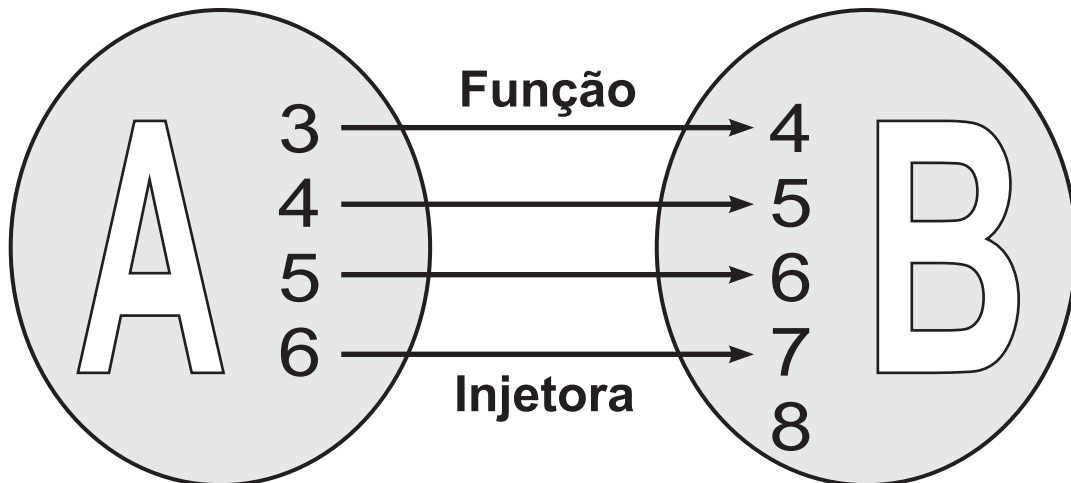
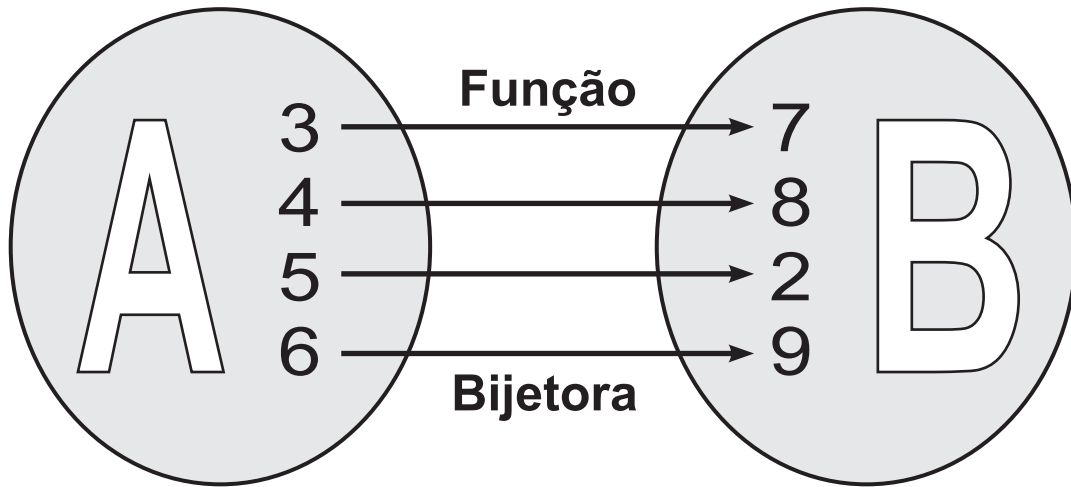
1.0 Blocos de Dados Interligados



Interconnected Data (I∞D)



8.1 Função Hash \equiv Função Bijetora



Bijetora: Para cada Entrada uma Saída



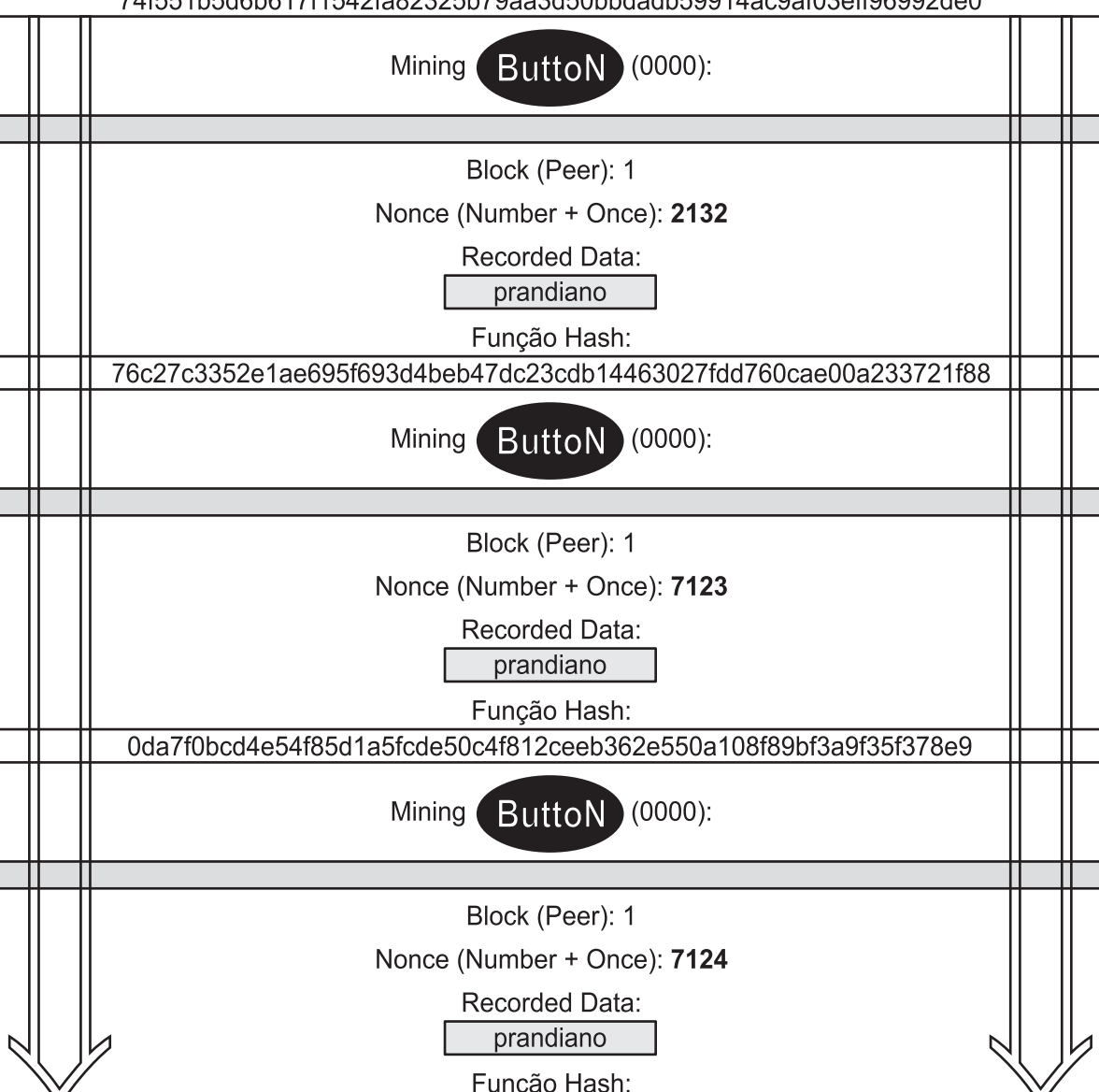
Block (Peer): 1
 Nonce (Number + Once): 72608
 Recorded Data:
 prandiano
 Função Hash:
 0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a
 Mining **ButtoN** (0000):

Block (Peer): 1
 Nonce (Number + Once): **72608**
 Recorded Data:
 prandiano
 Função Hash:
 74f551b5d6b617f1542fa82325b79aa3d50bbdad59914ac9af03eff96992de0
 Mining **ButtoN** (0000):

Block (Peer): 1
 Nonce (Number + Once): **2132**
 Recorded Data:
 prandiano
 Função Hash:
 76c27c3352e1ae695f693d4beb47dc23cdb14463027fdd760cae00a233721f88
 Mining **ButtoN** (0000):

Block (Peer): 1
 Nonce (Number + Once): **7123**
 Recorded Data:
 prandiano
 Função Hash:
 0da7f0bcd4e54f85d1a5fcde50c4f812ceeb362e550a108f89bf3a9f35f378e9
 Mining **ButtoN** (0000):

Block (Peer): 1
 Nonce (Number + Once): **7124**
 Recorded Data:
 prandiano
 Função Hash:
 0000b58ef8e57305f6d23c5b1fb620b61af412822a1db32e39c94b9b9ff6b74a6
 Mining **ButtoN** (0000):





BaaS

11.0 Backend-as-a-Service

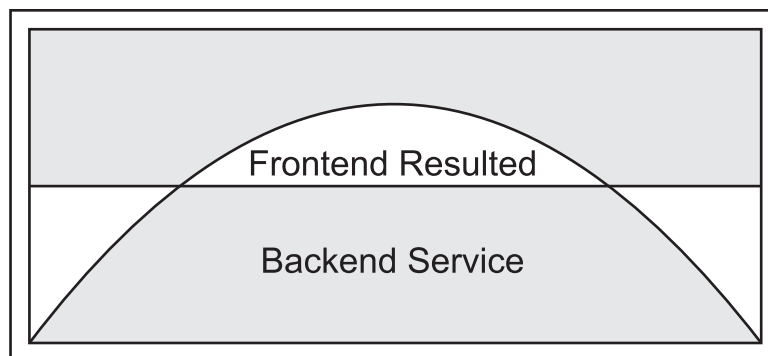
Huawei Cloud
Softwares Industriais

Exemplos

Amazon Managed
Softwares Comerciais

Tecnologia distribuída para desenvolvedores de aplicativos *mobile* e *web* que podem acessar blocos de programações imutáveis, prontos para serem usados com um mínimo esforço, quando e onde poderão juntá-los (“quantos forem”) para certa finalidade computacional.

Mobile



Web

Essa possibilidade (*middleware*) do Blockchain, gerar e armazenar blocos de código computacional, permite economia de tempo e principalmente de recursos para se construir, homologar e instalar aplicativos, uma vez que não se começa um projeto da estaca zero.

Facebook BaaS
Softwares Comportamentais

Exemplos

J.P. Morgan BaaS
Softwares Bancários

Frontend-as-a-Result

FaaS