



Aprender Economia
Projeto de Extensão da Unifal - MG



Conceitos básicos do Bitcoin

Aluno: José Carlos Tobias da Silva

Supervisor: Prof. Dr. Marcelo Lacerda Rezende

Cronograma

- Introdução
 - O Bitcoin
- Desmistificando Termos
 - Descentralização
 - *Blockchain* (Blocos Encadeados)
 - *Miners* (Mineradores)
- Transações
 - Carteiras
 - Verificações
 - Tipos básicos de transações
 - Exemplo de ciclo de vida de transação



INTRODUÇÃO



O Bitcoin

- Criptomoeda
 - Precursora do modelo empregado
- Surgimento
 - 31/10/2008:
 - *"A Peer-to-Peer Electronic Cash System"* por Satoshi Nakamoto
- Primeira transação
 - 01/03/2009

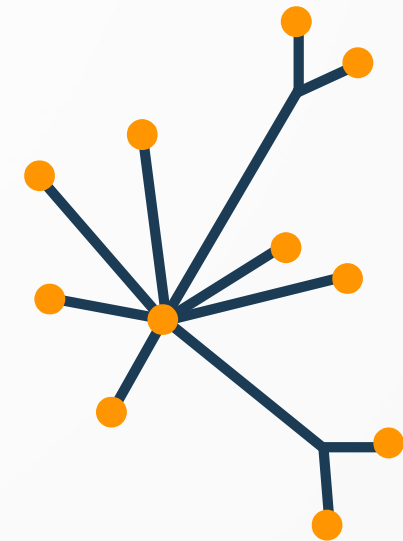


DESMISTIFICANDO TERMOS



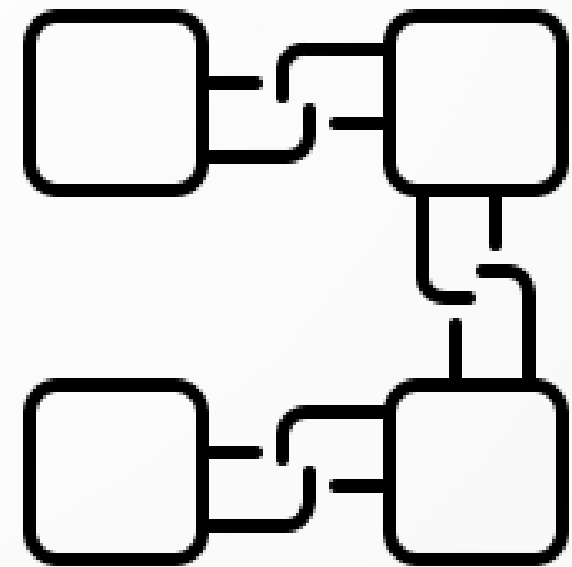
Descentralização

- Usuários são nós em uma rede
 - Executam ações de acordo com protocolos
- Não há mecanismo controlador central
 - Todos os usuários colaboram no funcionamento da rede
 - A rede se ajusta ao funcionamento sem intervenções



Blockchain (Blocos Encadeados)

- É um conjunto de protocolos
- Registro distribuído
 - Contém todas as transações feitas desde a criação da rede
- Principal inovação do Bitcoin
 - É a base para todas as criptomoedas atualmente, as vezes com pequenas alterações

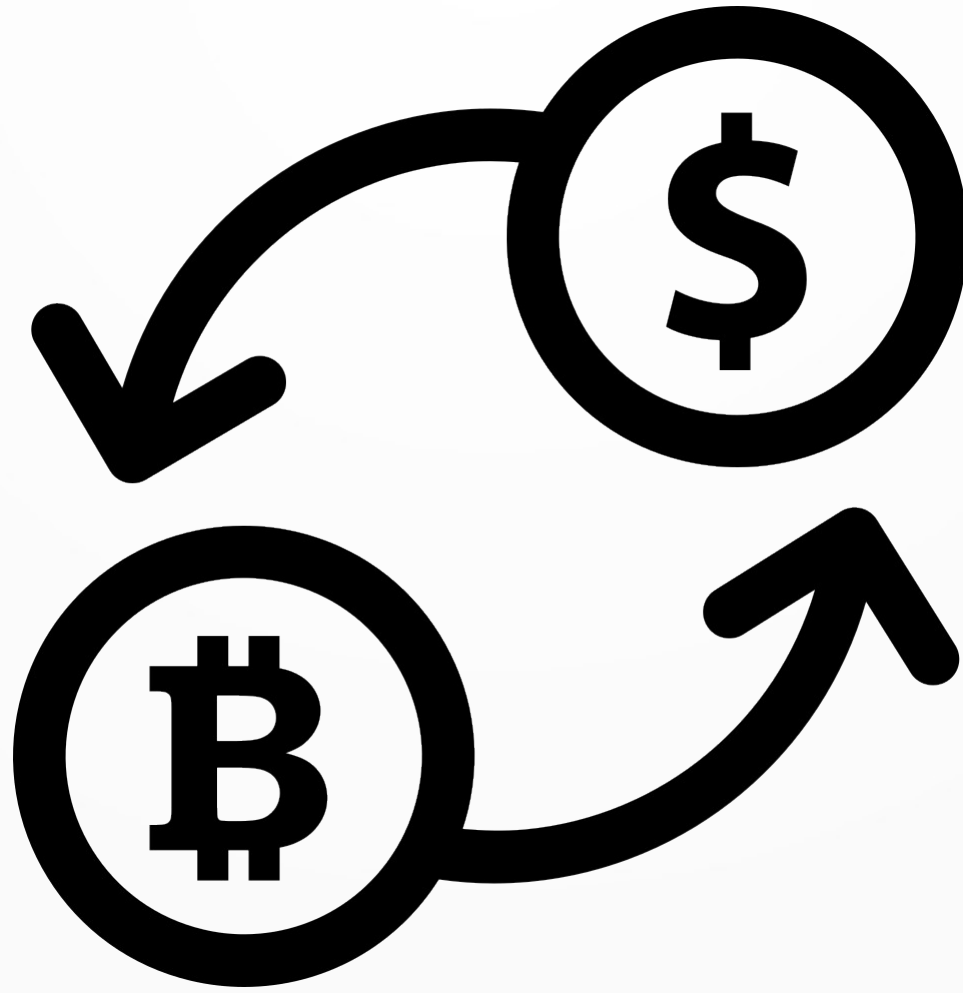


Miners (Mineradores)

- Confirmadores de transações
 - Executam o trabalho de juntar blocos de transações e adicioná-los ao *blockchain*
- Atividade é rentável
 - São remunerados fixamente com bitcoins por bloco confirmado, bem como pelos usuários com o pagamento de taxas opcionais
- Essenciais para o funcionamento da rede



TRANSAÇÕES



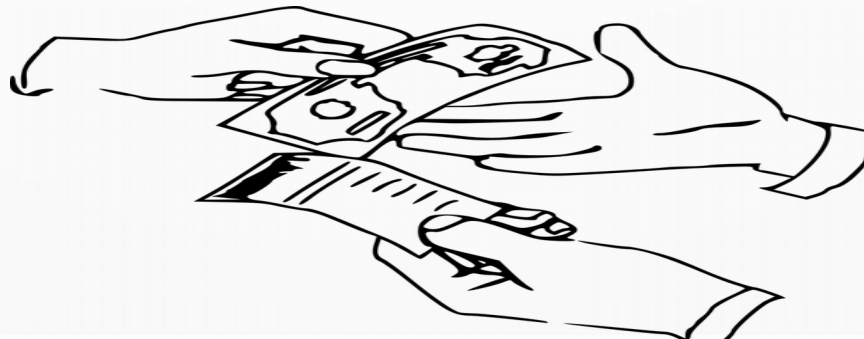
Carteiras

- Troca e monitoramento de quantias
- Empresas prestam serviços
 - Funcionalidades específicas
 - Fins variados
- Identificada por um endereço
 - *Bitcoin Address*
 - Conta de banco



Verificações

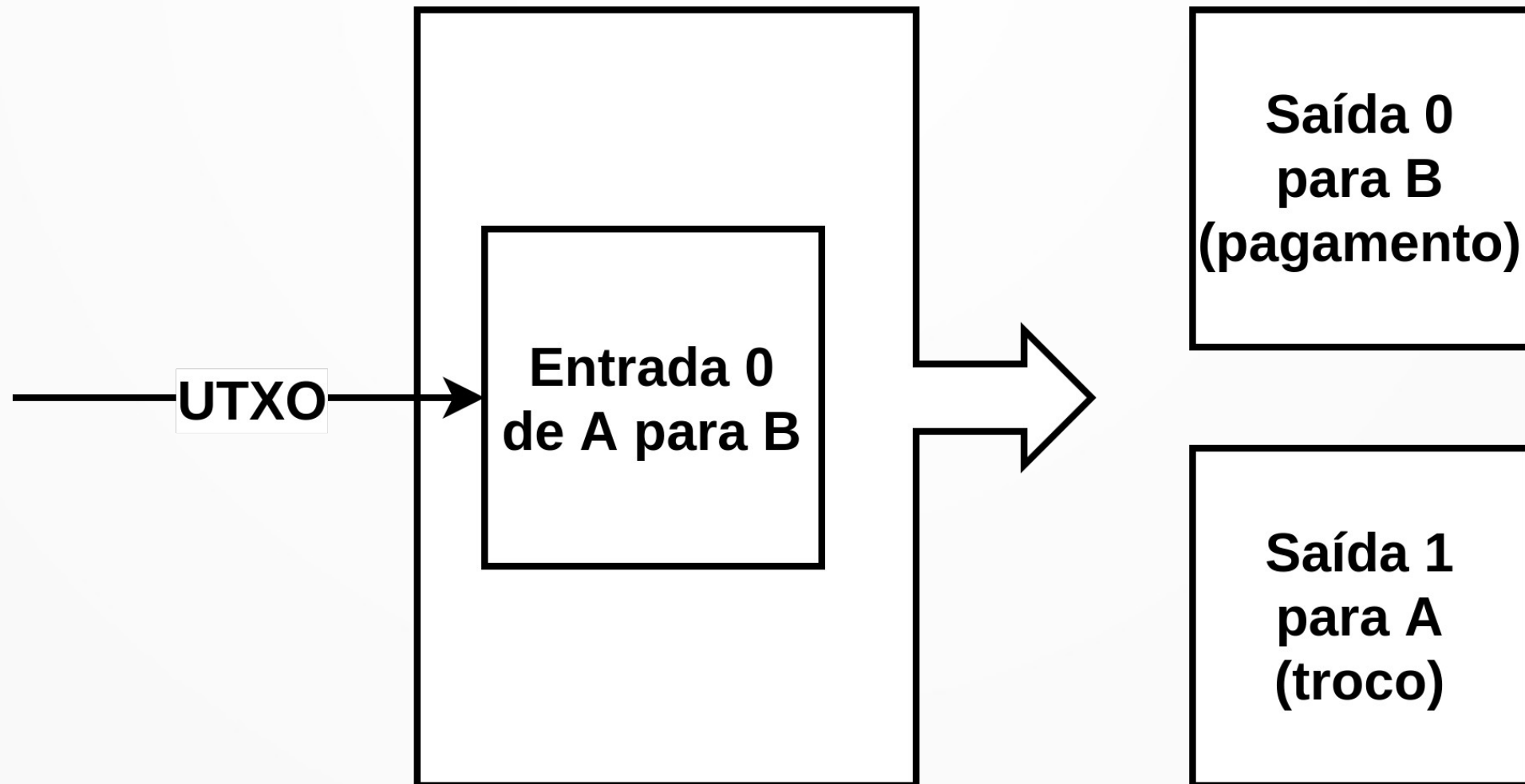
- Transações formam correntes de valores
 - Valores de saída não gastos (UTXO – *Unspent Transaction Output*) movidos para valores de entrada
- Valores disponíveis em trocas podem ser validados desde sua concepção
 - Poder dado pelo *blockchain*
- As trocas e trocos têm execução “como na vida real”



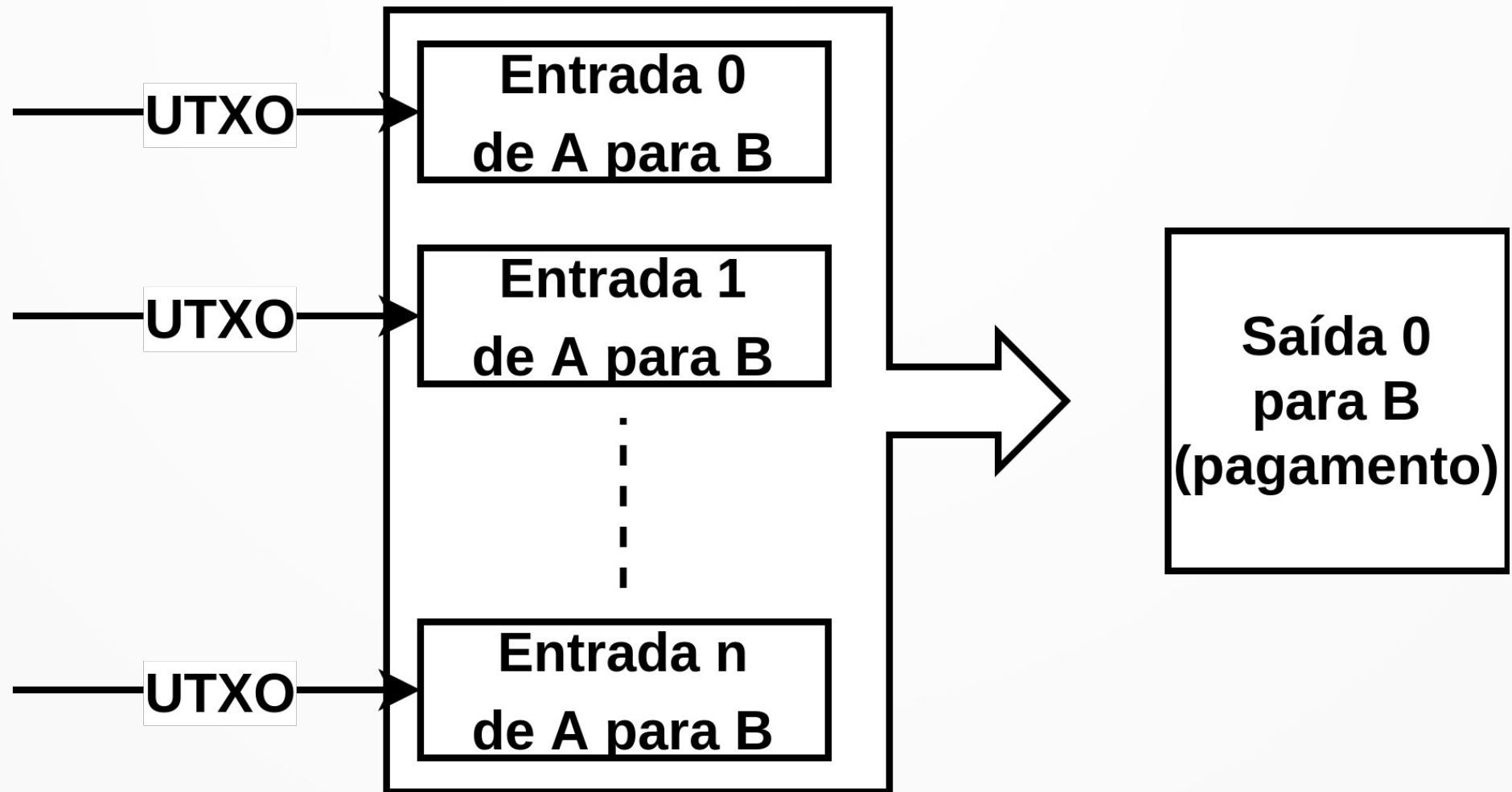
Tipos Básicos de Transações

- **Transação Comum** - 1 Entrada e 2 saídas
 - 1 envio de A para B, com um recebimento em B e um envio de troco de A para A
- **Transação Agregada** - Múltiplas entradas e 1 saída
 - 1 envio com o somatório de várias entradas de A para B, com um recebimento em B
- **Transação Distribuída** - 1 Entrada e múltiplas saídas
 - 1 envio de A para B, com um recebimento em B e vários envios de B para outros

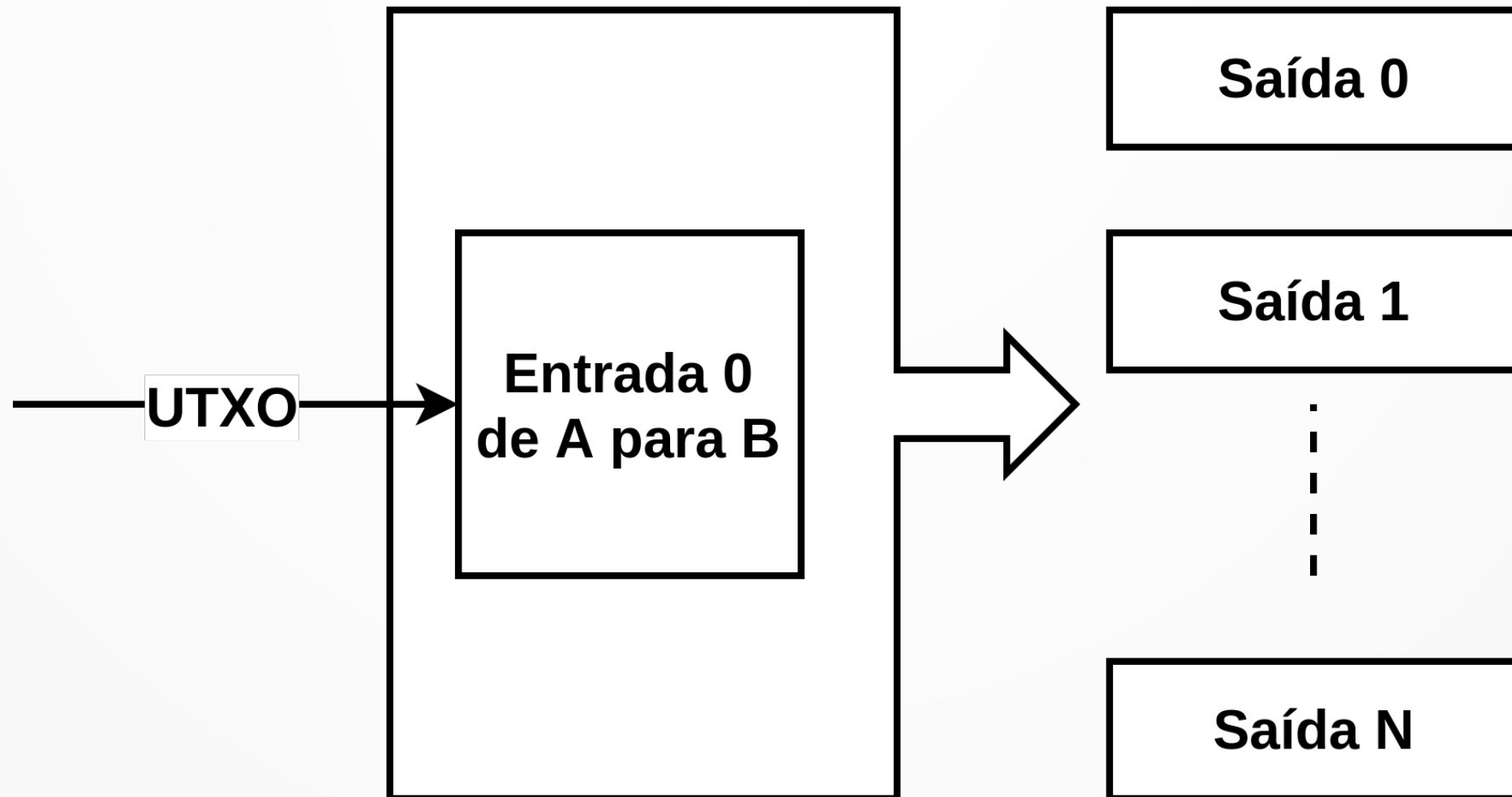
Transação Comum



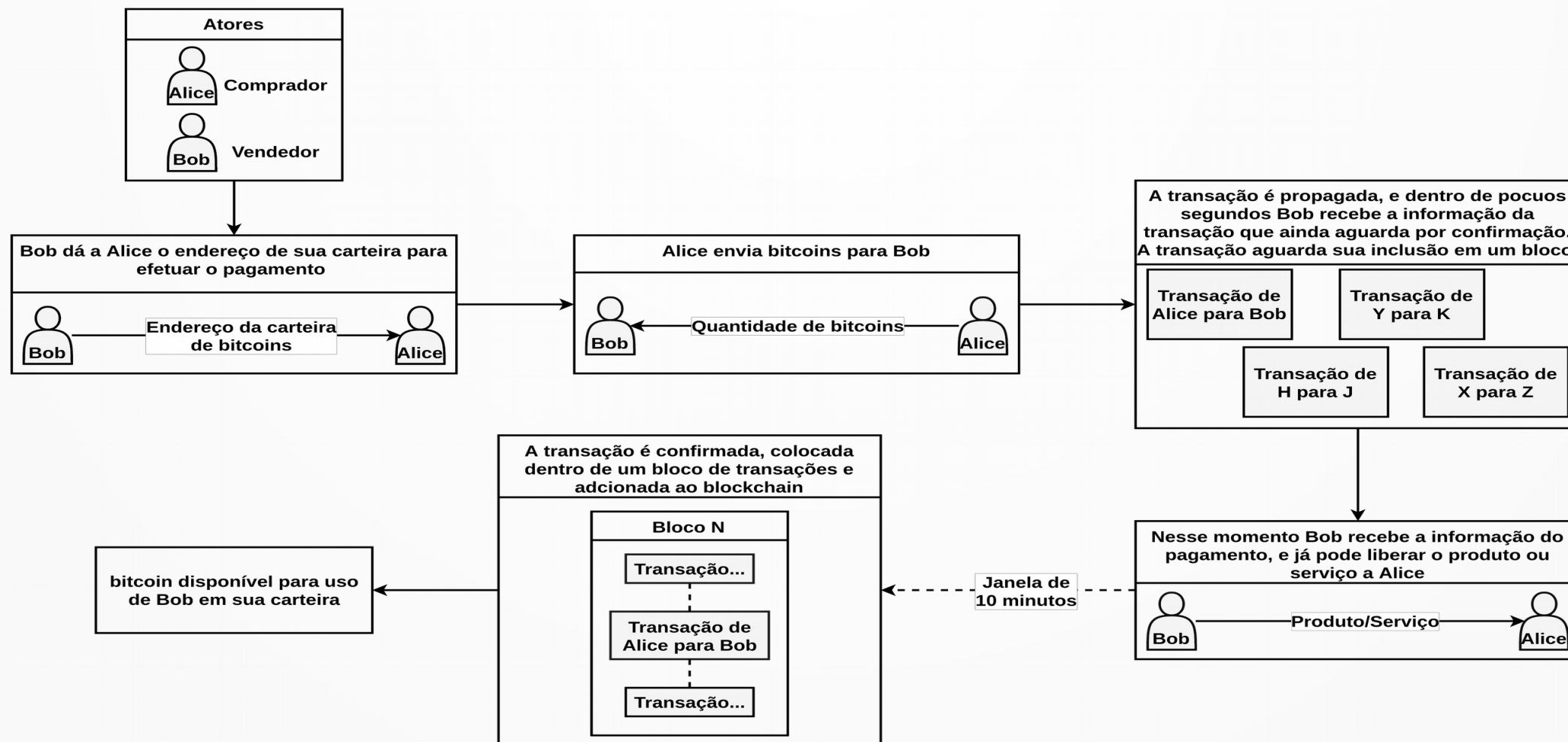
Transação Agregada



Transação Distribuída



Exemplo de Compra - Transação



Revisando

- Bitcoin é uma criptomoeda descentralizada
- A descentralização indica que não há um órgão controlador, e que a rede deve ter regras para garantir ajustes sem a intervenção de um conselho
- O *blockchain* é composto de um conjunto de protocolos – um protocolo pode ser entendido como um conjunto de “regras”, que devem ser seguidas por todos os participantes da rede para realizar ações que sejam aceitas
- Também é chamado de *blockchain* a cadeia de blocos de transações, que é o registro descentralizado e único de todas as operações na rede
- Os *miners* (mineradores) são responsáveis por incluir as transações no *blockchain*. Os mineradores ganham os bitcoins das taxas nas transações, bem como novos bitcoins gerados por bloco
- Carteiras são similares a uma conta de banco, possuindo um endereço. Uma carteira pode não possuir uma empresa que faça seu gerenciamento e ser totalmente administrada pelo usuário - mas este tipo de serviço de abstração é comum de ser prestado
- As transações feitas em criptomoedas são muito similares as transações feitas em vida real, podendo conter troco, distribuição e agregação de valores – e muitas vezes a combinação dos mesmos

Documentações Oficiais

- Para usuários
 - https://bitcoin.org/pt_BR/recursos
- Para desenvolvedores e estudantes
 - https://bitcoin.org/pt_BR/documentacao-do-desenvolvedor
- Para empresas
 - https://bitcoin.org/pt_BR/bitcoin-para-empresas



Aprender Economia

Projeto de Extensão da Unifal - MG



OBRIGADO!