Muito além das criptomoedas: Blockchain no governo

Prodasen

Outubro de 2018

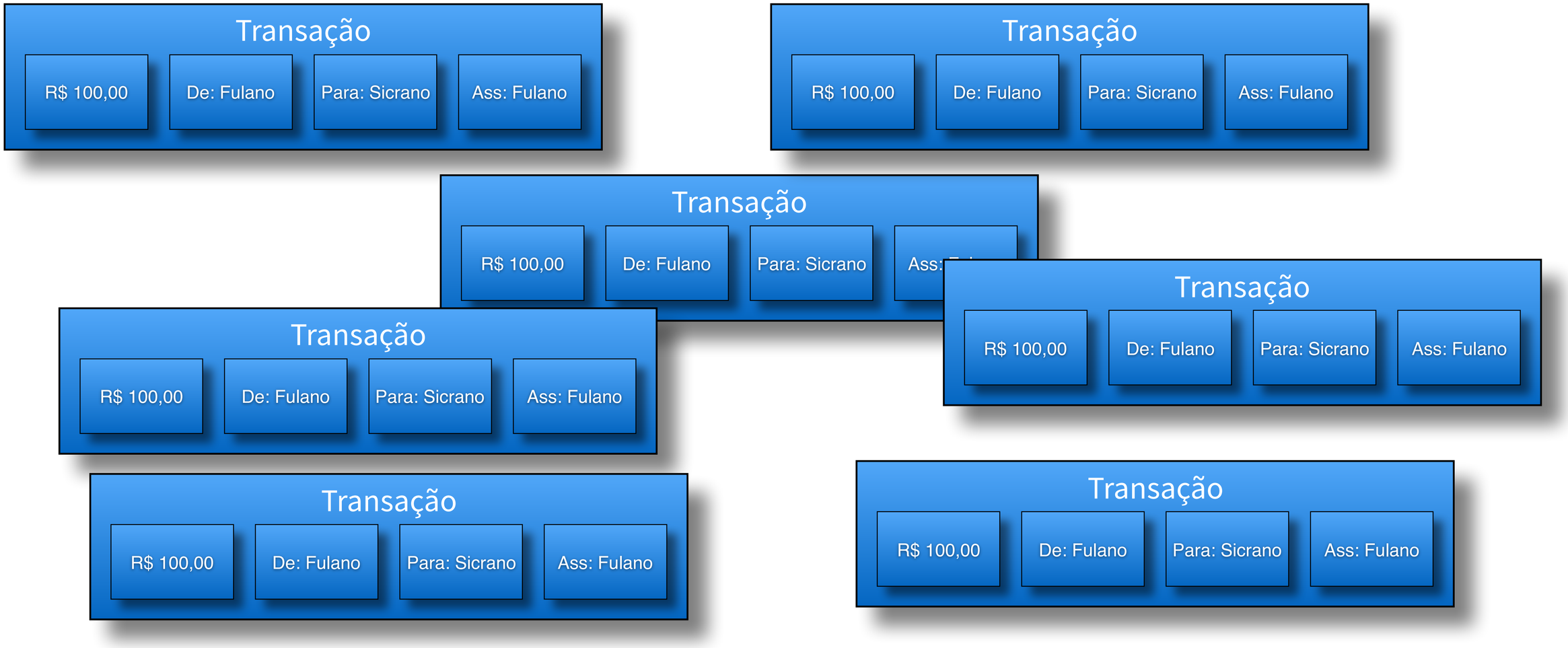
João Ferreira

Blockchain

Transação

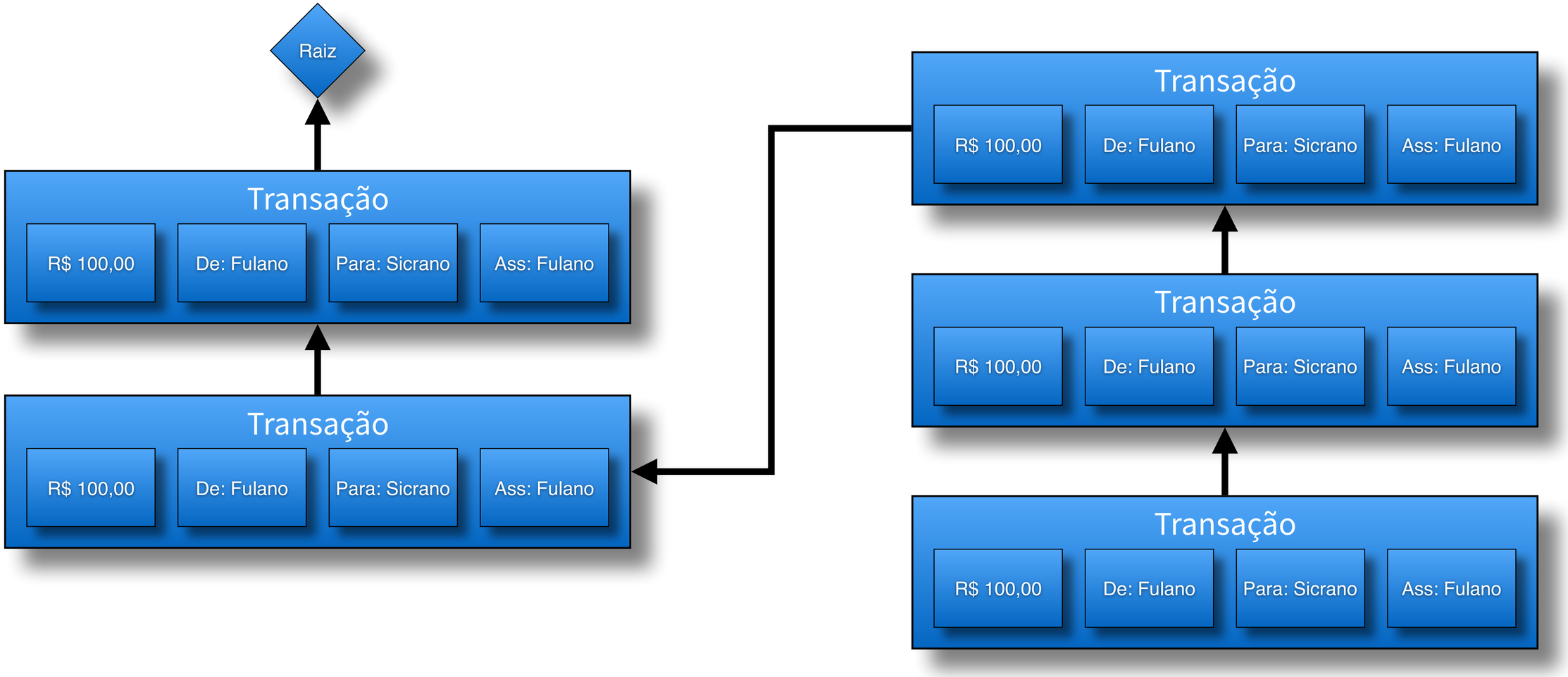
Transação

Conjunto de transações



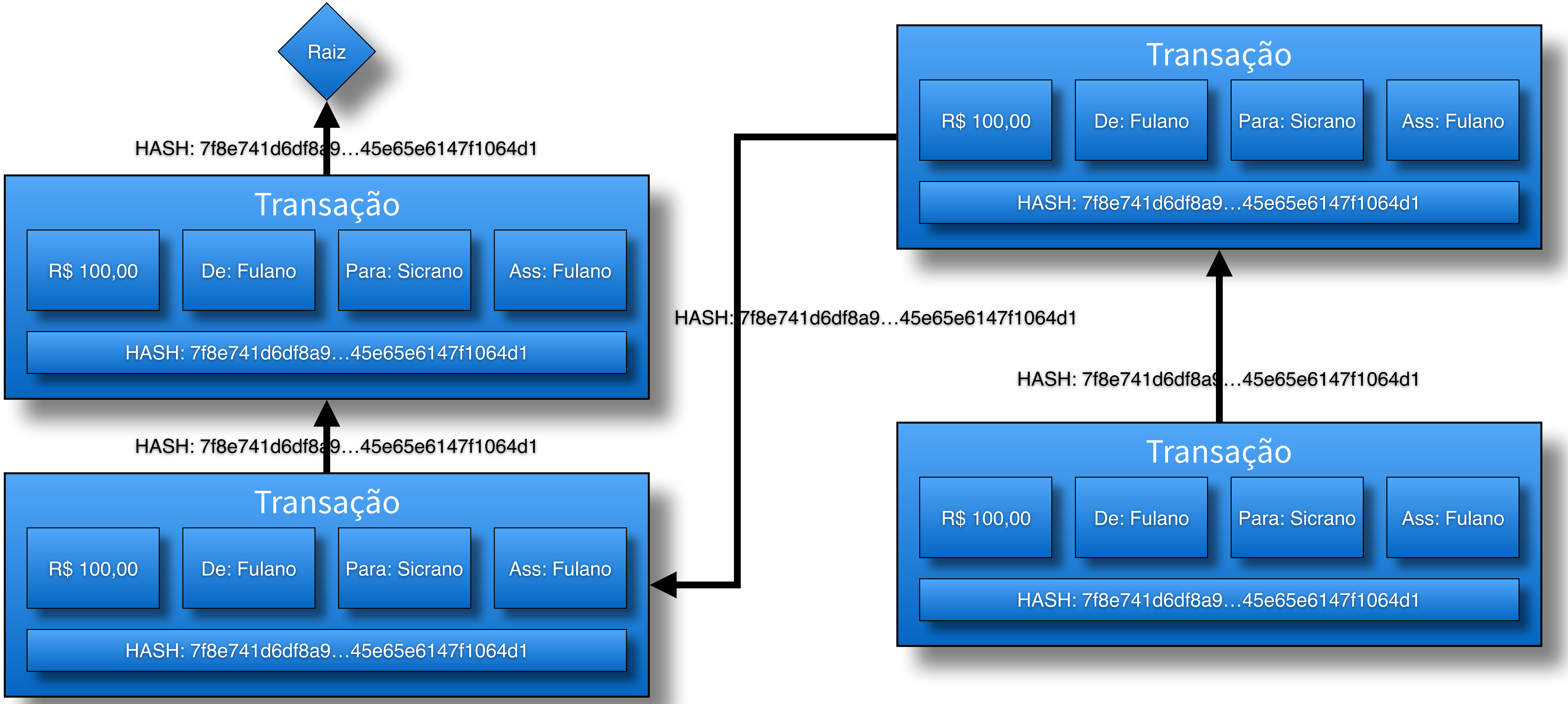
Ordenação: Lista encadeada de transações

Ordenação: Lista encadeada de transações



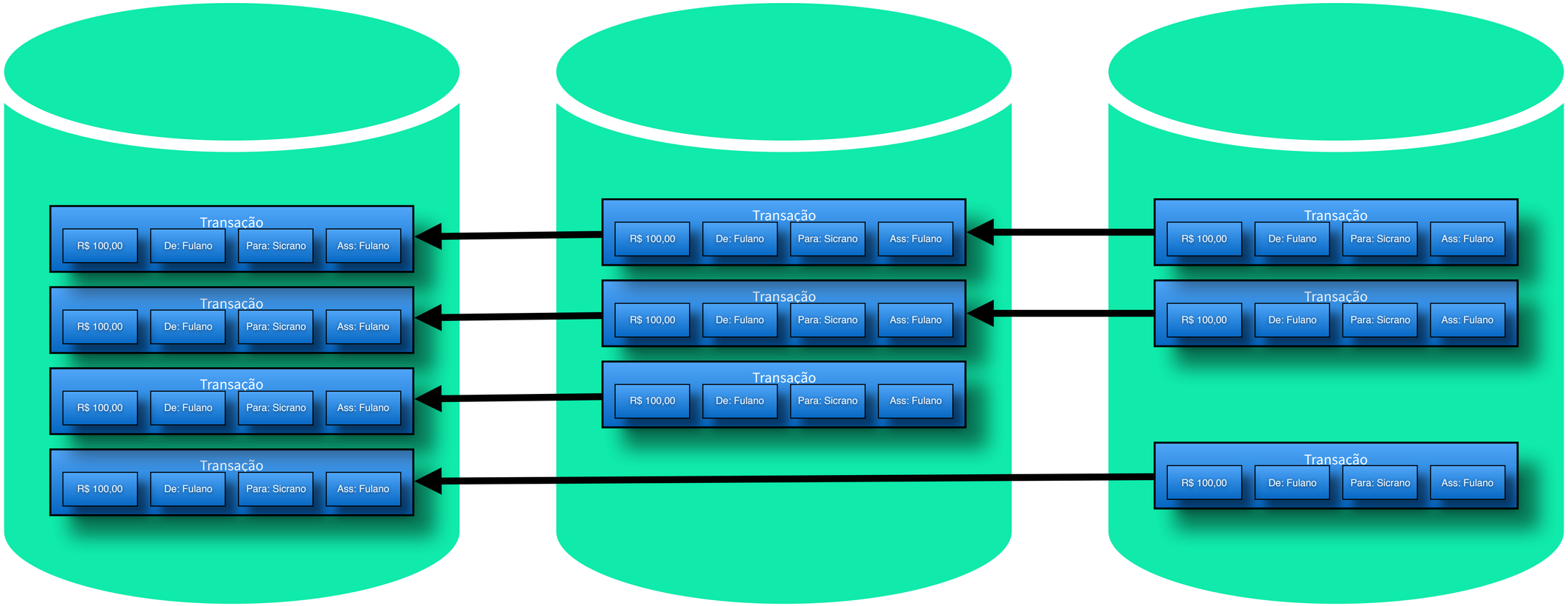
Indexação: hashes

Indexação: hashes

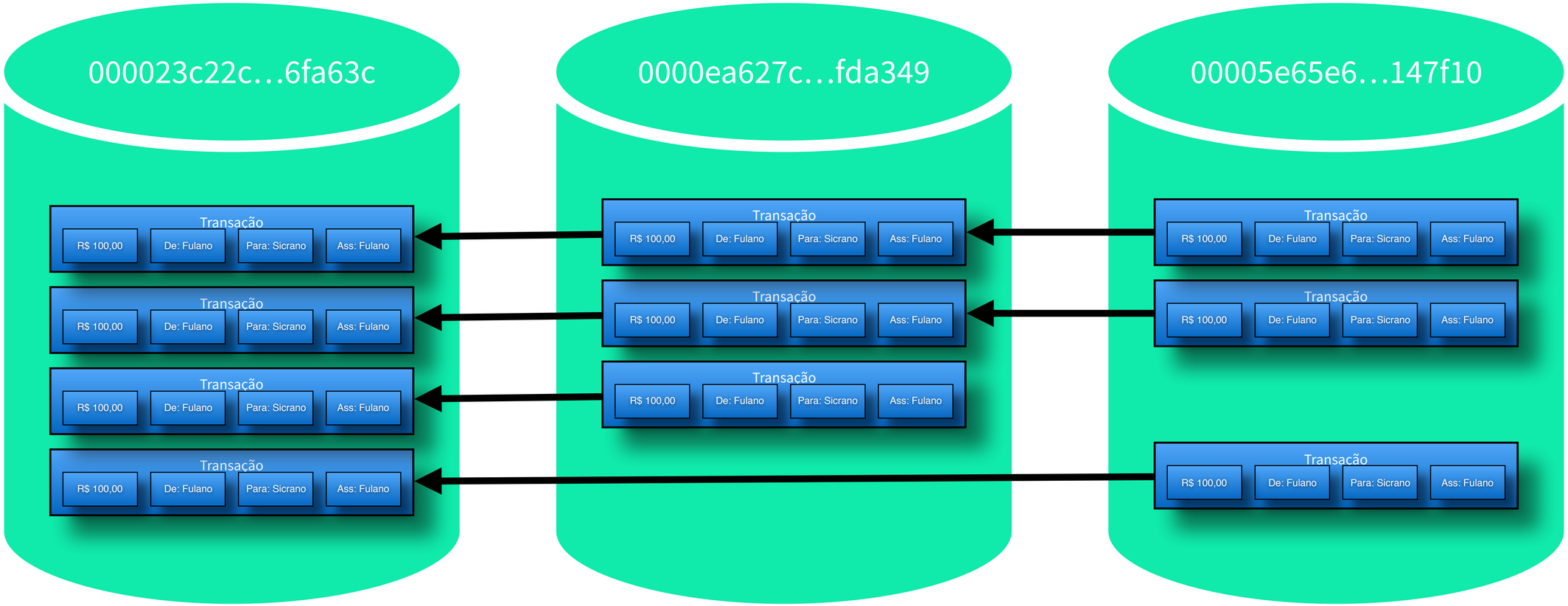


Agrupamento: Blocos

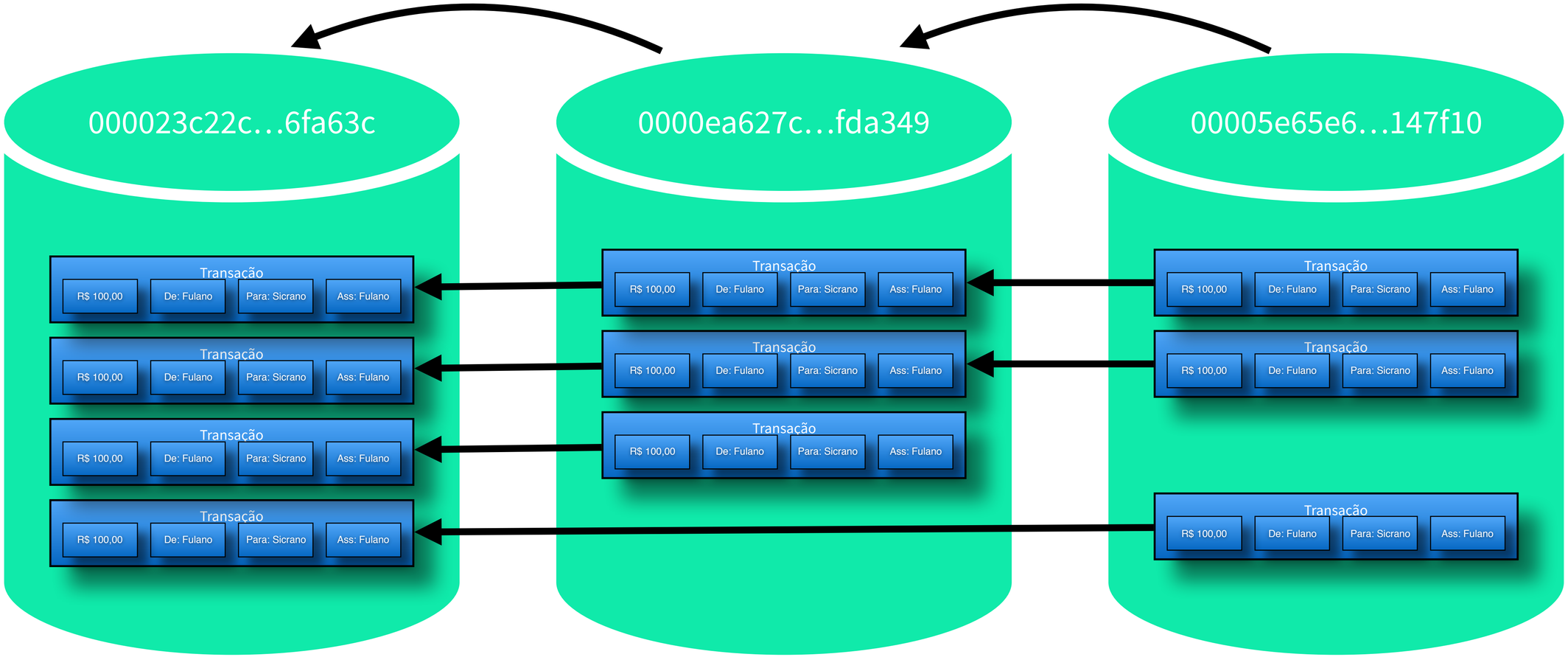
Agrupamento: Blocos



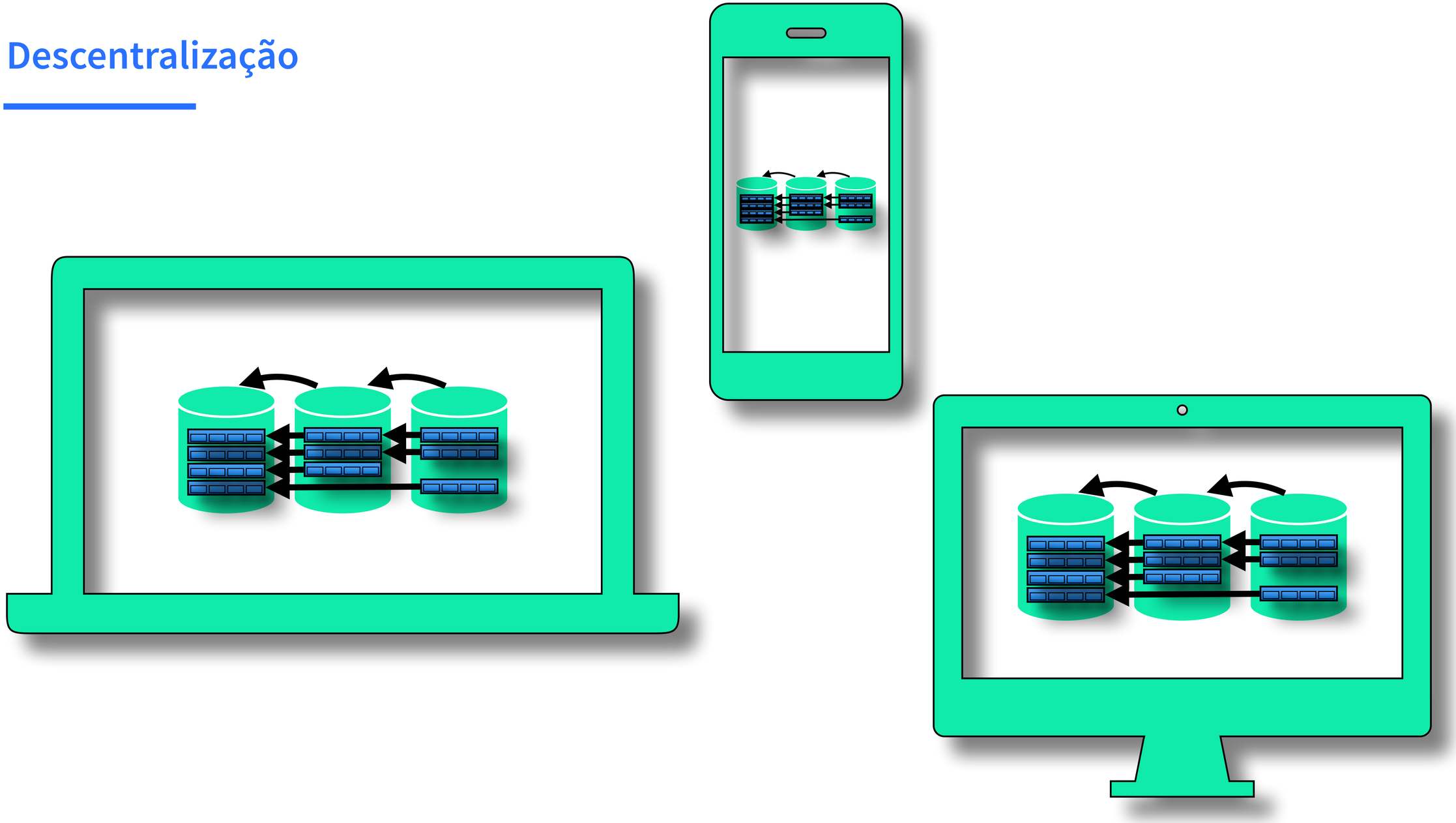
Timestamping: Protocolo de consenso



Timestamping: Protocolo de consenso



Descentralização



Quem pode escrever na blockchain?

- Algoritmo de consenso
    - Problema dos Generais Bizantinos Iterado
- Timestamping (protocolo/marcação de tempo)
- Regras de consenso
    - Imutáveis

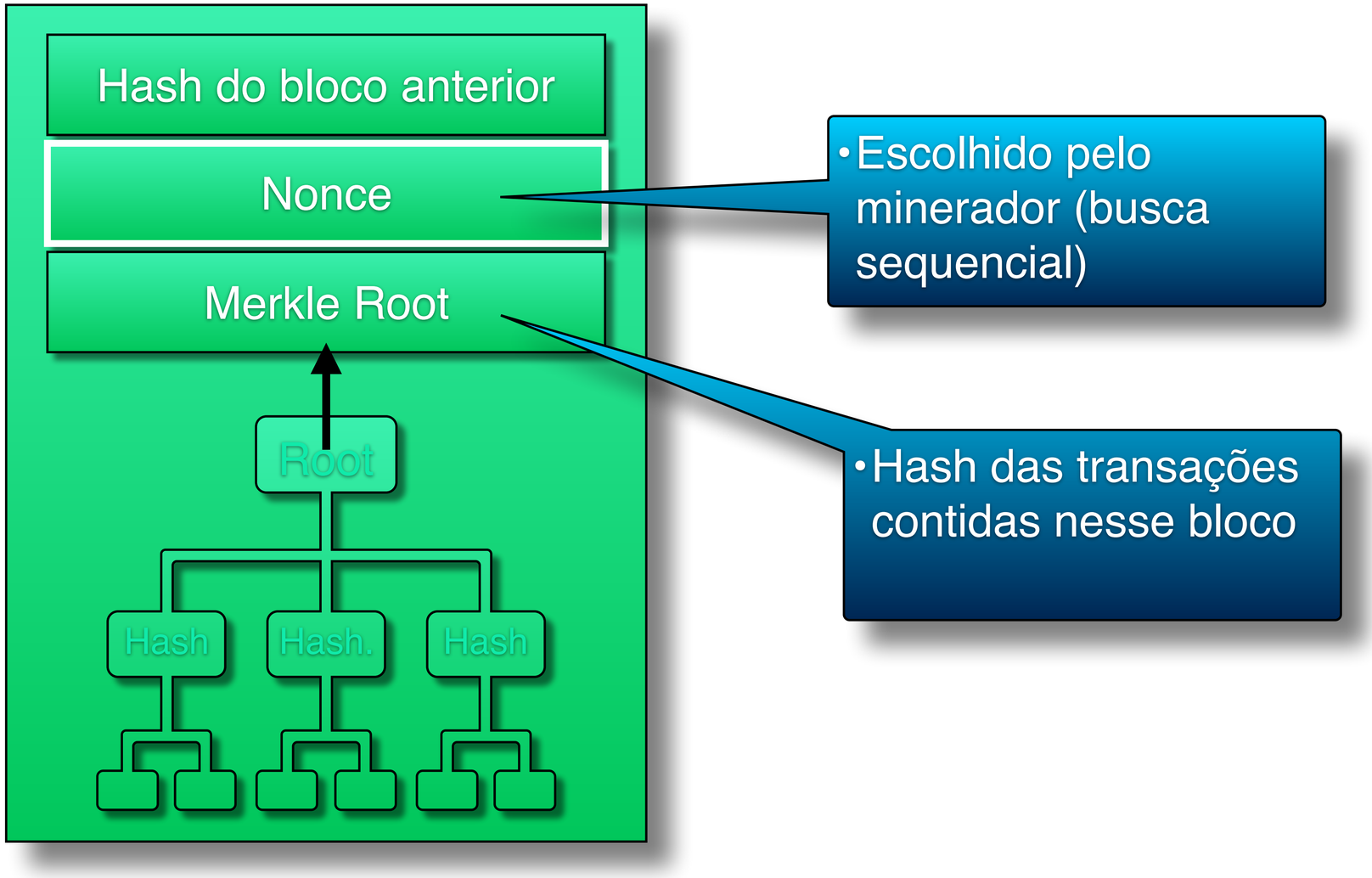
Bitcoin

- Prova de Trabalho (PoW)
  - HashCash
- Gameficação
  - Emissão de moedas
  - Taxas de transação

Mineração

- Prova de Trabalho
    - Difícil de Calcular, Fácil de verificar
- HashCash
    - Encontrar uma hash menor que a dificuldade
    - Tempo médio entre blocos previsível no longo prazo
    - Dificuldade ajustada a cada 2 semanas
- Validam as transações (regras de consenso)
    - Blocos inválidos são rejeitados pelos outros mineradores

Mineração: Cabeçalho dos blocos



Outros algoritmos de consenso

- Proof of Stake (PoS)
- Proof of Activity (PoW + PoS)
- Proof of Authority
    - Blockchains privadas
- Practical Byzantine Fault Tolerance
    - Hyperledger

Transaction Scripts

Transaction Scripts

OP_RETURN

OP_RETURN


Transação
R$
100,00
De:
Fulano
Ass:
Fulano
OP_RETURN <Dados opcionais até 80 bytes>

Smart Contracts

Smart contracts

- Processamento de dados descentralizado
- Não são contratos
    - São arbitradores eletrônicos
- Dapps
    - Aplicações que interagem com a blockchain usando smart contracts

Smart Contracts

- Bitcoin
  - Scripts simples
  - Não são *Turing complete*
  - Previstos nas regras de consenso
    - Novos OP_CODES exigem *hard fork*

Smart Contracts

- Ethereum
  - Linguagem de alto nível
    - Solidity, etc
  - Turing Complete
  - Estende regras de consenso
  - DAPPs

Smart contracts

- Customizar blockchain públicas
    - Vantagens
        - Segurança
        - Estabilidade
        - Facilidade
    - Desvantagens
        - Custo
        - Flexibilidade

Smart Contracts: exemplos

- Bitcoin
  - Endereços multiassinados (P2SH)
  - Registros de dados (OP_RETURN)
  - Atomic Swap
  - Lightning Network

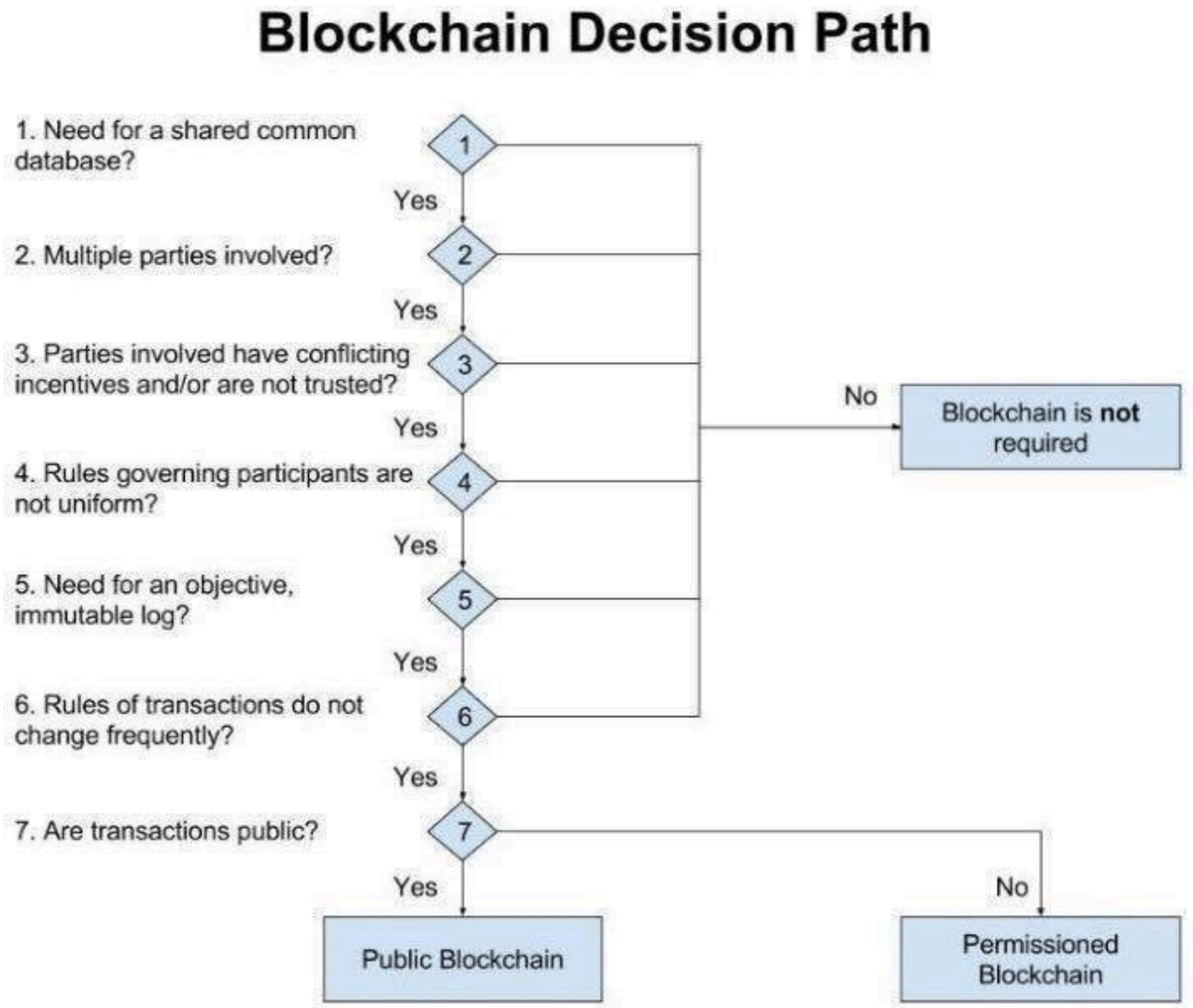
Smart Contracts: exemplos

- Ethereum
  - The DAO
    - Falhou, problemas de segurança
  - Tokens ERC20
  - Eleições eletrônicas

DAO: Organizações autônomas descentralizadas

- Decisões tomadas pelos stakeholders através de blockchain
- The DAO
    - Hackeado
- DASH
    - Criticas a pouca descentralizado
- Decred
    - Politeia
        - Registro de documentos offchain com rastro onchain
    - Criação de contratos dedicados
    - Permite o uso por terceiros (DAE)

Aplicações



Quando usar Blockchain?

- Descentralização custa caro
- Regras imutáveis
- Muitos atores
- Interesses conflitantes

Blockchain para registro financeiro

- SALT (Bacen)
    - Alternativa descentralizada ao SPB
    - https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf
    - Prova de conceito. Várias empresas e várias soluções foram testadas
- Bolsa de valores de Singapura
    - Emissão de ativos em blockchain, seguindo todas as regulamentações
    - Consensys
- BNDES token
    - https://www.bndes.gov.br/wps/portal/site/home/imprensa/noticias/conteudo/tecnologia-blockchain-sera-objeto-de-cooperacao-entre-bndes-e-kfw
- Holanda
    - subsídio parental

Blockchain para registros notariais

- Original my
    - Pioneira
    - Convenio com cartórios
- Portal de Assinaturas Certisign
- Registro de imóveis (Consensys)
    - Dubai
    - India
    - Holanda (prototipo)

Blockchain para comunicação e transparencia

- Pier (Bacen + SUSEP + CVM + Previc)
  - https://www.bcb.gov.br/pt-br/#!/c/noticias/249
- Governo de Dubai
  - Blockchain como principal ferramenta de comunicação governamental
  - Diversas iniciativas
- Holanda
  - Diversas iniciativas

Identidade em Blockchain

- Uport
  - Iniciativa livre / Linux Foundation
- Blockchain ID
  - Original My
- Portal de Assinaturas Certisign
  - Sovrin + ERC-725
- MPOG
  - Microsoft + Consensys
  - Registro unificado (CPF, RG, CNH, PIS, etc)
  - Baseado em Uport
- Internacional
  - India

Legislativo

- Mudamos
  - Leis de iniciativa popular
  - ITS Rio (Ronaldo Lemos)
  - Assinatura em blockchain
  - Aceito pela Câmara de João Pessoa


O que falta?

Potenciais usos de blockchain no governo

- Elaboração orçamentária
  - Orçamento participativo
  - Fiscalização e controle descentralizados
- Registro de propriedade intelectual
  - Remuneração direta (Elimina entidades como ECAD, MPAA, etc)

Proposta de blockchain legislativa

- Tramitação e registro de proposições legislativas
  - Transparencia
  - Registro histórico incorruptível
  - *Non repudiation*
  - Responsabilização

Agradecimentos

Agradecimentos

- Marcelo Amarante Ferreira Gomes (Prodasen)
- Patricia Cunha (Prodasen)
- Claudio Santana (Bacen)
- Valdo Noronha (Bacen)
- Paulo Henrique Araújo (Câmara dos deputados)
- Gustavo Rodrigues Silveira (Ministério do Planejamento)
- Marcelo Dutra (CLDF)
- Daniel Novy (Consensys - Dubai, India e Brasil)
- Edilson Osório Júnior (Original My)
- Carl Amorim (Blockchain Research Institute)
- Maria Tereza Aarao - Teka (Certisign)

Obrigado!

Prodasen

Outubro de 2018