UNIVERSIDADE D
COIMBRA

José Miguel Neto Braga

REMESSAS INTERNACIONAIS

TRANSFERIR UTILIZANDO TECNOLOGIA BLOCKCHAIN

Dissertação no âmbito do Mestrado em Engenharia Informática, especialização em Engenharia de Software, orientada pelo Engenheiro José Perdigão e pelo Professor Doutor Paulo José Osório Rupino da Cunha e apresentada ao Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Setembro de 2022

FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE Đ
COIMBRA
DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

José Miguel Neto Braga

Remessas Internacionais

Transferir Utilizando Tecnologia Blockchain

Dissertação no âmbito do Mestrado em Engenharia Informática, especialização em Engenharia de Software, orientada pelo Engenheiro José Perdigão e pelo Professor Doutor Paulo José Osório Rupino da Cunha e apresentada ao Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Setembro de 2022

FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D
COIMBRA

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

José Miguel Neto Braga

International Remittances

Transfer Using Blockchain Technology

Dissertation in the context of the Master in Informatics Engineering, specialization in Software Engineering, advised by Engineer José Perdigão and Professor Paulo José Osório Rupino da Cunha and presented to the Department of Informatics Engineering of the Faculty of Sciences and Technology of the University of Coimbra.

Setember of 2022

Agradecimentos

Em primeiro lugar gostaria de agradecer à empresa que acolheu o meu estágio, a WIT Software. Com um agradecimento especial ao grupo que mais próximo se manteve de todo o processo: José Perdigão, Bruno Coelho e Mylena Dias. Pela orientação, ensinamentos do mundo profissional e lições de vida, um obrigado. Queria ainda agradecer ao professor Paulo Rupino por todo o apoio e acompanhamento, em especial com a escrita do documento.

Gostaria de agradecer todo o apoio dos meus amigos que sempre me ajudaram a manter um bom equilíbrio entre o lazer e trabalho. Para aqueles que contribuíram diretamente para este documento: Carlos Soares, Vitalina Holubenko, Rodrigo Martins, José Simões, Rita Marques e Gabriel Pinheiro, um especial obrigado.

Gostaria de agradecer à minha família por todo o apoio e compreensão.

Gostaria de agradecer ao Departamento de Engenharia Informática por ser uma parte tão integrante do meu percurso académico.

E por fim, gostaria especialmente de agradecer à minha namorada Rita. Por todo o apoio que deu ao longo desta etapa, levo um carinho especial.

Resumo

O presente documento descreve o trabalho realizado por José Braga no âmbito do estágio com o título original *Envio de Remessas Internacionais usando Blockchain* do Mestrado em Engenharia Informática promovido e sob o acolhimento da empresa WIT Software.

Inserindo-se na atividade de envio de remessas internacionais, o objetivo do estágio consistiu na criação de uma solução que procura fornecer um serviço de transferência a um custo reduzido para o utilizador. A solução consistiu no desenvolvimento de um protótipo suportado por interações com uma rede blockchain, responsáveis pelo processo de conversão, transferência e levantamento. Existiu ainda um foco no mercado da Tanzânia, no entanto, ao longo do processo de desenvolvimento procurou-se sempre facilitar a integração futura com outros mercados.

Numa fase inicial, foi realizada uma análise à atividade de envio de remessas internacionais, nomeadamente com foco na importância que esta tem para a economia e quotidiano em países em desenvolvimento. De seguida, foi feito um estudo aprofundado aos vários conceitos subjacentes à tecnologia blockchain de modo a compreender a forma como esta poderia impactar o setor da atividade. A informação captada foi fruto de um estudo a diversas fontes e resultou da análise critica do responsável pela escrita deste documento.

De forma a suportar o desenvolvimento futuro e definir as tecnologias, foi feito uma análise a soluções semelhantes já implementadas e ainda foram comparadas as diferentes redes blockchain através de métricas como o impacto energético, custo e velocidade por transação. Depois de selecionar a rede e tecnologias subjacentes, foi desenvolvida a solução, seguindo-se de uma análise final aos resultados obtidos.

A solução desenvolvida apresenta-se como sendo 36.24% e 27.93% mais económica do que a média global para os montantes de 200 e 500 dólares enviados, respetivamente. Pode vir a impactar um mercado que anualmente representa mais de 185 milhões de dólares na Tanzânia. E no caso de serem integrados no futuro novos mercados, impactar uma atividade mundial que representou na totalidade em 2021 mais de 589 mil milhões de dólares.

Palavras-Chave

Remessas Internacionais, Blockchain, Rede Stellar

Abstract

This document describes the work carried out by José Braga within the scope of the internship *Sending International Remittances using Blockchain* inserted in the master's in informatics engineering promoted and hosted by the company WIT Software.

Related to the international activity of sending remittances, the internship objective consisted in the development of a solution that seeks to provide a transfer service at a reduced cost for the user. Associated with the solution, a prototype was developed supported by interactions with a blockchain network, which were in term responsible for the conversion, transfer and withdraw process. There was a particular focus on the Tanzanian market, however, throughout the development process, efforts were always made to facilitate future integration with other markets.

In an initial phase, an analysis was carried out on the activity of sending international remittances, namely with a focus on its importance for the economy and daily life in developing countries. Then, an in-depth study was carried out on the various concepts behind blockchain technology to understand how it could impact the sector. The information collected was the result of a study of different sources and resulted from the critical analysis of the person responsible for writing this document.

To support future development and define technologies, an analysis was made on similar solutions already implemented and a benchmark was created comparing the different blockchain networks through metrics such as energy impact, cost, and speed per transaction. After selecting the network and adjacent technologies, the development process began and, in the end, the results of the solution were analyzed.

The developed solution is 36.24% and 27.93% cheaper than the global average for the amounts of 200 and 500 dollars sent, respectively. It could impact a market that represents more than US$185 million annually in Tanzania. And if new markets are integrated in the future, impact a global activity that represented in total in 2021 more than US$589 billion.

Keywords

International Remittances, Blockchain, Stellar Network

Índice

Lista de Figuras

Lista de Tabelas

Capítulo 1
Introdução

Em países em desenvolvimento onde as perspetivas de rendimento não são as mais favoráveis, muitos optam pela emigração como solução. Desta escolha, resulta a necessidade de transferir dinheiro para os familiares que permaneceram no país de origem, o que por si leva ao aparecimento da atividade de envio de remessas internacionais. É uma atividade que tem crescido nos últimos anos e representa agora a maior fonte de rendimento para muitas economias nestes países [3]. No entanto o seu custo permanece alto, sendo em média 6.09% para uma transação de 200 dólares (transação mais frequente para a atividade) [4].

Em paralelo, há mais de uma década, surge uma tecnologia que procurou, através da Bitcoin, criar um sistema virtual descentralizado para cunhar, realizar e confirmar transações de uma moeda entre contas [5]. Essa tecnologia denomina-se como blockchain e com o passar do tempo foram identificadas uma série de outros problemas onde as características desta tecnologia poderiam ser úteis, acabando assim por contribuir para o acelerar da digitalização de processos. Comprovou os seus benefícios em diversos casos de uso que incluem o setor financeiro na forma como se demonstra ser uma solução mais rápida, transparente e confiável. Procura continuar a comprovar utilidade em muitos mais.

Atualmente para o envio de uma remessa internacional existem várias multinacionais de grandes dimensões, como a Western Union, que fornecem serviços para realizar esta atividade. No entanto, o processo de transferência envolve vários bancos intermediários o que resulta num custo elevado e num maior tempo de processamento [6]. Para além destes problemas, o rácio de conversão entre moedas é normalmente baixo.

Neste estágio, procura-se desenvolver um protótipo que efetua uma conversão e transferência de dinheiro de forma rápida, transparente e económica, fruto das funcionalidades e características presentes numa rede blockchain. O foco será transferências de euro, dólar ou libra para xelim tanzaniano devido ao interesse em explorar este mercado por parte da empresa que acolhe o estágio, WIT Software.

1.1 Contextualização

Esta dissertação foi escrita no âmbito da unidade curricular de Dissertação/Estágio em Engenharia de Software inserida no mestrado de Engenharia Informática do Departamento de Engenharia Informática da Universidade de Coimbra. O projeto teve início a 20 de setembro de 2021 e terminou no dia da entrega do documento final a 5 de setembro de 2022.

O estágio associado a este documento de dissertação encontrou-se sob o acolhimento da WIT Software, uma empresa com mais de 21 anos de experiência, que fornece sistemas e aplicações para operadoras de comunicação a nível mundial (ex: Grupo Vodafone, Deutsche Telekom, Softbank, AT&T, Safaricom, entre outros).

A equipa de desenvolvimento da solução consistiu unicamente no autor e na indispensável e fulcral orientação do professor Paulo Rupino, do engenheiro e orientador da empresa, José Perdigão, do engenheiro Bruno Coelho e da analista de negócio Mylena Dias.

1.2 Motivação

A atividade de envio de remessas internacionais possui cada vez mais impacto na economia de países em desenvolvimento [3]. Caracteriza-se como sendo um tipo de transferência internacional que envolve envio de um montante de dinheiro por parte de alguém deslocado da sua terra natal, normalmente associado à emigração de países em desenvolvimento para países desenvolvidos [7].

A totalidade da atividade envolve mais de mil milhões de pessoas [8] e representou só em 2021, mais de 589 mil milhões de dólares [2]. Em países como o Nepal, Quirguistão e Libéria contribui para mais de 25% do PIB[1] [9].

Vários estudos demonstraram que esta atividade pode reduzir os níveis de pobreza nos países em desenvolvimento, estando ainda associada ao aumento nos gastos relacionados com a saúde, educação e pequenos negócios. Estima-se que um aumento de 10% no montante enviado em cada remessa levaria a um decréscimo de 3.5% no número da população mundial em níveis de pobreza [10].

A blockchain demonstra cada vez mais aplicabilidade nos vários setores do mercado mundial. Promete transformar o paradigma financeiro tradicional atual e solucionar preocupações como a velocidade, acesso, transparência e custo elevado de transação [11].

Na figura 1, pode ver-se uma esquematização das diferenças entre o processo tradicional de envio de remessas e o mesmo suportado por tecnologia blockchain. A parte superior da imagem exemplifica o processo tradicional, onde um emissor da transferência (*sender*) recorre a um serviço fornecido por uma entidade bancária (*sender's bank*) com intenção de iniciar o processo de envio de dinheiro. O *sender's bank* normalmente não possui uma ligação direta com o banco associado ao recetor da remessa (*receiver's bank*), e por isso usufruir de serviços de um número arbitrário de

[1] PIB (Produto Interno Bruto) – Representa o montante dos bens ou serviços produzidos por um país num dado ano.

bancos intermediários (*intermediary bank*) como meio para concluir o processo, que normalmente, demora 3 a 5 dias úteis [7]. No caso da tecnologia blockchain, representado na parte inferior da imagem, a transferência ocorre diretamente entre contas dos envolvidos (*Crypto Wallets*) fruto da natureza descentralizada e distribuída da tecnologia. Em comparação, demora alguns minutos [12].

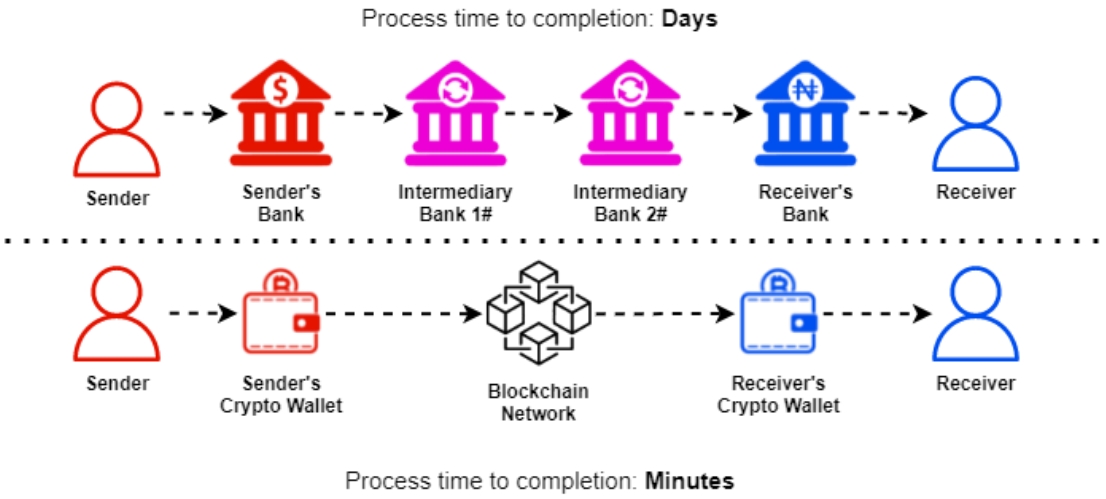


Figura 1 - Esquematização da diferença entre o processo de envio de remessas internacionais tradicional e o mesmo processo em blockchain.

1.3 Objetivos do Estágio

Baseado nos problemas apresentados na secção anterior, os objetivos deste estágio consistem no desenvolvimento de um programa na linguagem de programação *java* que efetua pedidos à rede blockchain de modo a transferir dinheiro entre duas contas bancárias, permitindo ainda ao recetor realizar um levantamento dos fundos recebidos. O foco será transferências de euro, dólar ou libra para xelim tanzaniano.

Espera-se desenvolver as seguintes componentes:

- Servidor para gestão de notificações relacionadas com o estado das operações (transferência e levantamento) e ainda uma API para exposição de endpoints que interagem com a rede blockchain para completar o processo.
- Aplicação web que demonstra o estado das operações (transferência e levantamento) através de uma interface intuitiva.

1.4 Estrutura do Documento

Este capítulo pretende atuar como um enquadramento para a leitura de todo o conteúdo exposto neste documento.

O segundo capítulo do documento serve para apresentar o estado atual dos dois temas mais importantes para o estágio: Remessas Internacionais e Blockchain, introduzindo e desenvolvendo alguns conceitos fundamentais para a compreensão e implementação da solução final. Na última subsecção é feito um cruzamento entre temas de forma a explorar as soluções atuais no mercado que se assemelham à solução que se procura desenvolver.

No terceiro capítulo é feita uma análise dos requisitos que devem constar na solução e com base nisso, é selecionada a rede blockchain que mais se adequa ao desenvolvimento do protótipo.

O conteúdo do quarto capítulo é relativo à solução desenvolvida. Começa por apresentar as ferramentas utilizadas e a arquitetura de software criada, seguindo-se da solução em si e terminando com a análise de resultados.

O quinto capítulo pretende apresentar o planeamento para todo o projeto durante os dois semestres, com ênfase em justificar as divergências que existiram entre o planeado e o executado.

O sexto capítulo é dedicado à conclusão do trabalho desenvolvido no âmbito do estágio.

No primeiro apêndice, podem ver-se diagramas de planeamento completos para o primeiro e segundo semestre.

No segundo apêndice encontra-se o documento de descrição de design construído com a ajuda da analista de negócios Mylena Dias.

No terceiro apêndice encontra-se o documento de especificação de requisitos criado no primeiro semestre para auxiliar no desenvolvimento da solução.

No quarto apêndice, pode ver-se a especificação de todos os endpoints criados.

No quinto apêndice, podem ver-se os diagramas de sequência para todas as operações possíveis de realizar dentro da solução.

No sexto apêndice é apresentado a tabela de custos da entidade ClickPesa associado ao serviço de levantamento de tokens TZS para uma conta bancária ou de mobile money.

Capítulo 2
Estado da Arte

A felicidade é fortemente influenciada pelas condições de vida às quais estamos sujeitos. Em países em desenvolvimento, onde as perspetivas de rendimento não são as mais favoráveis, muitos optam pela emigração como solução que mais os beneficia [13]. Desta escolha, resulta a necessidade de transferir dinheiro para os que permaneceram no país natal.

Atualmente existem vários serviços fornecidos por gigantes no setor financeiro mundial, como a Western Union, que permitem resolver este problema de transferência internacional de dinheiro. No entanto, para determinados pares de países (recetor e emissor da transferência) e para determinados pares de moedas (a do país emissor e a do país recetor) estão associadas elevadas taxas [14]. Isto deve-se em parte à regulamentação cada vez mais apertada (KYC[2] e aos esforços de combate à lavagem de dinheiro) mas essencialmente relaciona-se com a procura de lucros cada vez mais elevados [15]. Além disso, não é garantido que seja possível realizar a transferência para determinadas combinações de países e moedas [16].

2.1 Remessas Internacionais

As transferências internacionais referidas anteriormente são categorizadas como sendo remessas internacionais. Este termo representa uma tipologia particular de transferência monetária que se encontra associada à emigração e ao envio de dinheiro com pelo menos um câmbio da moeda entre o emissor e recetor [3].

O fluxo de remessas internacionais aumentou significativamente nos últimos anos e tornou-se o principal fator externo a influenciar as economias de vários países em desenvolvimento. Chega até a ser mais impactante que os tradicionais fatores externos, como investimento direto estrangeiro. O World Bank estima que as remessas internacionais compõem mais de um terço de todo o dinheiro entrante em países em desenvolvimento [17].

O impacto encontra-se dependente da forma como o dinheiro é despendido por parte do individuo ou entidade recetora da remessa. Se resultar num aumento no consumo em determinados setores económicos, os efeitos positivos acabam por se propagar para toda a economia nacional [17]. No Quénia, em média, 27.5% do dinheiro proveniente das remessas é gasto na construção de edifícios habitacionais, 22.9% na educação e 14.5% na alimentação [17].

[2] KYC (Know Your Customer) – Processo de verificação da identidade de um cliente.

A atividade de envio de remessas funciona ainda como uma medida forte contra a pobreza mundial. Estima-se que um aumento de 10% no montante enviado em cada remessa, levaria a um decréscimo de 3.5% no número da população mundial em níveis de pobreza [10].

2.1.1 Processo de Envio

Normalmente o processo de transferência é relativamente lento, demora em média 3 a 5 dias úteis (dependendo do país) [7] e existem sempre elevadas taxas cobradas por parte das entidades que fornecem o serviço [18]. Em certos países, pode ainda ser cobrado um imposto adicional por parte do sistema financeiro local que considera que se trata de uma entrada de dinheiro sujeita a tributação (independentemente se é uma compensação ou uma prenda) [19].

Existem diferentes formas de realizar o envio de uma remessa, sendo que os principais fatores de suporte à decisão se baseiam no **custo** e **tempo** associados à concretização da transação, na **forma de pagamento** e ainda na facilidade que os intervenientes têm no **acesso a infraestruturas bancárias**. Independentemente do método utilizado, o emissor tem de ter o saldo necessário de forma a realizar a transferência.

Depois da transação ser criada, os fundos são convertidos para a moeda desejada de acordo com o rácio de câmbio no momento. Posteriormente as taxas do banco são aplicadas e o dinheiro enviado será creditado na conta do recetor descontando a diferença resultante destes dois fatores (rácio de conversão e taxas aplicadas) [19].

Os métodos mais comuns no envio de remessas internacionais são:

1. **Cheques**

Apresenta-se como uma solução morosa para o envio de remessas internacionais devido aos vários passos que tanto o banco como o cliente têm de realizar para completar o processo (pode demorar mais de 30 dias até ao montante da transferência ser creditado na sua conta) [20]. Para além de se apresentar como uma solução lenta, existem várias pessoas envolvidas, o que pode originar numa ocorrência de erro humano que força ao cancelamento de todo o processo de transferência. No entanto, permanecem funcionais e ainda são uma das formas mais económicas de transferir dinheiro internacionalmente [19].

2. Automated Clearing House (ACH)

Trata-se de um sistema para processamento de lotes de transferências que normalmente realiza três iterações por dia. Especialmente benéfico e económico para situações de pagamentos recorrentes e calendarizados. No seu essencial, pode ser considerado uma digitalização do processo de envio de cheques [19].

De acordo com a Nacha (sistema eletrónico que conecta todos os bancos americanos), mais de 2 mil milhões de transferências com ACH foram realizadas em 2020 (um aumento de 15.2% em relação ao ano anterior) [21].

3. Transferência Eletrónica de Fundos (EFT)

Também denominado por depósito direto, é um método de transferência digital que não envolve qualquer tipo de interação com funcionários da entidade prestadora do serviço. Apesar de funcionalmente não ser diferente do ACH, a comunicação na EFT é direta entre bancos, enquanto no ACH todos os pedidos de transferência param no próprio sistema do ACH [22]. De acordo com o yStats, 59% dos pagamentos entre três das maiores regiões do mundo foram realizados através deste método [19].

a) ETF - Wire Transfer

É um tipo de transferência eletrónica de fundos (EFT) e a maioria das remessas são enviadas através deste método [23]. É caracterizado por ser um tipo de transferência realizada através de uma rede administrada por bancos de todo o mundo. Normalmente é necessário preencher alguma informação pessoal do remetente da transferência e ainda mencionar a razão pela qual se realiza a transferência. A partir do momento que essa informação se encontra documentada, o envio da remessa pode ser iniciado e processado através de um sistema seguro de transferência como o SWIFT[3] ou Fedwire[4] [24].

Relativamente ao procedimento habitual para o envio de remessas internacionais através de uma transferência eletrónica de dinheiro, é constituído pelos seguintes passos [25]:

1. **Autenticação** – Como requisito legal é pedido ao utilizador que insira as credenciais associadas à sua conta no sistema de forma a validar a sua identidade.
2. **Justificação da transferência** – Na maioria das transferências torna-se necessário justificar a razão pela qual se pretende realizar a operação.

[3] SWIFT: Society for Worldwide Interbank Financial Telecommunication, é um protocolo de comunicação de mensagens entre bancos que procura ser o padrão para o setor.

[4] Fedwire: Sistema usado por bancos centrais para solucionar disputas em tempo-real, normalmente no próprio dia. Diariamente movimenta biliões de dólares [145].

3. **Escolha do Montante** – Como em qualquer transferência de dinheiro, é necessário selecionar o montante de dinheiro a enviar, os detalhes da conta do recetor e a moeda destino que se pretende que seja creditada.

4. **Escolha do Método de Pagamento** – Para realizar a transferência é necessário selecionar um dos métodos de pagamento mencionados anteriormente, de acordo com a disponibilidade da entidade que providencia o serviço (EFT, ACH ou cheques).

5. **Conversão e Envio do Dinheiro** – A partir do momento que o banco recebe o pagamento, inicia o processo de transferência para o banco recetor. Na maioria dos casos de envio de remessas não existe uma ligação direta entre bancos [26]. A transferência tem de passar necessariamente por vários intermediários, o que origina um aumento no custo total resultado de uma taxa do serviço prestado. Para além desta taxa adicional, pode ainda ocorrer uma conversão de moeda suplementar intermédia (mais custos devido à perda no câmbio de moedas) [26]. Quando o dinheiro chega ao banco do recetor, o valor é creditado.

Na figura 2, o emissor da transferência (passo 1 - Representado a vermelho) começa por realizar a autenticação no fornecedor do serviço (ex: Western Union), segue-se o preenchimento da justificação para a transferência (passo 2). O emissor terá de preencher um formulário com todos os detalhes para realizar a transferência (Passo 3 - Ex: montante, moeda a enviar, identificador da conta bancária do recetor, …) e selecionar o método de pagamento para iniciar o processo (passo 4). Depois das taxas serem pagas, o dinheiro é convertido e enviado através de uma rede de bancos (ex: SWIFT) até chegar ao banco que possui a conta do recetor (passo 5), onde será depois creditado (passo 6).

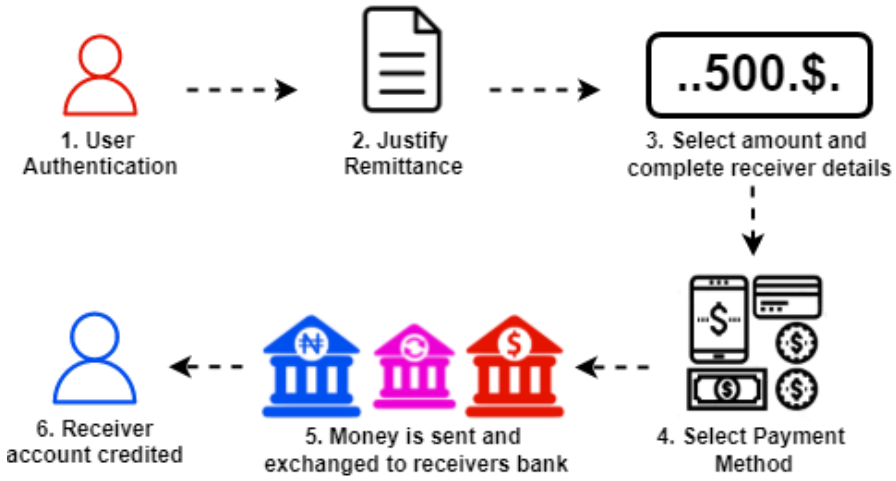


Figura 2 - Esquematização do processo de envio de uma remessa internacional de dinheiro.

2.1.2 Custos Associados

A atividade de envio de remessas representa uma porção significativa do PIB[5] para vários dos países em desenvolvimento. No Tonga e no Gâmbia os valores são inclusivamente superiores a 30% (43.9% e 33.8%, respetivamente). Enquanto noutros países como o Lesoto, Samoa, Quirguistão, Tajiquistão e Honduras a atividade representa mais de 20% do PIB (23.5%, 21.1%, 25%, 25% e 26.6%, respetivamente) [27]. Aumentar o número de remessas enviadas torna-se um objetivo financeiro importante que contribui para a inclusão mundial das economias destes países. Uma forma de atingir este objetivo passa por reduzir os custos assegurando que a transferência ocorre de forma segura e preferencialmente rápida [28].

No entanto, reduzir os custos associados a este serviço em países em desenvolvimento é uma tarefa extremamente difícil. Existem inúmeros fatores adversos. Para além das taxas adicionais impostas pelas entidades (ex: resultado de contratos de exclusividade entre bancos e empresas que fornecem serviços de transferência internacional de dinheiro) existe ainda uma falta de infraestrutura no local do recetor da remessa. Nas situações que isto não se verifica, pode existir ainda uma falta de concorrência entre fornecedores do serviço, o que origina uma monopolização do mercado local [28].

Uma outra vertente que tem impacto no custo é a baixa cotação no mercado que as moedas de alguns países em desenvolvimento possuem, o que influencia fortemente o rácio de conversão. Por outras palavras, a forma como a moeda original do emissor é convertida para a moeda do recetor. Os fatores que mais influenciam este rácio são: **diferenças na inflação** entre os dois países detentores das moedas a trocar (países com baixa inflação possuem moedas com maior valor de mercado); **défice de contas** entre o país e os seus parceiros comerciais (países que importam mais que exportam, sofrem uma depreciação da moeda local); **dívida pública** torna um pais menos atrativo para investidores o que leva a uma maior inflação; **estabilidade politica e performance económica** são características que atraem investidores estrangeiros e acabam por influenciar no rácio [29].

2.1.3 Oferta do Mercado e Tendência

Com um mercado a envolver mais de mil milhões de pessoas [8] e a representar só em 2021, mais de 589 mil milhões de dólares [2] existem inúmeras entidades bancárias envolvidas a competir no setor de atividade de envio de remessas internacionais. Categorizam-se em: ***Legacy*** e ***FinTech*** [30].

As entidades bancárias ***Legacy*** utilizam métodos tradicionais para proporcionar o serviço. São altamente confiáveis e apresentam métodos robustos para processamento da transferência, mesmo que, através de programas informáticos

[5] PIB – Produto Interno Bruto - representa o montante dos bens e serviços produzidos por um país num dado ano [146] .

desatualizados (ex: alguns bancos utilizam soluções construídas com a linguagem de programação criada em 1959, COBOL, que apresenta uma manutenção dispendiosa e incompatível com soluções da atualidade) [31]. São vistos como o exemplo padrão para solucionar o problema.

As entidades bancárias ***FinTech*** (abreviação de **Fin**ancial **Tech**nology) procuram competir com os métodos tradicionais financeiros através do uso da mais recente tecnologia. A tendência crescente na popularidade deste tipo de empresas resulta de três grandes fatores: **Tecnológico** - já não existe a necessidade de ativos permanentes para escalar o negócio, como criação de filiais (ex: a Revolut possui 15 milhões de utilizadores sem nenhum tipo de atendimento ao publico); **Clientes -** exigem cada vez mais dos serviços bancários e este tipo de entidades consegue adaptar-se de forma a responder às exigências; **Regulamentação -** é cada vez mais restrita e as entidades *FinTech*, como têm uma estrutura empresarial mais simples, não são tão afetadas pelos custos anuais associados ao respeitar esta regulamentação [32].

Na tabela 1 pode ver-se os dados relativos a custos e funcionalidades de algumas das empresas que operam neste setor de atividade, contabilizando num total de 16 mil milhões de dólares de capitalização do mercado [33]. Podemos averiguar que todas realizam transferências entre contas bancárias, mas nem todas permitem levantar dinheiro físico ou injetar dinheiro na conta através de serviços mobile. Os dados foram retirados para o exemplo de uma transferência de 200 dólares para reais brasileiros, e podemos verificar que os serviços *FinTech* são consideravelmente mais baratos que os serviços *Legacy*, existindo uma diferença percentual no custo de 7.66% entre o mais caro (Western Union) e o mais barato (Wise).

Tabela 1 - Comparação das funcionalidades e custos oferecidos por algumas das maiores empresas que fornecem o serviço de remessas para uma transferência exemplo de 200 USD para BRL.

		Western Union	**Ria**	**Xoom**	**Wise**
Method	**Type**	Legacy	Legacy	FinTech	FinTech
	Bank Transfer	yes	yes	yes	yes
	Cash Pickup	yes	yes	yes	no
	Mobile Top - ups	yes	yes	no	no
	Cost (USD - BRL)	9.79 %	4.15 %	3.62 %	2.13 %

Apesar da vasta e diversa oferta para o envio de remessas internacionais o custo, como referenciado anteriormente, permanece alto. A redução deste custo é uma preocupação da comunidade internacional, porque está diretamente relacionado com um maior grau de inclusão das economias mais afetadas por este setor de atividade [34].

Em 2009, o grupo de países G8[6] estabeleceu um objetivo económico de reduzir o custo de envio de remessas de uma média de 10% para 5%, em 5 anos (adotado futuramente pelo grupo G20[7]). Denominou-se o objetivo *5 by 5*. Em 2012, as Nações Unidas continuaram com esta missão internacional e estabeleceram uma nova meta num dos seus objetivos de desenvolvimento sustentável para 2030. Inserido no décimo objetivo de "*reduzir a desigualdade dentro e entre países*", definiu-se na alínea c), o objetivo de reduzir o custo médio do envio de remessas para 3% e eliminar corredores[8] com custos superiores a 5% [35] [36].

Na figura 3, pode ver-se uma representação gráfica do custo médio global trimestral desde 2011 até 2022 para uma transferência internacional de 200 dólares. No primeiro trimestre de 2022, o custo médio é de 6.09%, resultado da consideração dos custos para remessas digitais e não digitais. Numa remessa digital o pagamento é feito online e de forma autónoma, apresentando um custo para o primeiro trimestre de 2022 de 4.79%. Por outro lado, uma remessa não digital (pagamento com dinheiro físico) o custo médio para o mesmo trimestre é de 6.69%.

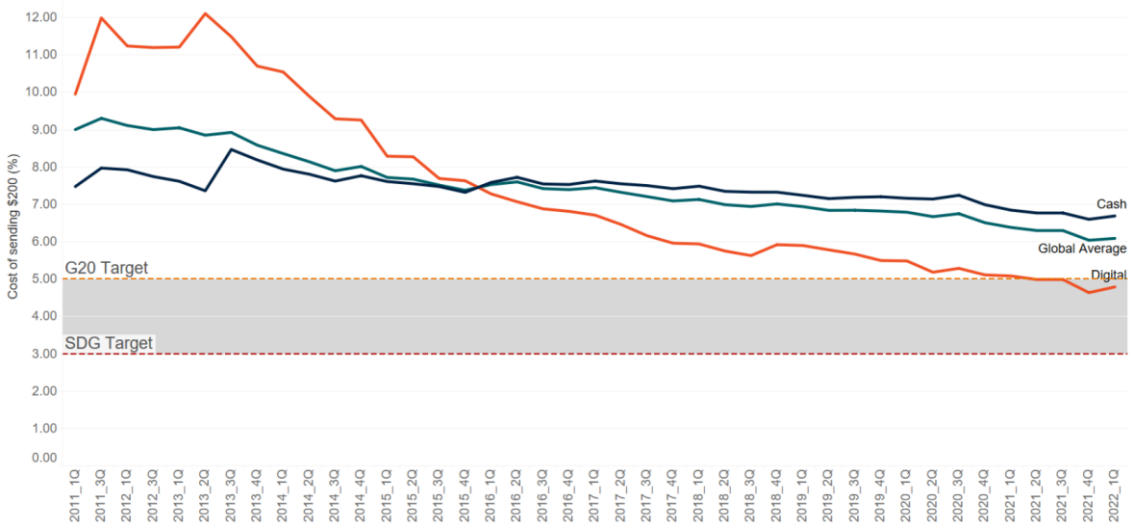


Figura 3 - Gráfico representativo dos dados relativos ao custo percentual global médio para o envio de uma remessa no valor de 200 dólares [35].

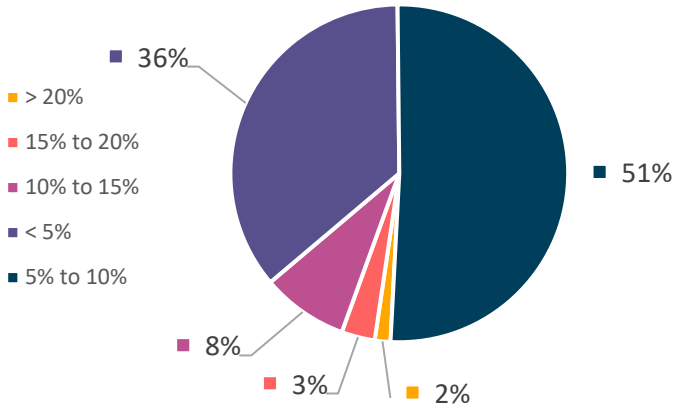
[6] G8 – Grupo de países constituído por: França, Alemanha, Itália, Inglaterra, Japão, Estados Unidos, Canadá e Rússia [147].

[7] G20 – Grupo constituído por 19 países e pela união europeia [148].

[8] Corredor - Neste contexto, refere-se a um grupo de países emissor-recetor específico numa transferência monetária.

Na figura 4, pode ver-se a distribuição dos vários corredores[9] de envio de dinheiro pelos diferentes intervalos de custo médio percentual envolvidos no envio de remessas (terceiro trimestre do ano de 2021). À direita está representada uma tabela com os valores correspondentes de acordo com o patamar de custo.

Verifica-se que a maioria dos corredores de envio de dinheiro (136, correspondente a 51%) apresentam um custo situado no intervalo de 5% a 10%. No entanto, corredores constituídos por países da África Subsaariana apresentam custos superiores a 20%.



Cost Bracket	Number of Contry Corridors
> 20%	4
15 % - 20 %	9
10 % - 15 %	22
5 % - 10 %	136
< 5 %	96

Figura 4 – Distribuição dos vários corredores de envio de dinheiro pelos diferentes intervalos de custo médio percentual envolvidos no envio de remessas para o terceiro trimestre do ano 2021. Fonte adaptada: [35].

2.1.4 Serviços Mobile Money

Em muitos dos países onde a atividade de envio de remessas internacionais tem um impacto direto na economia local existe uma falta de infraestrutura bancária o que dá origem a uma escassez na oferta do serviço de transferência [37]. De forma a colmatar este problema surgiu em 2007 o primeiro serviço de *mobile money*.

Trata-se de um serviço de pagamentos despoletado via telemóvel que permite ao utilizador: guardar, enviar e receber dinheiro [38]. É um mercado que em 2021 foi avaliado em mais de um bilião de dólares, contabilizando só no continente africano mais de 621 milhões de contas registadas [39].

Antes centrado nos pagamentos e transferências, começa agora a agregar outros serviços à sua oferta, como por exemplo: créditos, poupanças e até seguros, aproximando o serviço a algo como um ecossistema diverso em constante evolução.

O *mobile money* tornou-se extremamente acessível a estas populações e atua diretamente na atividade de envio de remessas internacionais na forma como permite

[9] Corredor – Neste contexto, refere-se a um par de países emissor-recetor específico numa transferência monetária.

realizar transferências rápidas e de baixo custo [40]. No entanto existem problemas relacionados com a segurança (*smishing*[10]) e limitações nas quantidades de dinheiro a enviar e receber [41].

Na figura 5, pode ver-se a forma como o serviço de *mobile money* pode operar no mercado tradicional local e contribuir para agilizar o processo de venda ao público. Neste caso encontra-se representado um comerciante que através do serviço de *mobile money* proporcionado pela empresa NBS Bank consegue aceitar pagamentos e ainda obter algum rendimento adicional na forma como funciona como um quiosque de carregamento para contas de *mobile money*.

Figura 5 - Exemplificação da utilização do serviço de *mobile money*. Fonte: [Developing Telecoms, 2017] [42]

2.2 Blockchain

Subjacente a qualquer solução para a atividade de remessas internacionais existe uma tecnologia que garante o seu funcionamento. Nesta subsecção vão ser apresentados conceitos de uma tecnologia emergente que tende a ser escolhida para desenvolver cada vez mais soluções neste mercado, a blockchain [43].

A blockchain apresenta-se como uma tecnologia que utiliza diferentes métodos de encriptação para armazenar dados de forma protegida. É uma forte alternativa à centralização de serviços, aos quais, normalmente se associam alguns aspetos negativos como: **falta de transparência** e **fragilidade** (*Single Point of Failure*[11]) [44]. Uma das principais diferenças é na forma como os dados presentes na blockchain são imutáveis.

Ao encontro do tema da dissertação, possui ainda características que aumentam a sua eficiência em vários casos de uso para múltiplos setores da economia [45].

[10] Smishing – Ataque informático feito através de mensagem de telemóvel onde a vítima é iludida a fornecer informação sensível [149].
[11] Single Point of Failure (SPOF) – Componente de um sistema que em caso de falha leva à falha total do sistema [150].

2.2.1 Definição da Tecnologia

A blockchain representa, de uma forma simplificada, uma base de dados que pode conter qualquer tipo de informação. Guarda os dados de uma forma que se apresenta extremamente difícil de alterar. Surgindo como um paralelismo ao conceito do setor económico de livro-diário (livro em que se regista o débito e o crédito das transações diárias de um individuo ou entidade [46], na língua inglesa: *ledger*) é um livro-diário digital, duplicado e distribuído por uma rede de computadores [44]. Cada bloco da cadeia que forma a blockchain, contém um conjunto de transações e sempre que uma nova transação é criada, um registo correspondente é adicionado a todos os extratos de todos os participantes na rede. Este tipo de tecnologia subjacente é denominado por *Distributed Ledger Technology* (DLT) [47].

Existem dois tipos de blockchain: **privadas** e **públicas** [48]. Nas blockchain privadas existe um controlo no acesso dado ao utilizador por parte de uma entidade centralizada. Nas blockchain públicas o acesso é livre e seguem uma arquitetura *peer-to-peer* totalmente descentralizada. Este tipo de arquitetura é caracterizado pela existência de um conjunto de computadores que possuem o mesmo nível de privilégios (todos podem contribuir e tomar decisões para a rede) e encontram-se conectados a partilhar dados e recursos, sem que seja necessário interagir com um dispositivo central (ex: servidor). Em ambos os tipos de blockchain, todos os intervenientes seguem o mesmo protocolo de comunicação e validação [49].

Um dos atributos mais importantes que define uma rede blockchain é a forma como é descentralizada. Para definir este atributo, Vitalik Buterin, criador da rede Ethereum, define três eixos para qualquer tipo de software descentralizado [50]:

1. **Arquitetura –** Referindo-se ao número de computadores físicos que constitui o sistema e à forma como são toleradas falhas por parte de alguns desses mesmos dispositivos.
2. **Política –** Referindo-se ao número de indivíduos/organizações que controlam o número de computadores que constituem o sistema.
3. **Lógica –** Referindo-se à forma como a estrutura de dados e a interface se comportam como um objeto monolítico[12] ou como um enxame amorfo[13].

[12] Monolítico - Arquitetura de um sistema onde tudo é executado num único processo [151].
[13] Enxame Amorfo – Refere-se a uma arquitetura de sistema onde se consegue manter a operacionalidade individual mesmo quando divido a meio

De acordo com estes três eixos, o atributo de descentralização da blockchain caracteriza-se por possuir:

- **Arquitetura descentralizada** – O sistema tolera falhas e *down-time*[14] por parte dos computadores que o constituem.
- **Política descentralizada** – Não existe nenhum individuo ou organização a controlar os computadores que constituem o sistema.
- **Lógica centralizada** – Porque se dividirmos a meio o sistema, ambas as partes não irão funcionar de forma independente.

Outros atributos fundamentais que caracterizam esta tecnologia são: **imutabilidade**, **confiabilidade**, **transparência** e **segurança** [51].

É através deste diverso conjunto de características que o interesse pela tecnologia cresce e leva a que os vários setores da atividade econômica procurem soluções que implementam tecnologia blockchain [52].

As próximas subsecções irão apresentar em maior detalhe a tecnologia e aspetos que a viabilizam como uma possível solução a explorar para o problema.

2.2.2 Arquitetura da Blockchain

A blockchain, como o nome indica e traduzindo para a língua portuguesa, é uma cadeia de blocos interligada e sequencial onde cada bloco tem uma referência para o bloco anterior. Todos os participantes da rede contêm uma cópia desta cadeia o que se apresenta como um método eficaz para evitar fraudes [53].

Na figura 6 pode ver-se um exemplo da inconsistência que surge na cadeia no momento posterior a uma tentativa maliciosa em alterar os dados presentes num bloco. Na parte superior da figura podemos verificar o estado normal da cadeia com valores exemplificativos. Na parte de baixo da figura, simulando um ataque que levou a alteração de dados no bloco, podemos verificar que o apontador para o bloco contido no bloco seguinte muda o seu valor de *hash*[15]. Desta forma, conservando previamente o valor original, rapidamente se detetava diferenças e se concluía que os valores tinham sido modificados.

[14] Down-time – Duração de tempo onde uma máquina/computador se encontra indisponível ao utilizador.
[15] Hash – É um valor resultado da passagem de um outro valor inicial (podem ou não divergir no tamanho de caracteres) por uma função matemática de *hashing*. É impossível obter a partir de uma hash o valor que lhe deu origem [152].

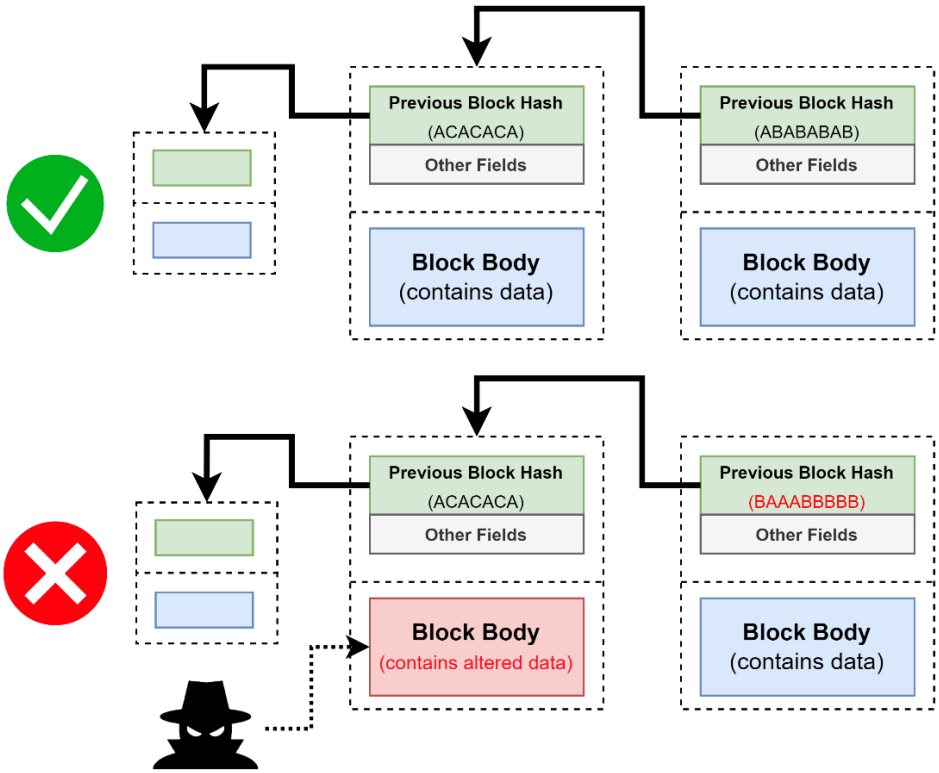


Figura 6 - Esquema representativo da inconsistência que surge na cadeia de blocos quando um valor nos dados de um bloco já construído é alterado.

Uma propriedade fundamental para o sucesso da blockchain parte da composição de cada bloco. Na sua forma mais simplificada, o bloco apresenta duas componentes distintas: um **cabeçalho** (*header)* e um **corpo** com os dados (*body*) [54]. O valor que identifica singularmente cada bloco é calculado através da passagem de todo o cabeçalho do bloco por uma função de *hash* [55].

Inserido no cabeçalho encontra-se o seguinte conjunto de variáveis:

- **Hash do bloco anterior**: Calculado através da inserção de toda a informação do bloco anterior por uma função de *hash* (ex: SHA, MD4, HAVAL, …) irá tornar possível detetar alterações no bloco anterior [56].

- **Timestamp**: Representa a média dos tempos retornados por todos os nós da rede blockchain quando o bloco é criado e validado na rede. Encontra-se no formato Unix, onde algo como “@1395103695” corresponde a “Mon Mar 17 14:48:15 HST 2014” [57].

- **Nonce** (*Number Only Used Once*): Número gerado sequencialmente através da junção arbitrária de outros números. Serve para garantir que quando o bloco é criado cumpre com as restrições impostas pela rede [58].

- **Merkle Root**: Raiz de uma árvore binária[16] (Figura 7) onde cada folha da árvore contém a *hash* de uma transação guardada no corpo do bloco, e os nós não-folha contêm uma concatenação da *hash* dos nós filhos. É utilizada de forma a detetar rapidamente alterações nos dados presentes nas transações [56].

Na figura 7 pode ver-se um exemplo de uma árvore binária, onde o valor presente nos nós representa a soma do valor dos nós que a ele estão subjacentes. Os nós coloridos a verde representam as folhas, enquanto o nó colorido a vermelho representa a raiz da estrutura. Uma alteração no valor de um dos nós resulta na mesma a ser propagada para nós superiores.

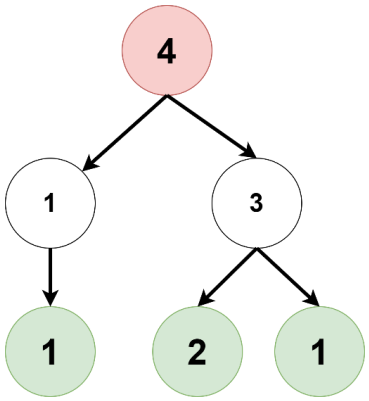


Figura 7 - Exemplo de uma árvore binária.

Na figura 8 pode ver-se a estrutura genérica resumida de um bloco com todas as variáveis descritas anteriormente. Neste exemplo, pretende-se guardar no bloco uma transação. Tratando-se de algo simples, é apenas necessário guardar dados relativos ao emissor, recetor e à quantidade enviada.

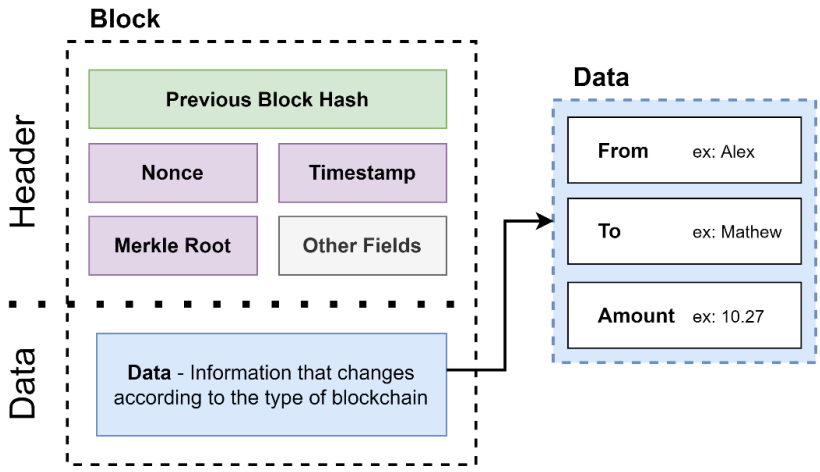


Figura 8 - Estrutura de um bloco.

[16] Árvore Binária – É uma estrutura de dados constituída por nós ligados, onde cada nó tem até 2 nós filhos. [153]

2.2.3 A Importância da Criptografia

A criptografia é essencial na forma como assegura a confiablidade e imutablidade dos dados conservados na blockchain. Define-se como a ciência que estuda técnicas de comunicação seguras entre recetor e emissor, garantindo a privacidade e integridade do conteúdo presente nos dados mesmo que esteja presente uma entidade que pretende realizar algum tipo de atividade maliciosa [59].

O método mais simples de encriptação é o **simétrico** e consiste numa chave única que encripta os dados [60]. Tanto o recetor como o emissor dos dados possuiem uma cópia idêntica da chave usada para encriptar que funciona também para desencriptar. Na figura 9 pode ver-se no esquema superior, uma simplificação de todo o processo descrito para a encriptação simétrica.

No entanto, surge um problema de segurança relacionado com o manter da chave (que tanto o recetor e o emissor possuiem) fora do alcance de uma terceira entidade que conseguiria assim intercetar e decifrar todas as comunicações [61].

De forma a procurar fortalecer a encriptação simétrica, foi desenvolvido um outro método, o **assimétrico**, também conhecido por sistema de chave pública. Neste caso, tanto o recetor como o emissor possuem um par de chaves: uma chave pública e uma chave privada. O emissor pede a chave pública do recetor e utiliza-a para encriptar o conteúdo da mensagem. No momento de receção, o conteúdo só consegue ser descodificado com uso da chave privada do recetor, traduzindo-se numa forma segura que garante o secretismo. A chave privada é ainda responsável pela assinatura de mensagens e a chave pública pela validação de assinaturas [62]. Na figura 9, pode ver-se no esquema central, uma simplificação de todo o processo descrito para a encriptação assimétrica.

Um outro método de encriptação popular funciona com base numa **função *hash***. É utilizado para comparar equivalências de conteúdos sem ter acesso aos mesmos, como por exemplo credenciais de contas numa aplicação [63]. Em oposição à encriptação simétrica e assimétrica, este não utiliza chaves e é praticamente impossível recuperar o conteúdo original da mensagem depois de encriptado. Utiliza uma cifra que muda de acordo com o algoritmo selecionado (algoritmo de *hashing*, por exemplo: SHA 256 bit, MD4, GOST, HAVAL) para gerar uma sequência de caracteres de tamanho fixo a partir da mensagem original.

Para a mesma mensagem, com o uso do mesmo algoritmo de *hashing*, a sequência resultante será sempre igual. Na figura 9 pode ver-se no esquema inferior, uma simplificação de todo o processo descrito da função de *hash*, no caso apresentado utilizou-se o algoritmo de *hashing* SHA 256 bit.

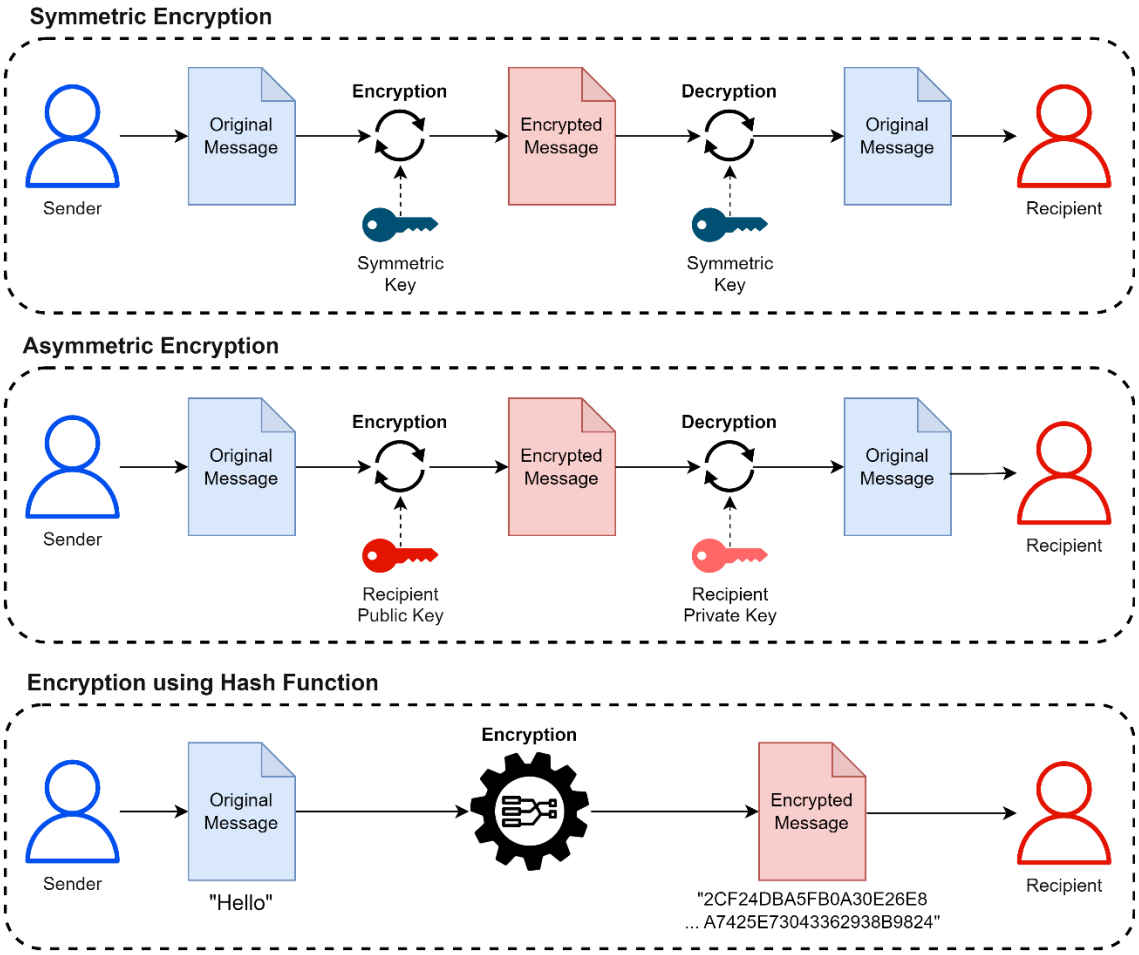


Figura 9 - Esquematização dos processos de encriptação mencionados.

A criptografia aplica-se à tecnologia blockchain na forma como a ideia subjacente de todo o funcionamento é uma cadeia de assinaturas digitais. Estas assinaturas são criadas pela combinação da *hash* da mensagem com a chave privada de um utilizador interveniente. A assinatura digital garante três das propriedades mais importantes no que toca à transferência de informação: **autenticação** (verificar a identidade da outra entidade através da chave pública), **integridade** (dados não são corrompidos ou alterados) e **não repúdio** (entidade responsável pela assinatura não pode negar o seu envolvimento). Existe ainda uma outra propriedade, a **confidencialidade** (dados escondidos de entidades não autorizadas) que é conseguida por algoritmos de encriptação como o *Advanced Encryption Standard* (AES) [64].

A assinatura digital permite aos utilizadores provar que são proprietários da chave privada que corresponde a uma transação sem nunca existir a necessidade de a revelarem [64].

2.2.4 Mineração de Blocos

O conceito de mineração aplicado à tecnologia blockchain refere-se ao processo de verificação e validação de todas as etapas envolvidas no momento de criação de uma transação até ao momento em que esta se encontra guardada na cadeia, ou seja, refere-se ao processo de adicionar novos dados à cadeia de blocos já existente [65].

Os indivíduos que participam neste processo são conhecidos por mineiros[17] (*miners*) e é através do uso do seu poder computacional que realizam a **validação** e **verificação** dos dados [65].

Os mineiros são incentivados a contribuir para a segurança e continuidade da rede através de uma recompensa em formato de um ativo digital (criptomoeda). Quanto maior for o esforço computacional da sua contribuição, maior será a probabilidade de receber esta recompensa [66].

No caso da rede blockchain mais popular, a Bitcoin, a recompensa por bloco validado é atualmente de 6.25 criptomoedas Bitcoin o que equivale a cerca de 316 250 dólares (dezembro, 2021) [67]. Normalmente os mineiros optam por se agrupar em grupos de mineração, ou seja, minam em conjunto através do combinar do seu poder computacional e repartem a recompensa entre si de acordo com o valor da respetiva contribuição. Desta forma, conseguem garantir um rendimento mais estável e constante [68].

Para que o mineiro consiga contribuir para a rede, tem de possuir *hardware*[18] com uma determinada capacidade computacional. O paradigma e o algoritmo de consenso de cada rede blockchain (maior detalhe na subsecção seguinte) são os fatores que ditam a exigência computacional de uma contribuição [69].

Existem diferentes equipamentos que procuram acompanhar as necessidades das, cada vez mais exigentes, redes blockchain. Segue-se uma enumeração dos equipamentos mais comuns para minerar:

- **Processador (CPU):** Tratando-se do circuito eletrónico que executa as instruções presentes nos programas informáticos, foi numa fase inicial da tecnologia a opção mais popular. Com o aumento das exigências e da dificuldade de mineração, tornou-se numa escolha não rentável. Existem, no entanto, determinadas redes blockchain onde só é possível utilizar este método para minerar [70].
- **Placa Gráfica (GPU):** Responsável por gerar imagens para um dispositivo de exibição (monitor) tem vindo a aumentar a sua performance impulsionada pela indústria de videojogos. Devido à sua eficiência, tornou-se o equipamento mais útil para a atividade de mineração [71].

[17] Mineiros - Termo emprestado, proveniente da prática de mineração de ouro. Deve-se à forma como um esforço, neste caso computacional, consegue produzir *pennies from heaven*, sendo estes referentes à quantidade de criptomoedas premiados ao nó.

[18] Hardware – Referente à parte física de um computador (ex: circuitos elétricos, placa gráfica, …) [154].

- **Application Specific Integrated Circuit Miner (ASIC):** Refere-se a um circuito integrado construído para um objetivo específico. Um mineiro ASIC apresenta uma maior eficiência energética, no entanto a lista de ativos que podem ser minerados é reduzida [72].

Algoritmo de Consenso

Na rede blockchain o algoritmo de consenso é responsável pela harmonia de todo o processo de adicionar novos dados à cadeia, ou seja, é através dele que é possível atingir concordância nos valores de dados numa rede distribuída de agentes. Resume-se num conjunto de regras e passos que avaliam a legitimidade de todas as contribuições [73]. Cada rede blockchain opta por implementar um algoritmo de consenso diferente consoante o que considera mais adequado.

Segue-se uma listagem de alguns dos algoritmos de consenso existentes de acordo com a popularidade da implementação nas diversas redes blockchain [74]:

- **Proof of Work (PoW):** Através deste algoritmo, todos os membros da rede irão utilizar o seu poder computacional para solucionar um problema arbitrário baseado em números primos relacionado com a variável de *Nonce*. Em cada ronda de criação de um bloco é selecionado apenas um nó que representa temporalmente o primeiro a solucionar o problema. Um dos grandes problemas da adoção deste algoritmo é o impacto energético [74]. Em 2021 o consumo de energia devido à rede blockchain da Bitcoin (que utiliza este algoritmo de consenso) excedeu os 91 TWh, que representa um consumo superior ao de 5.5 milhões de habitantes na Finlândia num ano [75].

  Na figura 10, pode ver-se a esquematização do processo envolvido no algoritmo. Cada nó mineiro constrói o cabeçalho do bloco com as variáveis necessárias que incluem o *Nonce*. O cabeçalho passa depois por uma função de *hashing* onde o valor resultante será comparado com o valor objetivo. Se for inferior, o novo bloco é construído. Se não for o caso, o *Nonce* é ajustado e o cabeçalho volta a ser construído [74].

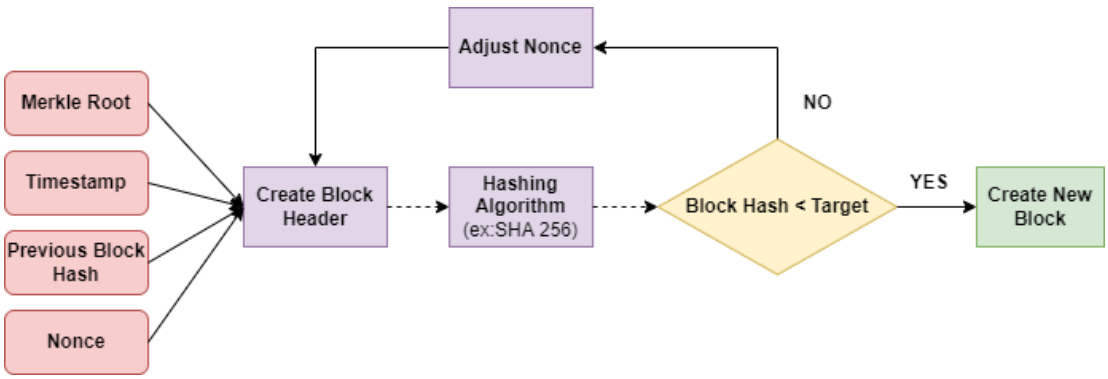


Figura 10 - Esquematização do processo no algoritmo de consenso Proof of Work.

- **Proof of Stake (PoS):** Para cada ronda de criação de um novo bloco, a escolha de quem será o responsável por validar o bloco é aleatória, mas a probabilidade aumenta lineamente de acordo com a quantidade que um nó possui na sua caução (*stake*). Permanece a necessidade de solucionar um problema arbitrário relacionado com a variável de *Nonce.* Uma consideração importante é o facto de que um nó só pode validar um bloco se a recompensa for inferior à caução e no caso de a validação ser comprovada como fraudulenta, será deduzido ao nó a recompensa de criação do bloco e toda a caução que depositou, o que se torna num incentivo à honestidade [74]. O método foi criado como uma alternativa ecológica ao Proof of Work, porque apenas nós selecionados podem validar blocos. Para a rede Ethereum, uma transação consome 84 000 Wh quando utiliza o algoritmo de consenso Proof of Work, enquanto com o algoritmo Proof of Stake são 35 Wh, ou seja 0.04% da energia [76].

  Na figura 11, pode ver-se a esquematização do processo envolvido no algoritmo. Cada nó mineiro começa por construir um cabeçalho e passar a informação por uma função de *hashing*. De seguida será avaliado se a quantidade da caução é superior à pedida pelo bloco (ex: para a rede ethereum é necessário que um nó possua no mínimo 32 ETH em caução [77]). No caso de não ser, o nó será excluído e passará a repetir o processo na próxima ronda. A caução demonstra-se assim como o fator determinante na escolha da responsabilidade de criação do novo bloco [74].

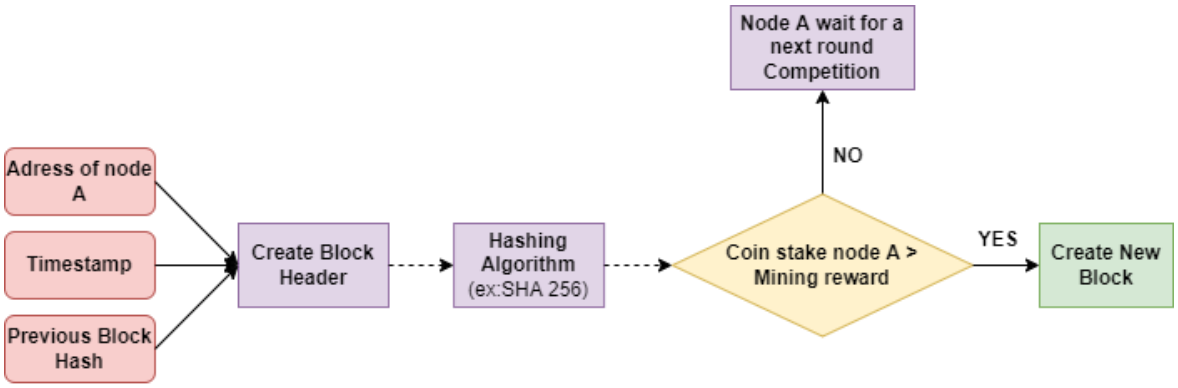


Figura 11 - Esquematização do processo no algoritmo de consenso Proof of Stake.

- **Delegated Proof of Stake (DPoS):** Derivação do algoritmo de Proof of Stake, baseia-se num princípio democrático. Todos os nós que possuem cauções na rede irão votar nos responsáveis pela criação de novos blocos [74].

  Na figura 12, pode ver-se a esquematização do processo envolvido no algoritmo. Os nós que possuem caução irão votar nos nós mineiros. Nós que possuam mais de 50% dos votos serão eleitos como nós mineiros. No caso de um nó mineiro eleito não gerar novos blocos, perderá o privilégio de minerar [74].

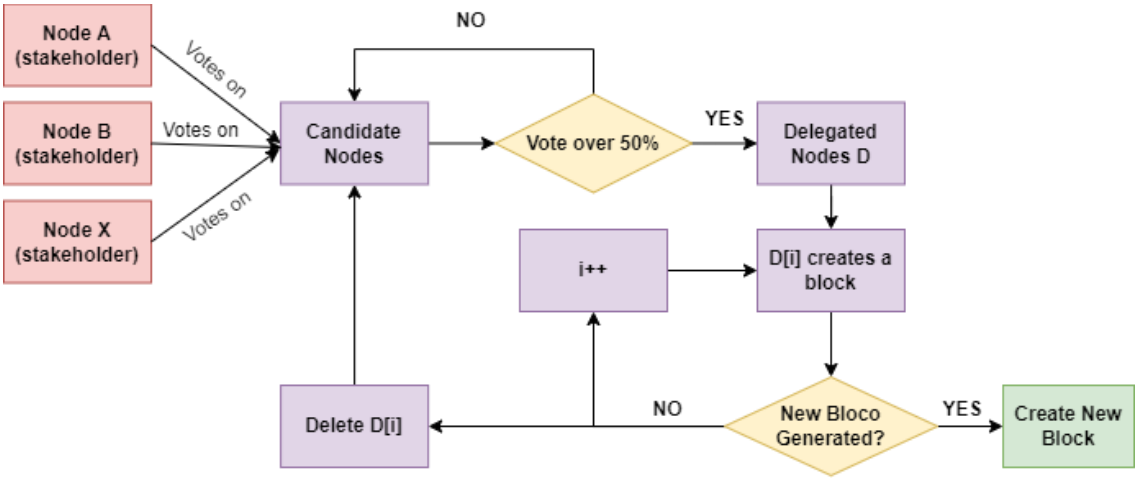


Figura 12 - Esquematização do processo no algoritmo de consenso Delegated Proof of Stake.

Antes de apresentar as diferentes versões da tecnologia blockchain é importante resumir todo o processo de adição de nova informação à cadeia.

Na figura 13, podem ver-se esquematizados os diferentes passos envolvidos na adição de um novo bloco à cadeia. O processo começa com nova informação que se pretende adicionar à cadeia de blocos (ex: dados relativos a transferências). Esta informação é transmitida a vários nós participantes da rede. Os nós responsáveis pela mineração irão procurar solucionar o problema relacionado com a variável de *Nonce*. A partir do momento que existe uma solução, é utilizado um método de consenso entre nós da rede para decidir qual o criador do novo bloco e por consequência qual o nó a ser recompensado [78].

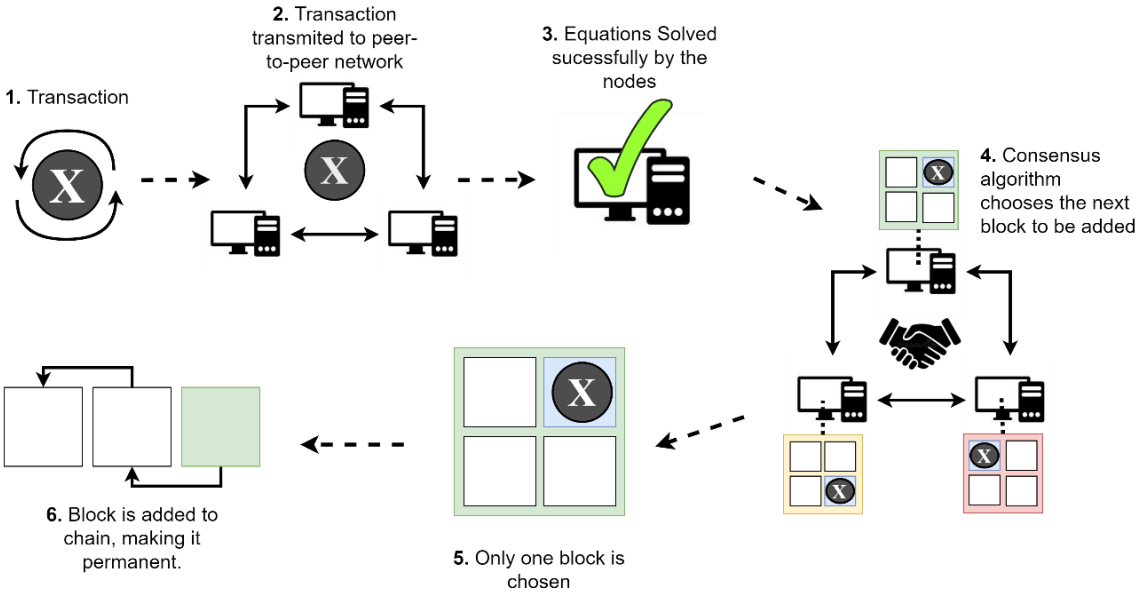


Figura 13 - Generalização do processo de adição de um novo bloco na blockchain.

2.2.5 Diferentes Versões da Tecnologia

Existem diferentes versões da tecnologia blockchain que se podem agrupar em diferentes gerações. Cada uma destas gerações possui características cada vez mais complexas. Quanto mais recente, menor o consumo energético, menor o custo de manutenção, menor o tempo de execução e maior a escalabilidade. [79]. Até ao momento, existem 4 gerações da tecnologia:

- **Blockchain 1.0:** Foi a primeira implementação. Limitada ao armazenamento de dados e transferência de valores por meio de criptomoedas[19], apresenta conceitos fundamentais como a transparência, distribuição pública da informação e uso de algoritmo de consenso (ex: Bitcoin) [80].

- **Blockchain 2.0**: Torna-se programável devido ao uso de *smart contracts* (definido em baixo), o que permite desenvolver aplicações que expandem o leque de aplicabilidade da blockchain (ex: Ethereum). Esta adição permite transformar a blockchain de uma visão relacionada com dinheiro e pagamentos para uma mais geral que se pode relacionar com qualquer tipo de ativo (ex: certificados, obras de arte, imobiliário, …) [81].

- **Blockchain 3.0:** Procura corrigir problemas relacionados com a escalabilidade, interoperabilidade[20] e privacidade de forma a difundir e aumentar o grau de adoção da tecnologia (ex: Polkadot) [82]. Foi ainda nesta geração que se deu o aparecimento das *Decentralized Applications* (DApp's) que se apresentam como aplicações onde o código é executado na rede blockchain. [79]

[19] Criptomoedas - Moeda digital, onde as transações são verificadas e mantidas através de um sistema descentralizado por meio de criptografia.
[20] Interoperabilidade - Capacidade de um sistema de comunicar com outro sistema distinto.

- **Blockchain 4.0:** Atualmente, a última geração da tecnologia, promete apresentar a blockchain como um ambiente de criação e de execução de aplicações para o negócio. A velocidade de processamento aumenta e o nível de especialização necessário para manusear com a tecnologia diminui [83].

Smart Contracts

Quer seja para trocas comerciais ou para parcerias estratégicas, no mundo empresarial os contratos servem como forma de solucionar conflitos legais e salvaguardar interesses estipulados. A blockchain cria na segunda geração da tecnologia algo que pretende atuar como uma analogia, os smart-contracts [84].

São contratos digitais que se auto executam quando certas condições pré-determinadas são cumpridas. São construídos à base de linhas de código que estipulam todos os termos entre ambas as entidades. Assim, o código e os termos contratuais encontram-se distribuídos de uma forma descentralizada por toda a rede blockchain.

2.2.6 Criptomoedas

Um dos pressupostos da economia atual é a troca de dinheiro (físico ou digital) por um produto ou serviço. No universo da tecnologia blockchain existe uma virtualização de um ativo que funciona como dinheiro digital, as criptomoedas [85].

Como o nome indica, são moedas cunhadas fruto do uso de criptografia, que apresentam correspondência com o proprietário atual através da lista de registos presentes na blockchain. Ao contrário das moedas tradicionais (fiat[21]), o valor das criptomoedas não é uma consequência de um acordo social nem provém da confiança da entidade que realiza a emissão monetária[22], representa apenas o valor que o mercado está disposto a pagar [86].

Na tabela 2, pode ver-se algumas métricas para as criptomoedas atualmente mais populares no mercado (janeiro de 2022), sendo que, somadas representam mais de 70% da capitalização total do mercado. Apesar do número de criptomoedas Bitcoin em circulação ser relativamente baixo (18 921 593), o valor unitário por moeda é elevado (43 053 dólares) e por isso a capitalização de mercado é alta (39.75%) [87].

[21] Dinheiro Fiat - Representa o conceito clássico de dinheiro, onde o valor deriva da confiança que as pessoas colocam nele (ex: euro, dólar, libra) [155].

[22] Emissão monetária - Ato de colocar moeda em circulação e de criar a responsabilidade pela sua aceitação em pagamentos ou trocas [156].

Tabela 2 - Analise de algumas métricas para as 4 criptomoedas mais populares do mercado [87].

	Crypto Currency	Price (un.)	Market Cap	Market Share (%)	Circulating Supply
	Bitcoin	43 053	814 377 591 712	39.75	18 921 593
	Ethereum	3 407	406 180 015 476	19.77	119 049 617
	Binance Coin	474	79 144 639 164	3.85	166 801 148
	Solana	149.83	46 495 128 474	2.26	309 418 662

A geração de criptomoedas encontra-se associada ao processo de mineração, nomeadamente, no momento de atribuição de recompensa ao nó criador do bloco. É algo concretizado coletivamente pela rede blockchain a um ritmo publicamente conhecido [88]. No entanto, existem alguns casos, como o da moeda XRP da rede Ripple, onde as criptomoedas já se encontram mineradas e uma entidade central controla a distribuição [89].

Na tabela 3, podem ver-se expressas duas métricas para o ciclo das criptomoedas: o teto máximo e o ritmo de criação. Algumas criptomoedas como a binance coin foram previamente criadas e já se encontram todas em circulação. Outras como a Solana, não possuem limitações, e o número total de criptomoedas vai reduzindo a um ritmo pré-determinado.

Tabela 3 - Ciclo de vida de algumas das criptomoedas mais populares no mercado (CoinMarketCap, 2021; Investerest, 2019).

	Crypto Currency	Max Supply	Rate of Creation
	Bitcoin	21 000 000	6.25 a cada 10 min
	Ethereum	18 000 000 criadas/ano	2-3 a cada 15 segundos
	Binance Coin	166 801 148	Todas já criadas
	Solana	Não tem	Diminui percentualmente até ser 1.5% por ano

2.2.7 Token

A principal diferença entre um token e uma criptomoeda é o facto da criptomoeda possuir uma rede blockhain própria (ex: Bitcoin ou Ethereum) enquanto o token é criado numa camada superior de uma rede blockchain através das funcionalidades do ecossistema (ex: DAI ou LINK que foram criadas para utilizar a rede blockchain Ethereum). Uma outra diferença, é a forma como o token pode representar um ativo físico ou um serviço (ex: Token que representa um Dinar kuwaitiano com correspondência 1:1 para o Dinar real dentro da rede Ripple) [90].

Na figura 14, pode ver-se a representação de uma analogia que ajuda na compreensão da definição. Os tokens são como fichas num casino, usados para substituir a quantidade de dinheiro que suportam. A ficha substitui o ativo (dinheiro), sendo que este só pode ser utilizado numa situação pré-determinada no próprio ambiente (estabelecimento do casino). A troca da ficha que representa o dinheiro tem de ocorrer dentro do casino. O valor da ficha não se mantém fora do casino. O mesmo acontece com vários tokens no universo da blockchain, sendo que o casino representa a rede onde estão inseridos [91].

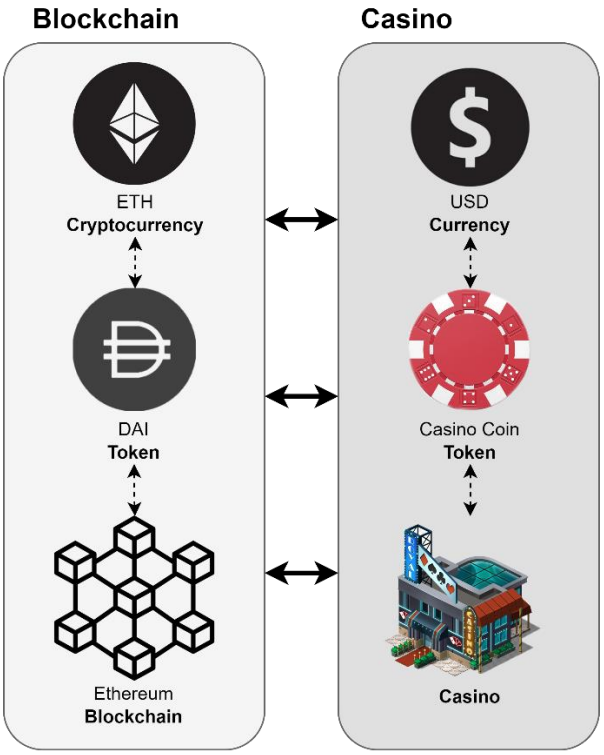


Figura 14 – Esquematização de uma analogia entre tokens da blockchain e tokens de casinos.

2.3 Envio de Remessas utilizando Blockchain

Na atualidade, a economia das remessas internacionais encontra-se fortemente interligada com instituições centralizadas como bancos e agências de câmbio. No entanto a tecnologia blockchain tem sido utilizada nos últimos anos como base para desenvolver soluções financeiras interoperáveis[23] que procuram satisfazer as necessidades neste mercado de uma forma transparente, rápida e económica [92].

Os projetos que se encontram atualmente a operar tendem a focar-se em determinados mercados dentro da atividade de envio de remessas. Exemplo disso é a empresa Everex sediada em Singapura que proporciona através da rede blockchain Ethereum, soluções para transferências no mercado asiático [93]. Um caso concreto foi a parceria entre a Everex e o Shwe Urban & Rural Development Bank que permitiu estabelecer o serviço entre os emigrantes de Myanmar que se encontravam a trabalhar na Tailândia e pretendiam enviar dinheiro às suas famílias em Myanmar [94]. O mercado de remessas de Myanmar representa um total de 9.3 mil milhões de dólares, correspondendo a 3.2% do PIB do país [95].

Todos os continentes, com exceção da Antárctica, possuem hoje pelo menos uma solução para a atividade de envio de remessas que utiliza parcial ou totalmente blockchain para o seu funcionamento.

Na figura 15 pode ver-se a distribuição do número de soluções que utilizam blockchain existentes no mercado pelos diferentes continentes. O continente africano e o continente sul-americano carecem na oferta deste tipo de serviços. Só para determinados corredores é que as populações conseguem ter acesso a uma oferta mais rápida e mais barata que utiliza tecnologia blockchain. No caso do continente africano, que é o que se encontra mais próximo da realidade que recai em foco do estágio, apenas em 4 países (Gana, Gibraltar, Quénia e Africa do Sul) é que se torna possível aceder a serviços de envio de remessas que utilizam a tecnologia blockchain.

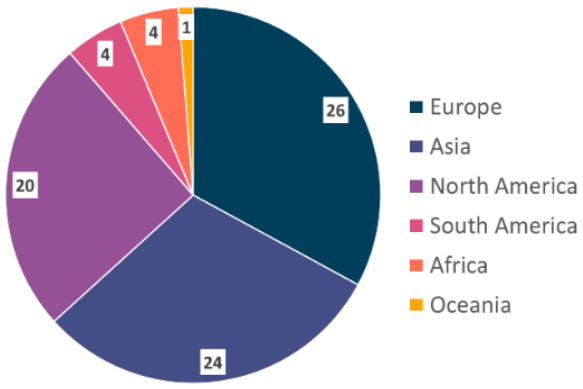


Figura 15 - Distribuição do número de soluções que utilizam blockchain atualmente existentes no mercado por continente [96].

[23] Interoperável – Capacidade de um sistema de se comunicar de forma transparente com outro sistema. É importante que trabalhe com padrões abertos ou ontologias [157].

Soluções Semelhantes

Com 79 soluções diferentes atualmente disponíveis no mercado mundial que geram e atraem milhões de dólares de investidores privados, a fatia de mercado de serviços que utilizam tecnologia blockchain para operar na atividade de envio de remessa é cada vez maior [96]. Torna-se assim importante analisar algumas das atuais soluções de sucesso para compreender a forma como a rede blockchain pode contribuir positivamente para o funcionamento das aplicações.

Bithumb

É uma plataforma de câmbio de criptomoedas na Coreia do Sul que permite transações entre contas com comissões baixas (0.04% - 0.25%) [97]. Com maior foco no mercado local apenas suporta a moeda de Won Sul-Coreano que permite aos seus utilizadores trocar por Bitcoin, Ethereum, Dash, Litecoin e Ripple a custo zero. Controla 59.19% do mercado de criptomoedas da Coreia do Sul.

Em 2019 estabeleceu uma parceria com a BitPay de forma a competir nos mercados internacionais de remessas, nomeadamente no corredor de transferências entre os países ocidentais e a Coreia do Sul. Promete reduzir os atuais custos médios deste corredor de transferências de 4% e de uma duração de 4 dias para 1% e 1 dia [98].

Todas soluções da Bithumb resultam atualmente do sucesso da rede desenvolvida pela empresa, a rede Bithumb Chain que utiliza a moeda nativa Bithumb Coin para todas as operações [99].

Digiledge

É uma empresa sediada na India com foco no mercado local. Proporciona soluções que utilizam tecnologia blockchain para o setor bancário, de seguros e de transporte de mercadorias [96].

Atualmente detentora de uma plataforma para envio de remessas internacionais (DIRP - *Digiledged International Remittance Plataform*) pretende adquirir parte da fatia comercial da atividade para o corredor internacional de envio de remessas EUA – India [100].

Ao contrário da Bithumb, a Digiledge utiliza unicamente a tecnologia blockchain para conectar e unificar os vários participantes já existentes na atividade de envio de remessas (forex dealers, empresas de câmbio de moedas, departamento do tesouro, …) e por isso não utiliza nenhum tipo de criptomoeda nativa. Todo o sistema é construído na rede Corda [101].

One Pay FX

Em 2019, a empresa espanhola Santander que possui um forte conhecimento do setor financeiro mundial, investiu na tecnologia blockchain como promessa de melhorar a experiência futura do utilizador face aos serviços atuais (Santander, 2021).

Atualmente, disponibiliza a solução *One Pay FX* para cobrir a atividade de transferências internacionais, nomeadamente com foco nas remessas provenientes da América Latina visto tratar-se de um mercado que detém um maior conhecimento comercial. A solução blockchain encontra-se desenvolvida na rede Ripple com uso da tecnologia de pagamentos *xCurrent* [103].

Adicionalmente, o Santander incorporou a tecnologia dos Smart Contracts através de uma parceria com a plataforma de blockchain da IBM (tecnologia Hyperledger) de forma que empresas clientes pudessem beneficiar da segurança, velocidade e custos associados ao realizar de contratos digitais com outras entidades (Santander, 2022) [105].

Capítulo 3
Análise e Definição Tecnológica

A solução a desenvolver no âmbito do estágio pretende inserir-se no mercado africano de envio de remessas internacionais. O país piloto selecionado para o desenvolvimento do protótipo foi a Tanzânia e por isso é importante começar por analisar este mesmo mercado e tê-lo sempre em consideração em todas as escolhas arquiteturais. De seguida serão analisadas várias redes blockchain de forma a selecionar e validar a mais adequada para o desenvolvimento.

3.1 Requisitos Específicos ao Mercado da Tanzânia

Em 2020, um total de 409.14 milhões de dólares foram enviados para famílias na Tanzânia resultado da atividade de envio de remessas internacionais [106] [107]. Este número tende a aumentar todos os anos, em especial com a recém-entrada de empresas no mercado que procuram oferecer novas soluções para a atividade [108].

Esta atração ao mercado tanzaniano por parte de empresas internacionais provém não só pela relevância da atividade para a economia do país, mas também pelos apoios e incentivos do estado local para atrair empresas *FinTech* que ajudem a reduzir a percentagem de população *unbanked*[24] (ex: a Tanzânia foi o primeiro país no mundo a implementar a interoperabilidade financeira, ou seja, o utilizador pode transferir dinheiro entre contas de *mobile money*[25] diferentes mesmo que sejam de empresas competidoras) [109].

A maioria dos fluxos das remessas internacionais para a Tanzânia são provenientes dos Estados Unidos da América e do Reino Unido o que torna essencial para o sucesso da operação garantir o câmbio entre Dólar-Xelim Tanzaniano e Libra-Xelim Tanzaniano [109]. Na figura 16, pode ver-se todos os países que constituem o fluxo entrante de remessas internacionais para a Tanzânia.

[24] Unbanked – Termo utilizado para descrever populações de idade adulta com falta de acesso à infraestrutura bancária [158].

[25] Mobile Money – Um dos principais instrumentos financeiros tecnológicos para servir os que não tem acesso a infraestrutura bancária, é uma forma de utilizar serviços de pagamento através do telemóvel (mesmo que se trate de um telemóvel rudimentar) [38] (maior detalhe na subsecção 2.1.3).

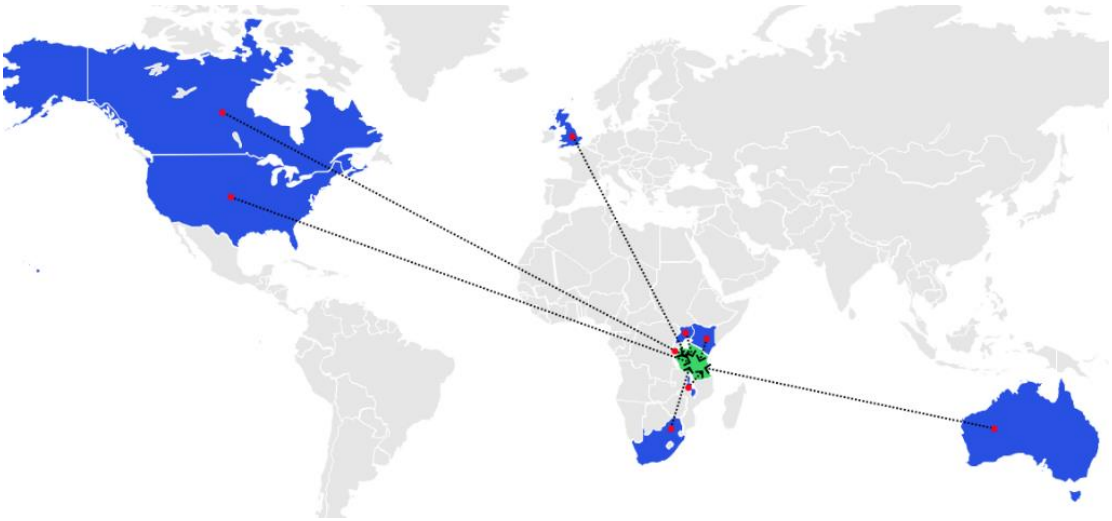


Figura 16 – Representação geográfica dos países que constituem o fluxo entrante de remessas internacionais para a Tanzânia.

3.2 Escolha da Tecnologia de Desenvolvimento

O protótipo a desenvolver no âmbito do estágio teria que permitir ao utilizador concretizar o seguinte fluxo: depositar dinheiro, enviar dinheiro e levantar dinheiro para uma conta bancária ou de *mobile money*. Para que fosse possível realizar todas estas operações bem como as relacionadas com a gestão da carteira digital, é necessário que a solução interaja com uma rede blockchain que será responsável por toda a lógica subjacente.

Após a analise na secção anterior ao mercado da Tanzânia, podemos concluir que existe um conjunto de fatores a considerar na escolha da rede blockchain:

1. **Aceitar depósitos de USD e GBP**.
2. Permitir **converter USD/GBP para TZS**.
3. Aceitar **levantamentos para contas de *mobile money***.

Outros fatores a considerar que se relacionam com a escalabilidade e competitividade da solução a produzir são:

4. **Preço por transação** (USD) - De forma a garantir que é mais baixo que a média de mercado.
5. **Tempo por transação** (segundos) – De tal modo que seja suficientemente rápido para existir uma preferência pelo utilizador.
6. **Mecanismo de consenso** (impacto energético) – Importante garantir que a solução mantém um impacto ecológico reduzido mesmo na situação de escalar.

3.2.1 Escolha da Rede Blockchain - Benckmark

Para suportar a escolha da rede blockchain para o protótipo, foi construída uma tabela benchmark[26] que tivesse em consideração o conjunto de fatores considerados necessários para o sucesso da solução no mercado alvo (referidos anteriormente no formato de uma lista).

Na tabela 4, pode ver-se uma comparação de algumas das redes blockchain mais populares face aos fatores considerados e listados anteriormente. Cada coluna representa respetivamente o enumerado na lista anterior.

Tabela 4 - Benchmark a diferentes redes blockchain.

Network	USD/GBP Deposit *	Exchange USD/GBP to TZS	Withdraw to mobile money	Transaction Price (Dollar)	Transaction Time (Secound)	Consensus Mechanism (Impact)
Ripple	✓ [110]	✗ [111]	✓ [112]	0.000003215 [113]	3 – 5 [114]	RPCA[27] (low) [115]
Stellar	✓ [116]	✓ [117]	✓ [118]	0.000001100 [119]	3 – 5 [120]	SCP[28] (low) [115]
Algorand	✓ [121]	✗ [122]	✓ [123]	0.000311500 [124]	< 5 [125]	PoS (average) [126], [115]
Ethereum	✓ [127]	✗ [128]	✓** [129]	2.182000000 [130]	15 – 300 [131]	PoW (high) [115]
Chia	✓ [132]	✗ [133]	✗ [129]	0.020088533 [134]	60 - 300 [135]	PoC (low) [115]

Ao analisar a tabela 4 que compara diferentes redes blockchain de acordo com os fatores considerados anteriormente, concluímos que apenas a rede da Stellar verifica todos, é a única a permitir converter USD/GBP para TZS e ainda a que apresenta a taxa de transferência mais baixa. A rede da Stellar foi então a selecionada para desenvolver o protótipo.

[26] Benchmark – Algo que se tem conhecimento da qualidade ou quantidade e pode ser usado para comparar com outras coisas.

[27] RPCA (*Ripple Protocol Consensus Algorithm*) – Algoritmo de consenso próprio da rede Ripple construído com base no mecanismo de consenso de *Byzantine Fault Tolerance*.

[28] SCP (*Stellar Consensus Protocol*) – Algoritmo próprio da rede Stellar construído com base do mecanismo de consenso *Federated Byzantine Agreement*.

*O depósito de USD/GBP é realizado numa empresa de câmbio de criptomoedas como por exemplo a Coinbase/Binance, onde se torna possível trocar dinheiro fiat por criptomoedas e transferir para a carteira digital da respetiva rede.

**Para realizar o levantamento para uma conta de mobile money é necessário utilizar um serviço externo como por exemplo o KeeCash.

3.2.2 Rede Blockchain Stellar

A rede Stellar foi criada em 2014 pela *Stellar Development Foundation* e encontra-se entre as redes blockchain mais populares com uma das criptomoedas nativas[29] mais dominantes do mercado (capitalização de mercado de 2.7 mil milhões, na posição 18# de popularidade) [136]. É uma rede descentralizada e *open-source*[30] ligada ao setor financeiro com o objetivo de facilitar, acelerar e proporcionar um serviço mais barato, servindo como complemento e não substituto ao atualmente disponível no mercado [120].

A principal missão da Stellar é permitir que o poder da economia digital esteja presente em todo o mundo e para todos, em especial para a população *unbanked* que se encontra afetada pela atividade de envio de remessas internacionais. Pretende reduzir a dificuldade e custos no desenvolvimento de soluções que contribuíam para corredores de transferência internacional mais baratos [137]. Este *motto*[31] alinha-se com os objetivos do estágio e reforça novamente a escolha da tecnologia.

Aspetos Relevantes

O sucesso atual da rede Stellar deve-se largamente a duas componentes que integram a rede: plataforma descentralizada de câmbio de criptomoedas (**Stellar DEX**) e à noção da entidade existente na rede que serve para converter moedas reais em criptomoedas e vice-versa (**Anchor**).

A **Stellar DEX** é um mecanismo interno da rede que permite aos utilizadores trocar e converter criptomoedas. Apresenta-se como algo essencial em operações de transferência internacional onde a moeda enviada é muitas vezes diferente da moeda recebida [138].

A conversão dos ativos é realizada através da criação de pedidos de venda e compra por parte de contas existentes na Stellar, ou seja, de forma simétrica ao tradicional livro de ordens que existe no mercado mundial [138].

Na figura 17, pode ver-se uma representação exemplo de um livro de ordens para a troca de ovelhas por trigo. O número de ordens aumenta para as extremidades dos pedidos de venda do ativo, isto porque são os pedidos que mais beneficiam o vendedor. A *spread* no meio do gráfico representa a diferença entre a ovelha mais barata à venda no mercado e o trigo mais barato à venda no mercado.

[29] Criptomoeda nativa – Criptomoeda desenvolvida pela própria rede blockchain que serve de ativo primário para todas as operações.
[30] Open-Source – Software cujo código fonte encontra-se disponível para ser modificado e distribuído.
[31] Motto – Frase curta que encapsula os ideais de uma instituição.

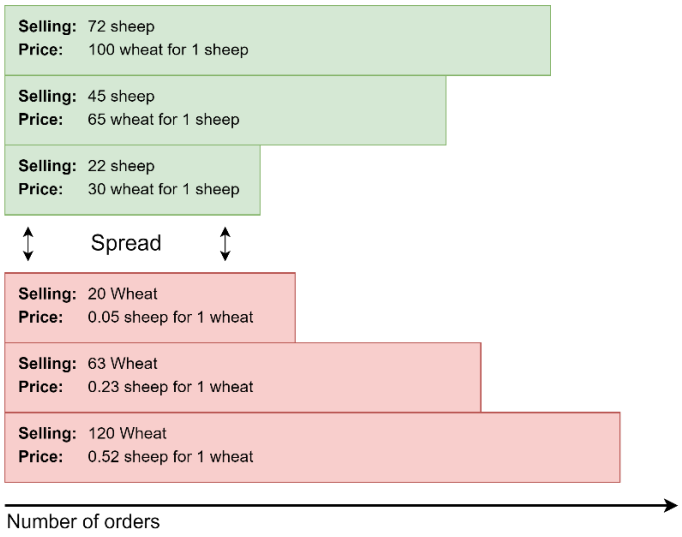


Figura 17 - Exemplo de um livro de ordens para a troca de ovelhas por trigo.

No paradigma atual, cada região do mundo possui uma arquitetura única para realizar transferências de fundos entre contas (ex: ACH, SEPA, SPEI, …) que não são interoperáveis entre si.

De modo a solucionar esta lacuna de comunicação entre instituições bancárias de diferentes regiões, a rede Stellar permite representar todas as moedas do mundo em formato de tokens digitais. Para além disso, existe também uma entidade na rede, o **Anchor**, que permite ao utilizador converter dinheiro fiat em tokens e tokens em dinheiro fiat, servindo de ponto de entrada e saída ao universo da blockchain na rede Stellar. É então uma entidade que permite conectar bancos tradicionais à rede, existindo a opção de eles próprios se tornarem num Anchor [139].

Na figura 18, pode ver-se uma esquematização da forma como o Anchor funciona. Neste caso o Anchor A converte o dinheiro fiat em tokens dentro da rede Stellar com a correspondência 1:1 para a carteira digital do utilizador que realizou o pedido de depositar os fundos. O utilizador irá realizar um pedido de conversão e transferência de tokens (neste caso para um que representa o real brasileiro) e o recetor da transferência para obter os reais brasileiros correspondentes na sua conta bancária terá de utilizar um outro Anchor.

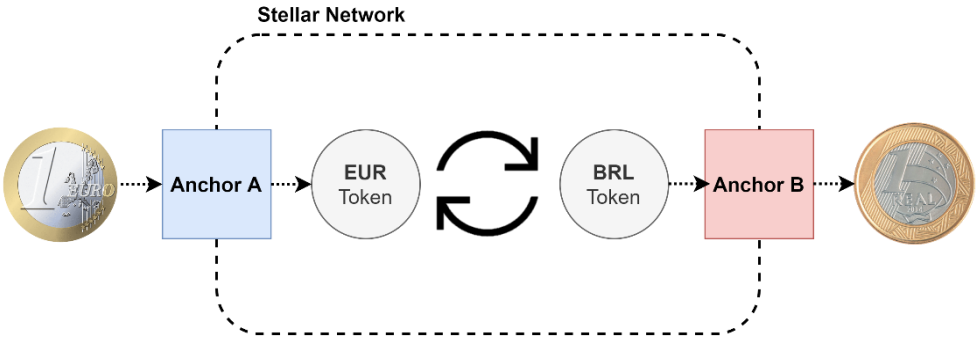


Figura 18 - Esquematização da interação de um Anchor com a rede Stellar.

3.3 Análise da Documentação da Rede Blockchain Escolhida

Para adquirir maior conhecimento técnico sobre a rede Stellar e validar que seria possível desenvolver todos os componentes responsáveis por assegurar os objetivos do protótipo no âmbito do estágio foi explorado a ferramenta Stellar Laboratory.

O Stellar Laboratory permite aos desenvolvedores interagir com a rede de teste da Stellar de uma forma prática, rápida e sem custo. Todos os endpoints e funcionalidades estão disponíveis para testes, o que inclui: criação de conta na rede, construção e submissão de transações e ainda visualização de informação importante sobre o estado atual da rede.

Na figura 19, pode ver-se uma captura de ecrã representativa do formulário que guia o utilizador na construção de uma transação, para que esta fosse então submetida na rede.

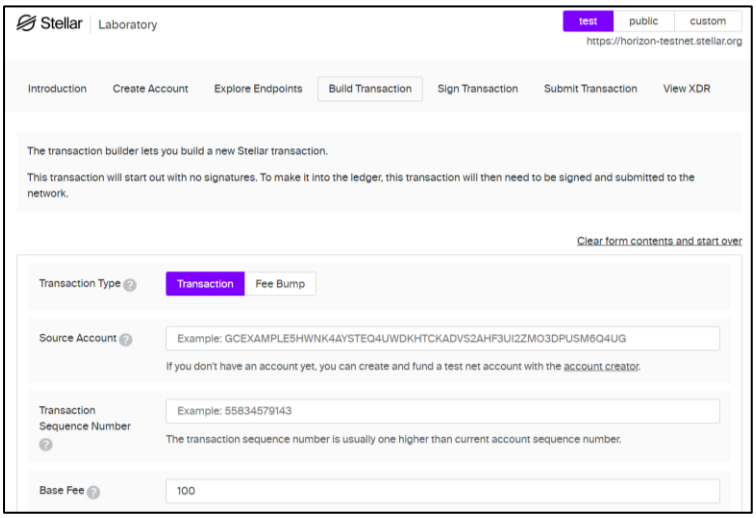


Figura 19 - Captura de ecrã do Stellar Laboratory.

Seguem-se algumas das operações base na rede de testes da Stellar de forma a abranger as funcionalidades disponíveis sem custos para o autor.

1. **Criação de uma Conta**

O primeiro passo para interagir com a rede Stellar é criar uma conta. Na criação de uma conta é gerado um par de chaves: a chave pública e a chave privada. Para que uma conta seja capaz de receber e enviar ativos na rede Stellar tem de se encontrar ativa. Uma conta encontra-se ativa na rede quando possui um saldo mínimo de XLM (criptomoeda nativa da Stellar) de acordo com a seguinte formula:

Saldo Mínimo *= (2 + # entradas + # entradas patrocinadas - # entradas que patrocina) * reserva base*

As entradas representam criação de ofertas no mercado, assinaturas, entradas de dados e o estabelecer de linhas de confiança (trustlines, que serão abordadas mais abaixo). As entradas patrocinadas/que patrocinam representam situações onde contas suportam o saldo mínimo de outras contas. A reserva base é um número estabelecido pela rede que define a quantidade mínima para contas com zero entradas, atualmente (2022) é de 0.5 XLM.

Na figura 20, pode ver-se a forma como é possível criar e ativar uma conta no Stellar Laboratory. Na secção "Create Account" (1) podemos gerar a chave pública e privada da conta (2) e de seguida adicionar 10 000 XLM de teste para assegurar que a conta se encontra ativa na rede (3).

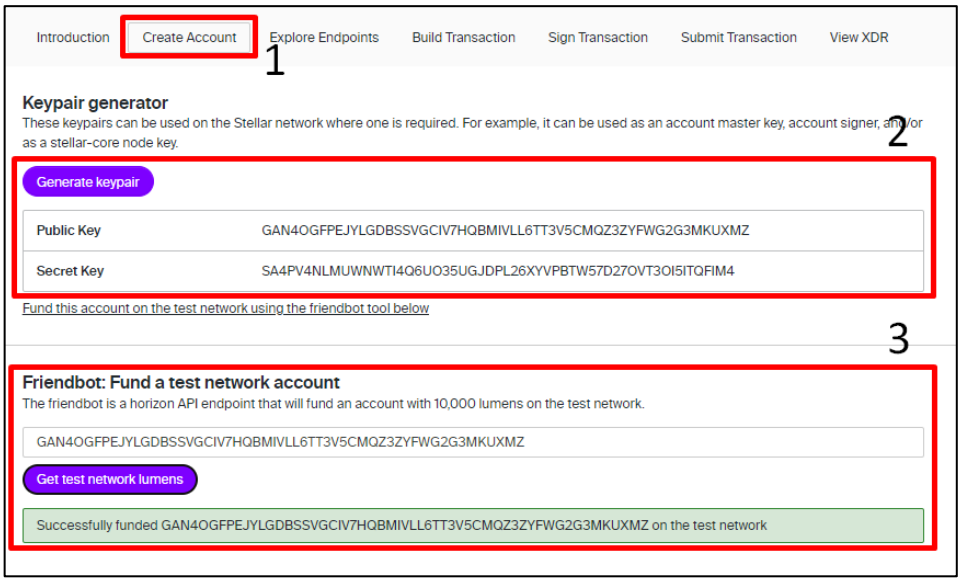


Figura 20 - Captura de ecrã para a criação e ativação de uma conta na rede de testes da Stellar.

2. Transferência direta

Uma transferência direta na rede Stellar envolve transferir os fundos sem conversão de moeda entre duas contas ativas distintas. É necessário construir o objeto de transação que será constituído obrigatoriamente por:

- **Identificador da conta emissora** – Chave pública
- **Número de sequência da conta emissora** – Número associado a uma conta de forma a impedir transações duplicadas.
- **Taxa** – Quantidade de XLM que os emissores se dispõem a pagar aos mineiros.
- **Tipo de operação** – Definir o tipo de operação, neste caso de uma transferência direta é um *Payment*.
- **Destino** – Identificador da conta destino.
- **Ativo** – Identificar o ativo a enviar.
- **Quantidade de ativo a enviar**.

Para garantir que quem construiu o objeto de transação é de facto o detentor legitimo da conta que enviou os fundos, é necessário assinar a transação com a chave privada. Só assim é que a transação será submetida e executada com sucesso na rede.

Na figura 21, pode ver-se uma transação construída no momento de assinatura com a chave privada. O envelope (1) contém uma encriptação das operações que se desejam realizar, neste caso uma operação de transferência direta. Podemos visualizar os restantes parâmetros da transação (2) e o local onde se insere a chave privada para assinar (3).

Figura 21 - Captura de ecrã do momento de assinar uma transação já construida.

Verificando o saldo das duas contas através de pedidos ao endpoint *https://horizon-testnet.stellar.org/accounts/* da rede de teste da Stellar, verificamos que a transferência foi um sucesso e que os 500 XLM foram transferidos.

Na figura 22, pode ver-se à esquerda o saldo final da conta emissora e à direita o saldo final da conta recetora.

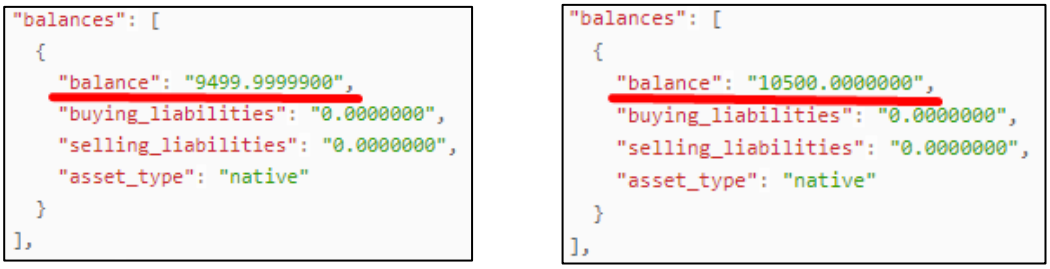


Figura 22 - Saldo final das contas envolvidas na transação.

3. Transferência com conversão

Numa transferência com conversão de moeda entre duas contas a rede Stellar utiliza a sua plataforma descentralizada de câmbio (Stellar DEX) para automaticamente converter a moeda que a conta emissora da transferência envia na moeda que pretende que a conta recetora receba.

A operação com conversão de moeda pode ser de dois tipos: ***Path Payment Strict Send*** ou ***Path Payment Strict Receive***. Divergem respetivamente na forma como na primeira o emissor bloqueia a quantidade de moeda que pretende enviar e na segunda na forma como o emissor bloqueia a quantidade de moeda que pretende que o recetor receba. Esta diferença entre o que se envia e o que se recebe deve-se à volatilidade no mercado, e é uma forma do utilizador controlar os custos. Ou fixa o que paga pela transação ou fixa o que o recetor recebe.

Apesar da operação ser semelhante à operação de transferência direta, existem agora dois novos parâmetros no objeto de transação:

- **Moeda enviada** – Criptomoeda que o emissor deseja utilizar para pagar a transferência.
- **Moeda destino** – Critptomoeda que o emissor pretende que o recetor receba.

Adicionalmente surge um novo conceito fundamental para concretizar a operação, o conceito de **trustline**. No momento que uma conta se torna ativa, esta só poderá enviar e receber a criptomoeda nativa da rede, ou seja, o XLM. Para que seja possível receber uma criptomoeda diferente é necessário o detentor da conta estabelecer explicitamente uma trustline com a conta que gere a criptomoeda desejada (**Issuer**). Esta operação representa uma linha de confiança com o ativo, ou seja, a conta confia no valor daquele token e aceita recebê-lo numa transferência.

As figuras 23, 24 e 25 relacionam-se com uma transferência com conversão (simulam uma transferência internacional) e representam capturas de ecrã de passos importantes na operação.

Na figura 23, pode ver-se uma captura de ecrã com os parâmetros que são necessários preencher para estabelecer uma operação do tipo trustline (1) com a criptomoeda que se pretende receber (2), onde é necessário especificar a quantidade máxima limite que a conta aceita confiar (o saldo relativo a esta criptomoeda não pode ultrapassar este limite) (3). Na parte direita da figura verificamos que depois de estabelecida a trustline, o saldo da conta possui a nova criptomoeda.

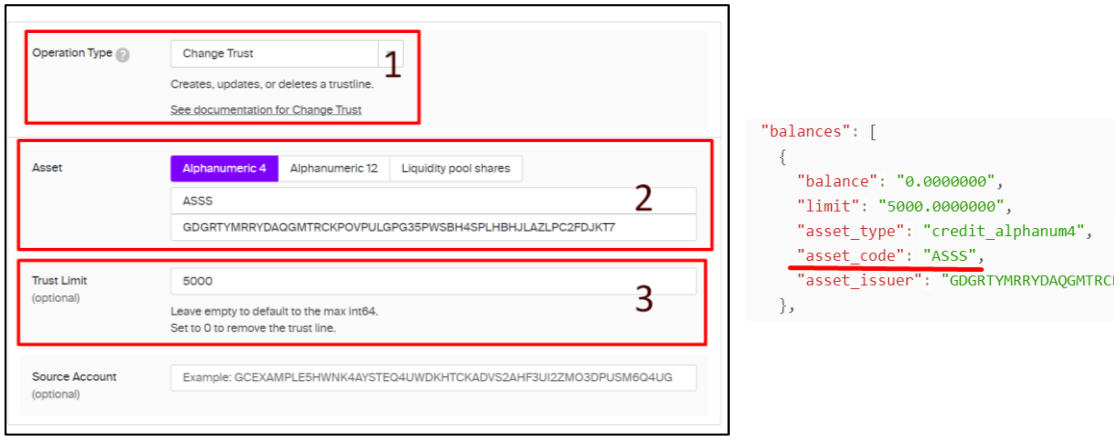


Figura 23 – À esquerda uma captura de ecrã do formulário de construção da operação de trustline. À direita o saldo da conta recetora depois do estabelecer da trustline.

Na figura 24, pode ver-se os parâmetros necessários a preencher para a operação do tipo *Path Payment Stric Send* (1) onde é necessário definir a criptomoeda que vamos utilizar para realizar o pagamento da transferência (2) e a criptomoeda que pretendemos que a conta recetora seja creditada (3).

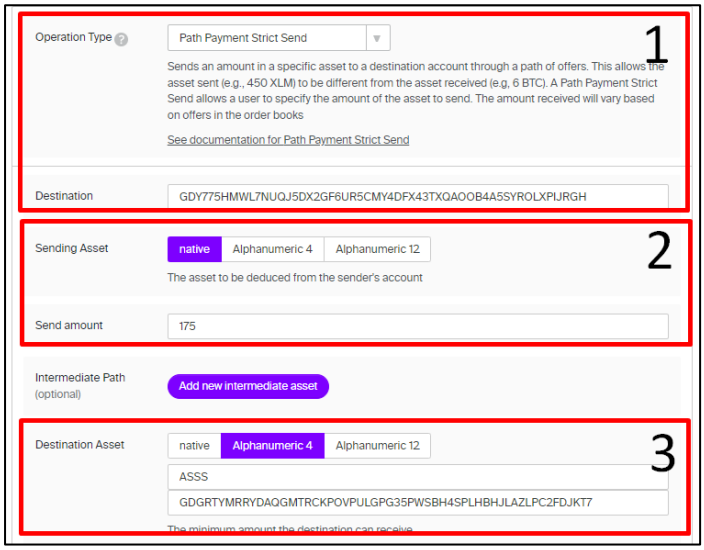


Figura 24 - Captura de ecrã do formulário de construção da operação de path payment strict send.

Na figura 25, pode ver-se o sucesso da operação e a forma como os saldos foram alterados. À esquerda o saldo da conta do emissor, e à direita o saldo da conta do recetor com 175 da criptomoeda destino.

Figura 25 - Saldo final das contas envolvidas na transação.

4. Levantamento de Fundos

Um dos objetivos do protótipo a desenvolver no âmbito do estágio passa também por garantir que é possível realizar o levantamento dos fundos que se encontram na carteira dentro da rede Stellar para uma conta bancária ou de *mobile money*. Isto torna-se possível através da entidade Anchor referida anteriormente.

Para testar esta funcionalidade existe uma outra ferramenta da rede Stellar que se encontra disponível para os desenvolvedores, a Stellar Demo Wallet (*demo-wallet.stellar.org).*

Na figura 26, pode ver-se uma captura de ecrã da ferramenta da Demo Wallet. Do lado esquerdo são apresentados detalhes relativos à chave da conta e ao saldo de fundos associado (já com 499 do ativo que irá ser usado na operação de levantamento). E do lado direito são apresentados detalhes relativos aos pedidos e respostas à rede Stellar de acordo com as ações do utilizador.

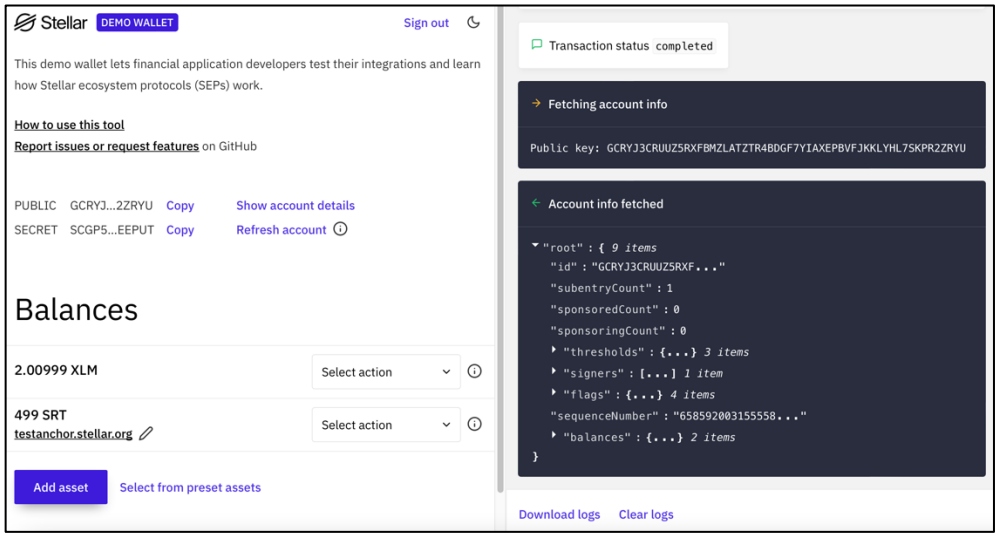


Figura 26 - Captura de ecrã da Demo Wallet.

Para realizar desta operação foi utilizado o Anchor de teste fornecido pela Stellar com o domínio (*testanchor.stellar.org*) onde é possível simular todos os passos envolvidos num levantamento sem custos para o desenvolvedor.

Na operação de levantamento existem dois protocolos disponibilizados pelo Anchor: **SEP-6** e **SEP-24**. Divergem respetivamente na forma como o detentor da conta preenche o formulário para realizar a operação. No protocolo SEP-6 o formulário é construído dentro da aplicação considerando os parâmetros necessários e a resposta é enviada para um dos endpoints do Anchor. No protocolo SEP-24, o utilizador é redirecionado para uma janela externa da aplicação, controlada pelo Anchor onde preenche o formulário com os valores pedidos.

Na figura 27, pode ver-se o preenchimento dos formulários para concretizar a operação de levantamento através do protolo SEP-6. Existe ainda um passo adicional de autentificação do cliente (KYC – *Know Your Customer*) que apenas é realizado na primeira interação entre conta da Stellar e o Anchor.

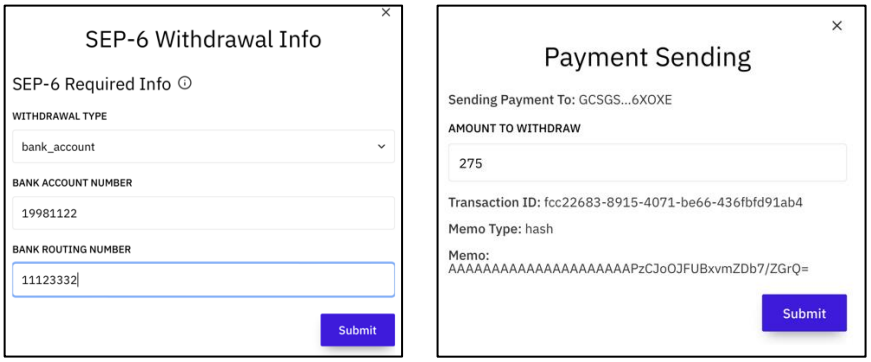


Figura 27 - Captura de ecrã dos formulários relativos ao levantamento através do protocolo SEP-6.

Na figura 28, pode ver-se o sucesso da operação e a forma como o saldo da conta foi deduzido. Apesar de não existir qualquer tipo de transferência para uma conta bancária real, a dedução e a mensagem de sucesso servem como prova de conceito que a operação é possível na rede Stellar.

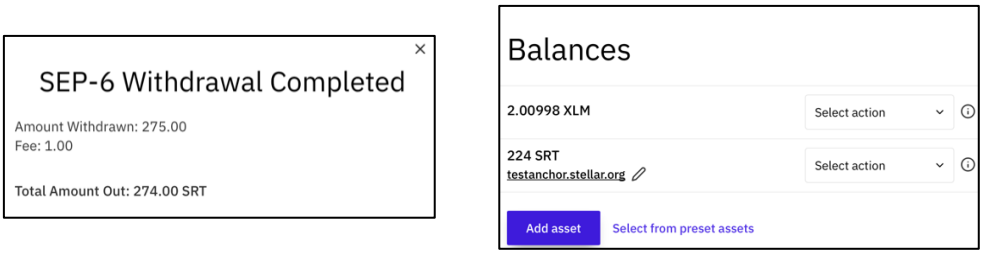


Figura 28 - Captura de ecrã relativa ao sucesso da operação de levantamento.

5. Resultado

Através da análise experimental realizada nas ferramentas *Stellar Laboratory* e *Demo Wallet* foi possível:

- Criar uma conta na Stellar.
- Realizar uma transferência direta entre duas contas.
- Realizar uma transferência com conversão de moeda entre duas contas.
- Realizar um levantamento de fundos.

Com o sucesso destas operações validou-se a rede Stellar como uma tecnologia capaz de cumprir com os objetivos da proposta para o estágio.

Esta página foi intencionalmente deixada em branco.

Capítulo 4
Proposta de Solução

Torna-se agora fundamental estruturar através de uma arquitetura de software a forma como as diferentes componentes da solução irão interagir para fornecer um serviço capaz de solucionar o problema apresentado.

A implementação desta arquitetura numa aplicação web reativa (portal de interação com o utilizador final) e num servidor responsável pela exposição de endpoints e gestão de notificações foram as componentes fundamentais para a concretização dos objetivos do estágio.

No entanto, uma parte ainda mais fulcral que se encontra subjacente, foi a parte de interação com a rede blockchain escolhida. Tornou-se desafiante porque exigiu um compreender pleno de várias operações existentes na rede blockchain e na forma como estas poderiam ser concretizadas e interpretadas para integrar com a solução desenvolvida.

Neste capítulo irá ser apresentada a arquitetura da solução e o produto final desenvolvido com todos os aspetos relevantes devidamente introduzidos e explicados.

4.1 Ferramentas de Desenvolvimento

No decorrer do estágio foram utilizadas várias ferramentas de software para permitir planear, testar e implementar os vários aspetos relacionados tanto com o desenvolvimento da solução final como até deste mesmo documento. Esta subsecção pretende listar e definir todas as tecnologias utilizadas.

Ferramentas de suporte ao desenvolvimento:

- **Diagrams.net (Draw.io) (versão 19.0.3)** – É um software *open-source* para criação de diagramas (flowcharts, wireframes, UML, …). Foi utilizado para criar a maioria das figuras presentes neste documento.
- **Trello (versão 4.3)** – Aplicação que serve como ferramenta de gestão de projeto. Foi utilizado para gerir os *sprints* (secção de planeamento) de acordo com a metodologia escolhida.
- **Figma (versão 116.0.5)** – Aplicação de edição gráfica vetorial que pode ser utilizado como ferramenta de prototipagem. Foi através dele que os *mockups*[32] foram construídos e a composição dos ecrãs discutida.
- **Paint.NET (versão 4.3.11)** – É um software de edição de imagens. Foi utilizado para construir e editar variados elementos presentes tanto neste documento como na solução final.
- **Mendeley (versão 1.19.8)** – Software para gestão de referências. Utilizado em extensão com o Microsoft Word.
- **ONDA DEI (versão 3.0)** – Ferramenta de modelação de base de dados desenvolvida pela comunidade do Departamento de Engenharia Informática.

Ferramentas de desenvolvimento:

- **Visual Studio Code (versão 1.68)** – É um editor de código da Microsoft. Foi utilizado para desenvolver todo o código da solução.
- **Postman (versão 9.21.3)** – Plataforma API para construir e testar APIs. Foi utilizado para validar de forma ágil os endpoints criados.
- **Stellar Laboratory (versão 2.3.0)** – Plataforma com um conjunto de ferramentas para permitir interagir com a rede de testes da Stellar de forma prática e com intuito de aprofundar conhecimentos.

[32] Mockups – Representação estática de um produto para demonstração do funcionamento a um utilizador ou *stakeholder* [159].

- **Stellar Demo Wallet (versão 2.0.0)** – Plataforma que interage com a rede de testes e a rede pública da Stellar de forma a realizar testes práticos e aprofundar conhecimentos relacionados com a carteira digital da Stellar.
- **PgAdmin (versão 6.10)** – Ferramenta para interagir com uma base de dados local ou remota de Postgres.

Tecnologias:

- **Java (versão 18.0)** – Linguagem de programação utilizada para escrever o código do *back-end* da solução.
- **Maven (versão 3.8.6)** – Ferramenta de gestão de dependências de código.
- **Spring Boot (versão 2.6.4)** – Framework baseada em Java utilizada para criar aplicações independentes prontas a executar no mercado.
- **Stellar Java SDK (versão 0.31)** – SDK[33] que permite integração com a rede Stellar.
- **React (versão 18.2.0)** – Livraria JavaScript para desenvolvimento *front-end*[34] da interface do utilizador com base em componentes de UI (ex: componentes de navegação, informação ou de *input*).

4.2 Arquitetura da Solução

Na figura 29, pode ver-se representadas a vermelho as componentes da arquitetura implementadas para concretizar a solução. Segue-se uma listagem dos diferentes elementos que compõem o esquema e uma breve explicação da forma como interagem com o sistema e contribuem para as funcionalidades presentes no protótipo.

[33] SDK (***S**oftware **D**evelopment **K**it*) – Conjunto de ferramentas e programas de software que facilitam o desenvolvimento de aplicações para plataformas específicas [160].
[34] Front-End - Refere-se à componente da interface que o utilizador interage [161].

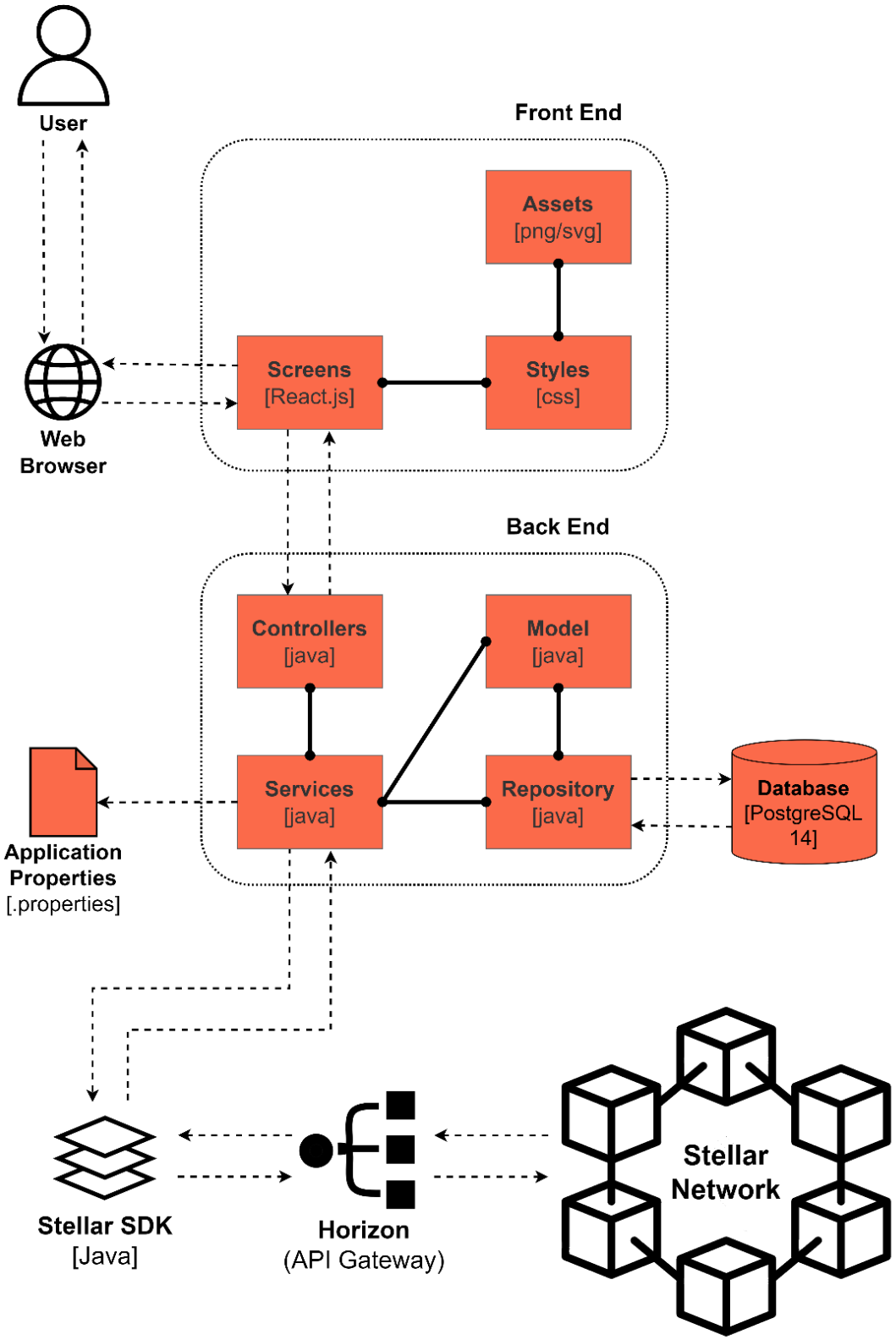


Figura 29 - Arquitetura do protótipo desenvolvido.

1. **User** - Representa o utilizador da aplicação web que interage através do *web browser* (2) num dispositivo móvel de modo a usufruir do serviço (ex: emigrante da Tanzânia).
2. **Web Browser** - Aplicação utilizada para realizar pedidos ao protótipo e apresentar os diferentes ecrãs (3.c) (ex: google chrome).
3. **Front-End:**
    a. **Assets** - Conjunto de elementos gráficos que serão renderizados nos ecrãs da aplicação de forma a contribuir para a usabilidade final do protótipo. Encontra-se interligado com os estilos (3.b) (ex: símbolo de *refresh*).
    b. **Styles** - Ficheiro CSS que contém toda a parametrização dos estilos para as componentes presentes nos ecrãs (3.c) (ex: tipo e tamanho da fonte)
    c. **Screens** - Ficheiros JavaScript (framework react) que definem toda a lógica de construção dos ecrãs. Certas interações nos ecrãs por parte do utilizador resultam em pedidos para os *endpoints* expostos pelos controladores (4.a) (ex: utilizador insere através de um formulário as suas credenciais e a informação é enviada a um dos endpoints dos controladores de forma a validar o login).
4. **Back-End:**
    a. **Controllers** - Constitui um dos elementos da arquitetura MVC e é responsável por expor uma API REST que recebe pedidos HTTP e através da lógica presente nos Serviços (4.b) devolve uma resposta aos ecrãs (3.c) que serão responsáveis pelo tratamento da informação recebida (ex: a validação das credenciais inseridas é enviada para o endpoint localizado no endereço /auth/login2).
    b. **Services** - Classes Java que contêm toda a lógica funcional do protótipo. Integra o SDK da Stellar (7) de forma a comunicar com a rede Stellar. Usa os modelos (4.c) para definir a estrutura dos objetos java. O repositório (4.d) é utilizado para fazer pedidos à base de dados (5). Utiliza valores de variáveis definidas no ficheiro de configuração (6) (ex: os endereços fixos dos responsáveis pelo levantamento de fundos).
    c. **Model** – Constitui um dos elementos da arquitetura MVC e representa classes Java que definem os diferentes objetos utilizados (ex: estrutura dos pedidos e respostas aos endpoints dos controladores (4.a)).
    d. **Repository** - Classes Java que utilizam a extensão JPA (Java Persistence API) de forma a facilitar as interações com a base de dados (5) para operações CRUD (Create, Read, Update & Delete).
5. **Database** – Componente onde são persistidos os dados da solução. A gestão é feita pelo sistema de base de dados PostgreSQL, versão 14.
6. **Application Properties** - Contém variáveis de configuração global da solução que são utilizadas pelos serviços (4.b) (ex: tempo máximo em segundos para concretizar uma operação na rede Stellar).

7. **Stellar SDK** (Software Development Kit) - Conjunto de ferramentas de software fornecidas pela Stellar que interagem com a Horizon (8) de forma a facilitar as interações com a rede blockchain (ex: livrarias, APIs e exemplos de código).
8. **Horizon** (API Gateway) - Gere pedidos às APIs de forma a permitir comunicar com a rede (9). Centraliza o local onde se devem enviar pedidos.
9. **Stellar Network** - Rede blockchain que persiste as alterações nas carteiras digitais e permite realizar as operações necessárias ao funcionamento do protótipo.

4.3 Base de Dados

A forma de persistir os dados relativos aos utilizadores da aplicação mesmo depois de terminar a sessão é através de uma base de dados. Para tal, construíram-se esquemas para todas as entidades com todas as variáveis constituintes de modo a garantir que os requisitos da aplicação seriam cumpridos (utilizou-se para a construção dos esquemas o programa ONDA, no endereço: http://onda.dei.uc.pt/v3/). O diagrama conceptual (fig. 30) e o diagrama físico (fig. 31) representam os esquemas criados manualmente para gerar automaticamente através do ONDA, os comandos SQL que construíam a base de dados. Na tabela 5, 6 e 7 pode ver-se a legenda de todas as colunas que constituem as entidades.

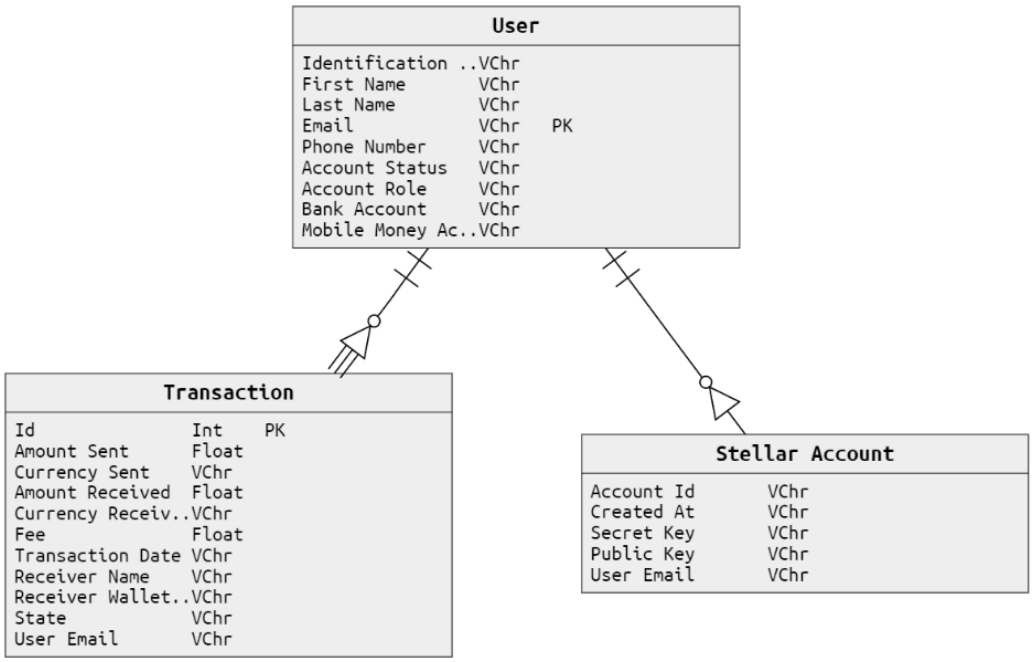


Figura 30 - Diagrama conceptual da base de dados.

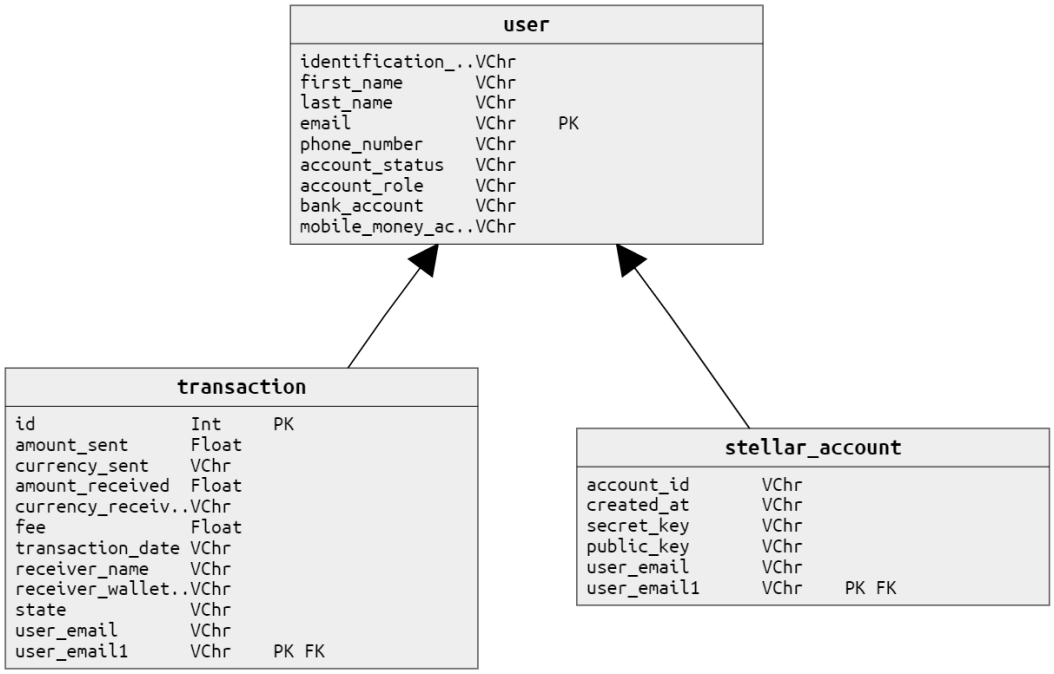


Figura 31 - Diagrama físico da base de dados.

Tabela 5 – Definição das colunas que constituem a entidade User (fig. 30) da base de dados.

Entidade	Variável	Significado
User	Identification Number	Número de identificação pessoal
User	First Name	Primeiro nome
User	Last Name	Sobrenome
User	Email	Endereço do correio eletrónico
User	Phone Number	Número de telemóvel
User	Account Status	Estado da conta (Ativo, desativo ou bloqueado)
User	Account Role	Nível de privilégios (User ou Admin)
User	Bank Account	Identificador da conta bancária
User	Mobile Money Account	Identificador da conta de *mobile money*

Tabela 6 - Definição das colunas que constituem a entidade Stellar Account (fig. 30) da base de dados.

Entidade	Variável	Significado
Stellar Account	Account Id	Identificador da carteira digital
Stellar Account	Created At	Data de criação da carteira digital
Stellar Account	Secret Key	Chave privada da carteira digital
Stellar Account	Public Key	Chave pública da carteira digital
Stellar Account	User Email	Endereço do correio eletrónico do detentor da carteira

Tabela 7 - Definição das colunas que constituem a entidade Transaction (fig. 30) da base de dados.

Entidade	Variável	Significado
Transaction	Id	Identificador da transação
Transaction	Amount Sent	Montante enviado
Transaction	Currency Sent	Moeda utilizada para pagamento da transferência
Transaction	Amount Received	Montante recebido
Transaction	Currency Received	Moeda recebida pelo recetor
Transaction	Fee	Taxas associadas à transação
Transaction	Transaction Date	Data de envio da transação
Transaction	Receiver Name	Pseudónimo do recetor da transação
Transaction	Receiver Wallet Address	Endereço da carteira digital do recetor
Transaction	State	Estado da transação (sucesso ou descrição do erro)
Transaction	User Email	Endereço do correio eletrónico do emissor da transação

4.4 Implementação do Protótipo

Com a arquitetura do sistema definida e a base de dados esquematizada e validada foi possível iniciar a fase de implementação do protótipo.

Numa fase inicial, foi utilizado o programa PostMan para validar de uma forma ágil os endpoints dos controladores que expunham a lógica. Na figura 32, pode ver-se à esquerda um objeto JSON que contém as credenciais a serem enviadas através do método POST para o endpoint de login. Depois de processado, o sistema responde com um novo objeto JSON que contém o resultado do pedido e a descrição do erro (parte direita da figura). Desta forma foi possível confirmar que o comportamento do sistema era o esperado face a um pedido com credenciais sem correspondência na base de dados.

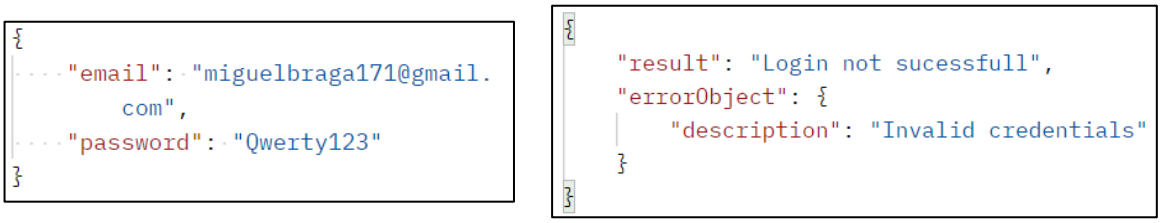


Figura 32 - Pedido e resposta à operação de login de utilizador (formato JSON).

Depois de desenvolvidas algumas das componentes funcionais, iniciou-se o desenvolvimento do front-end do protótipo com uso do processador de template[35] Thymeleaf. Através deste desenvolvimento paralelo com o das componentes de serviços e controladores foi possível compreender melhor o fluxo a partir de uma visão mais próxima do utilizador final e detetar erros e lacunas. Foram então priorizadas inicialmente as funcionalidades base (transferência de fundos, saldo de conta, gestão da informação da carteira digital) e por isso o aspeto visual do protótipo desenvolvido era rudimentar.

Na figura 33, pode ver-se o ecrã de *homepage* desenvolvido em thymeleaf para realizar testes ao protótipo de uma forma rápida e que permitisse averiguar a funcionalidade de diferentes endpoints do sistema. Ao utilizador são apresentadas as diferentes operações possíveis (2), conseguindo adicionalmente visualizar o saldo atual que a carteira digital possui para os diferentes tipos de criptomoedas (1).

[35] Processador de template – Software desenhado para combinar templates com modelos de dados de forma a produzir documentos [162].

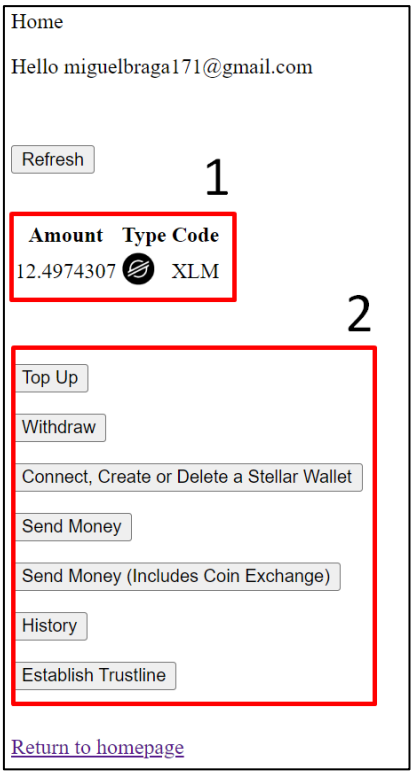


Figura 33 - Ecrã de homepage do protótipo desenvolvido em thymeleaf.

Com todas as componentes fundamentais para o estágio desenvolvidas (transferência direta, transferência com conversão, levantamento e gestão da carteira digital) para a rede de teste da Stellar, foi priorizado melhorar a experiência do utilizador final através de uma interface que seguisse as normas da WIT. Para tal, foi criado (com a ajuda da analista de negócios) um documento (em anexo no segundo apêndice) que descrevesse o design pretendido através de uma lista de *features*. Este documento foi enviado à equipa de designers da WIT que após uma reunião (onde foram explicadas as funcionalidades base do protótipo) entregaram os *mockups*[36] através do programa Figma que serviram como base de referência para a implementação do front-end em React.js.

Na figura 34, pode ver-se alguns dos ecrãs que fazem parte dos mockups entregues pela equipa de design da WIT de forma a guiar o desenvolvimento das componentes de front-end do protótipo. Alguns ecrãs (ex: relacionado com a gestão da carteira digital) não foram criados nos mockups e por isso responsabilizei-me pela sua criação. Na implementação foi sempre procurado manter a coerência visual do resto para os ecrãs que não tinham mockups de referência.

[36] Mockup – Design estático de uma web page ou de uma aplicação de modo a apresentar um esquema (não funcional) final com todos os elementos gráficos presentes [163].

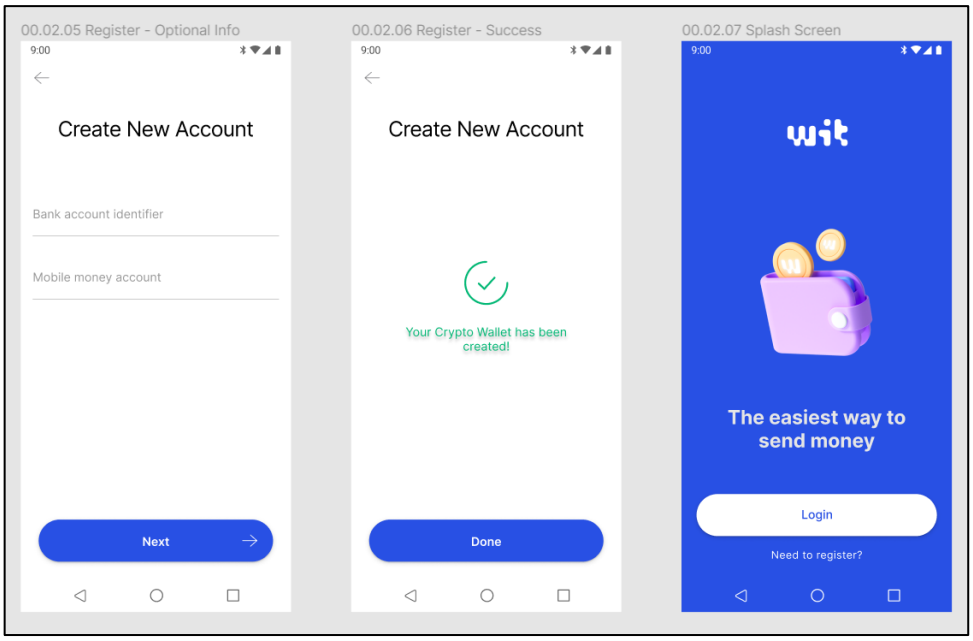


Figura 34 - Alguns ecrãs pertencentes aos mockups desenvolvidos pela equipa de design da WIT para o protótipo.

Na figura 35, pode ver-se as diferenças entre o *front-end* (para o mesmo ecrã) que estava inicialmente desenvolvido em Thymeleaf para o *front-end* final desenvolvido em React.js. Para além da experiência para o utilizador ter sido melhorada, a aplicação web é agora responsiva (alterações na dimensão do dispositivo originam uma reorganização dos componentes).

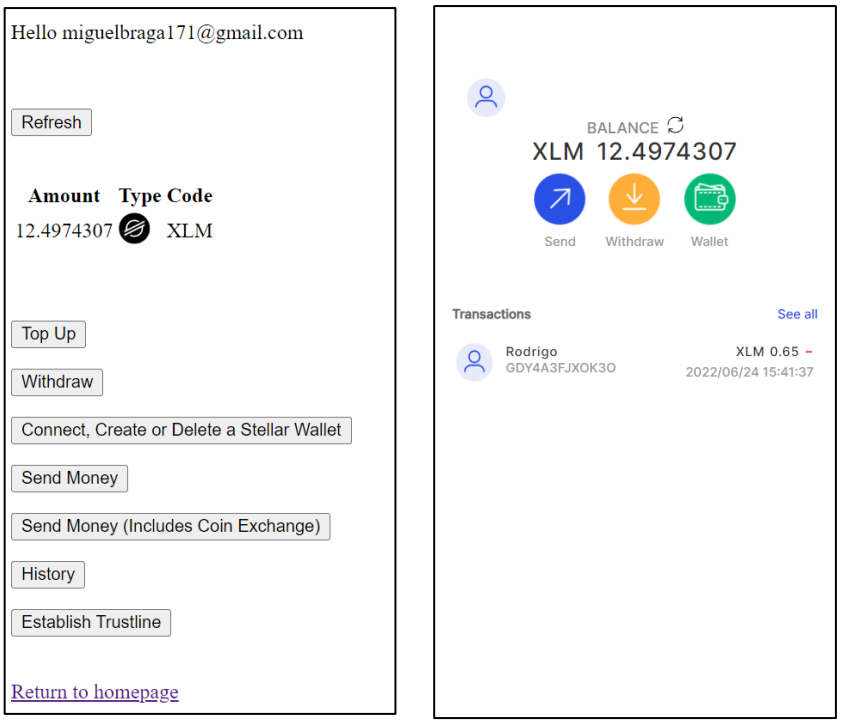


Figura 35 - Diferença entre o front-end inicialmente implementado (esquerda) em Thymeleaf e o implementado em React.js (direita).

Relativamente ao *back-end* do protótipo, foi desenvolvida uma API com quinze endpoints no controlador que utilizam a lógica dos serviços para expor todas as funcionalidades de forma a responder a pedidos criados no *front-end* (Especificação de cada um dos endpoints em anexo no quarto apêndice):

1. **/login** – Recebe um objeto com as credenciais de um utilizador e confirma se existe uma correspondência na base de dados.

2. **/register** – Recebe um objeto com toda a informação pessoal de um utilizador (incluindo credenciais), valida os valores inseridos e caso não exista um duplicado na base de dados, persiste a nova conta.

3. **/home** – Recebe um objeto com as credenciais (de forma a autenticar o utilizador) e devolve um objeto que contém uma lista com os montantes para os diferentes fundos na carteira digital.

4. **/history** – Recebe as credenciais e devolve uma lista de todas as transações que envolvem o utilizador.

5. **/walletData** – Recebe as credenciais e devolve os detalhes da carteira digital.

6. **/assetsToWithdraw** – Recebe as credenciais e devolve uma lista dos ativos ao utilizador dos quais o consegue realizar um levantamento para uma conta bancária ou de *mobile money*.

7. **/fetchAnchorInfo** – Recebe um objeto com o ativo que se pretende realizar um levantamento e devolve informação essencial (ex: endpoints) do *anchor* que representa a entidade que realizará a operação.

8. **/submitWithdrawRequest** – Recebe um objeto com a informação obtida pelo */fetchAnchorInfo* mais alguns detalhes da transação (ex: montante a enviar e endereço da carteira do recetor) e submete para a rede Stellar o pedido de levantamento.

9. **/createWallet** – Recebe as credenciais e cria a partir do SDK da Stellar uma nova carteira digital para o utilizador.

10. **/deleteWallet** – Recebe as credenciais e desassocia no sistema a carteira digital com o utilizador.

11. **/connectWallet** – Recebe as credenciais e uma chave privada de uma carteira digital já existente na rede Stellar e associa-a ao utilizador.

12. **/fetchDirectSendCost** – Recebe um pedido de transferência direta entre duas carteiras digitais e envia o pedido para a rede Stellar de forma a devolver o custo total da operação.

13. **/establishTrustline** – Recebe um ativo que o utilizador pretende confiar e estabelece através da rede Stellar uma ligação de confiança com esse ativo (*trustline*).

14. **/fetchPathSendCost** – Recebe um pedido de transferência com conversão de moeda entre duas carteiras digitais e envia o pedido para a rede Stellar de forma a devolver o custo total da operação.

15. **/sendPathTransaction** – Recebe um pedido de transferência e submete-o à rede, retornando a mensagem de resposta da operação ao utilizador e em caso de sucesso, persiste toda a informação na base de dados.

Nas próximas páginas, seguem-se duas figuras (fig. 36 e fig. 37) que procuram respetivamente esquematizar o funcionamento da aplicação para duas operações exemplo através de duas perspetivas diferentes. Com a primeira é possível visualizar as interações das componentes da arquitetura de uma forma mais superficial para uma transferência com conversão. A segunda figura apresenta os passos internos que ocorrem para uma operação de transferência direta.

Na figura 36 pode ver-se um dos diagramas de sequência criados para esquematizar a lógica subjacente ao funcionamento do protótipo (os restantes encontram-se em anexo no documento de especificação de endpoints). Neste caso, encontra-se representado o diagrama para a operação de transferência entre contas (com conversão da moeda enviada).

A sequência ocorre na seguinte ordem:

- Preenchimento e submissão de um formulário pelo utilizador onde lhe é pedido que insira os valores: montante a enviar, moeda escolhida para realizar o pagamento da transação, moeda destino e endereço da carteira digital do recetor.

- Através do *front-end* é gerado um pedido HTTP com headers e payload JSON composto pelos valores preenchidos e enviado para o endpoint */sendPathTransaction (Back-end)*.

- É realizada uma validação inicial de forma a garantir que não se encontram presentes valores nulos ou inválidos. Caso o formulário esteja nos conformes, o processo de transferência continua e são enviados vários pedidos à rede Stellar de forma a validar os valores no formulário (ex: fundos suficientes presentes na conta, existência ou não do endereço do recetor).

- Caso todas as condições sejam válidas, um pedido final é realizado à rede Stellar para obter o custo da operação. O custo é depois enviado ao *front-end* que o apresenta ao utilizador.

- Com esta informação, o utilizador pode ou não confirmar o pedido. Caso confirme, o *back-end* do sistema constrói a transação, submete na rede Stellar e os dados relativos à mesma são persistidos na base de dados.

- No final, o utilizador é informado do sucesso da operação.

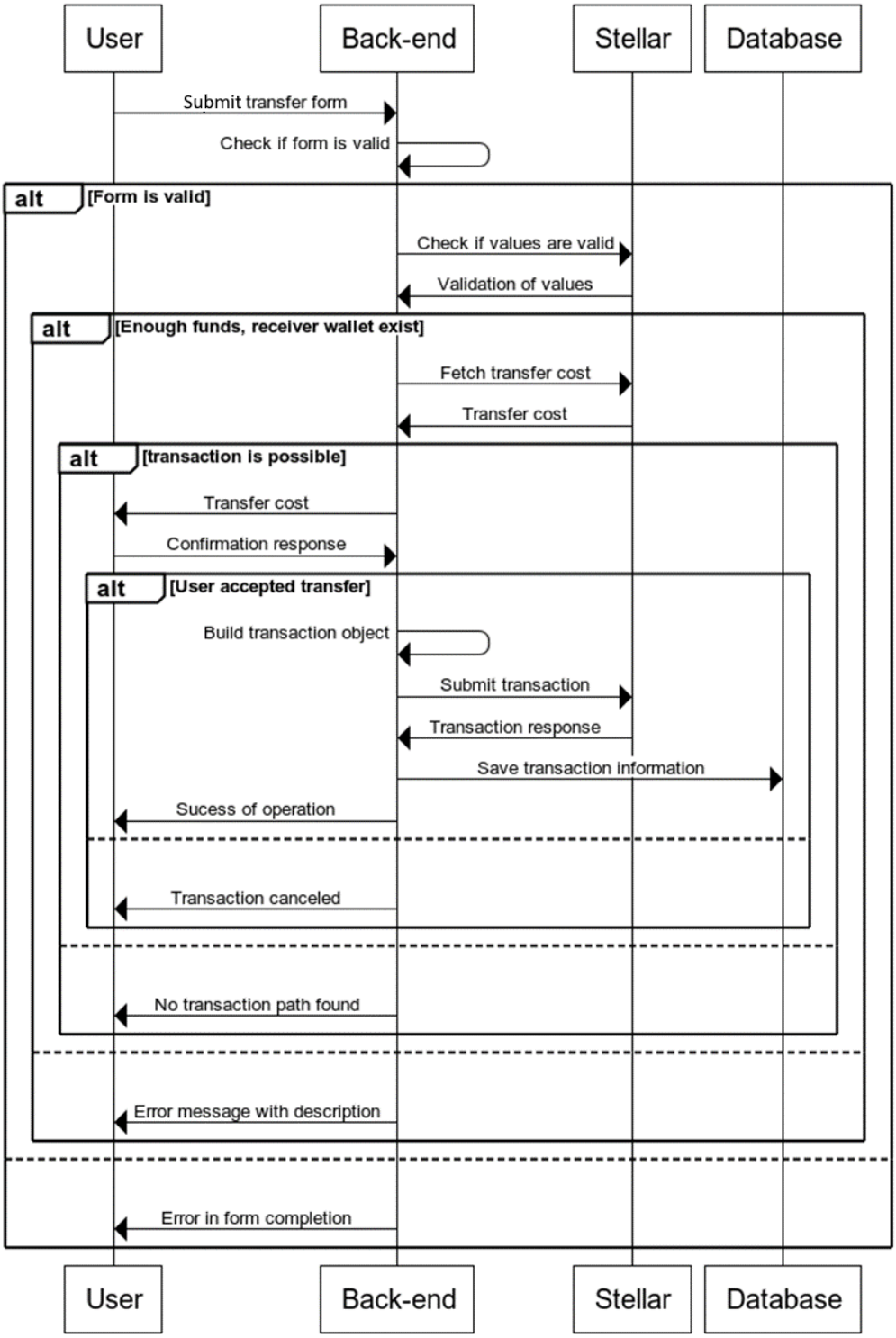


Figura 36 - Diagrama de sequência para uma transação com conversão de moeda.

Na figura 37, pode ver-se a esquematização de todo o processo que ocorre no sistema face ao pedido do utilizador para visualizar os custos totais de uma operação de transferência direta de fundos (sem conversão de moeda). Foi selecionada a interação com este endpoint pela simplicidade na forma como pode ser interpretada e na maneira como é uma representação concreta dos diferentes passos executados pelos diferentes componentes da solução em resposta a um pedido.

O processo ocorre na seguinte ordem:

- O utilizador preenche um formulário com os dados para concretizar a transferência (**passo 1**).

- Submete o formulário e um objeto JSON do tipo *PathTransactionRequest*[37] é gerado e enviado para o endpoint do controlador */fetchDirectSendCost* (**passo 2**).

- O endpoint executa a função *fetchDirectSendCost* dos serviços que irá atribuir o custo à transação (**passo 3**). No entanto, antes da atribuição de custo é necessário validar as variáveis do objeto *PathTransactionRequest*.

- Deste modo, é executado internamente a função *validateTransaction* (**passo 4**) que através do SDK valida (**passo 5**) a legitimidade da criptomoeda a enviar, a existência da carteira digital do recetor e o saldo da conta do emissor. Estes múltiplos pedidos são assim enviados para a rede Stellar (**passo 6**).

- A rede Stellar gera uma resposta (**passo 7**) onde valida os diferentes valores. Esta validação é devolvida à função *fetchDirectSendCost* localizada nos serviços (**passos 8 e 9**) que no caso da não existência de erros, calcula o custo total e devolve um objeto do tipo *PathTransactionRequest* (**passo 10**) com este valor associado ao controlador.

- No final, o objeto é interpretado pelo *front-end* e desta forma apresentado ao utilizador (**passo 11**).

[37] Objeto PathTransactionRequest – Contém o email do emissor, endereço da carteira do recetor, criptomoeda a enviar, quantidade a enviar e a alcunha do recetor.

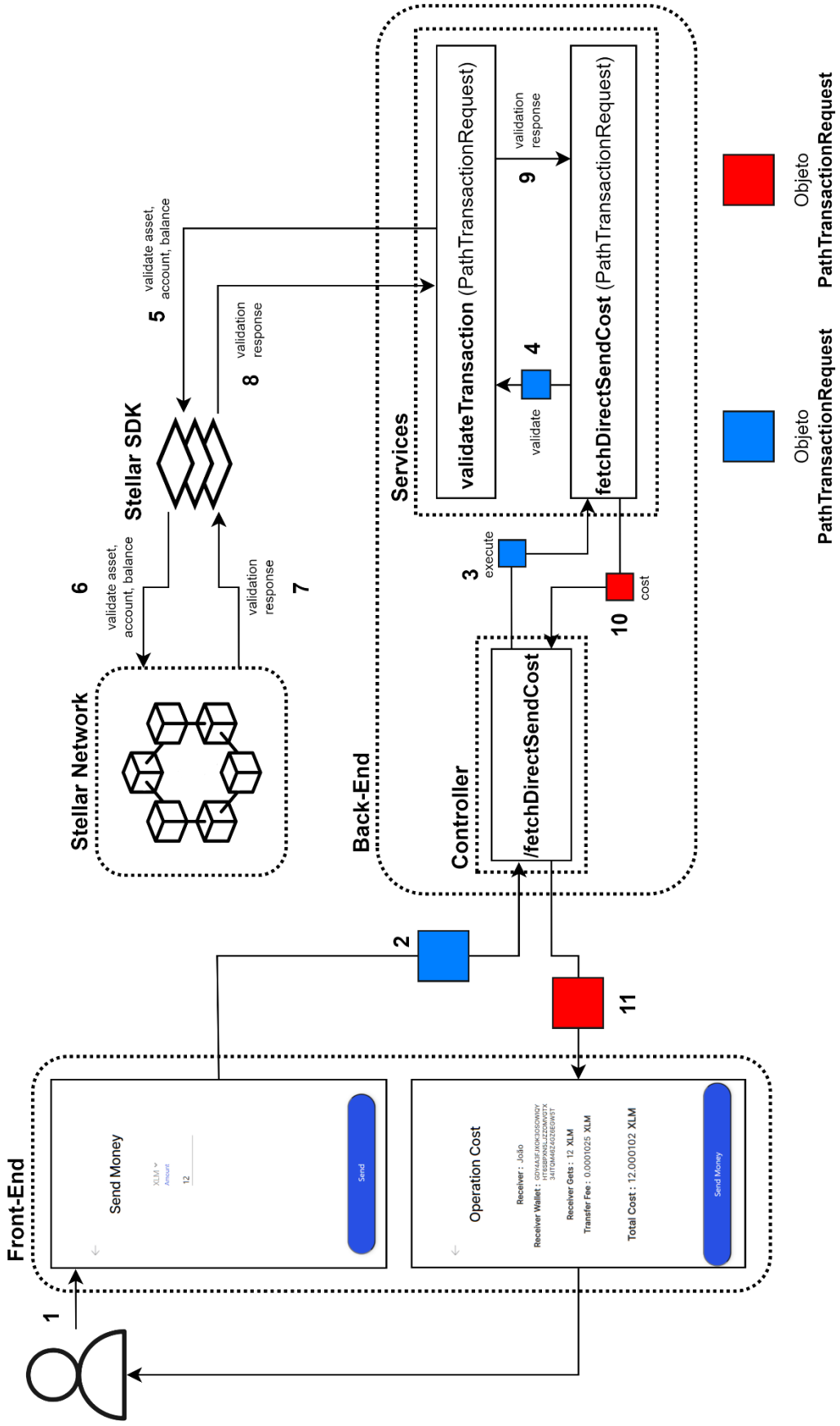


Figura 37 - Esquematização da interação com um endpoint do protótipo, neste caso o de obter o custo de uma transação direta.

4.5 Análise de Resultados

Os objetivos do estágio consistiam no desenvolvimento de uma solução protótipo para utilizadores na Tanzânia que proporcionasse um serviço de transferências internacionais de dinheiro (inserido na atividade de remessas internacionais) de forma mais económica e intuitiva. Com a solução desenvolvida e a estrutura analisada em secções anteriores, é necessário (através desta subsecção) analisar a viabilidade económica da solução para o mercado da Tanzânia.

Antes de uma análise comparativa face aos custos atuais do mercado, é necessário definir e repartir o processo de transferência em três passos fundamentais que totalizam no custo final para o utilizador: **depósito**, **transferência** e **levantamento**.

Na figura 38, pode ver-se a ordem em que ocorrem estes três passos e a forma como são essenciais para o sucesso da transferência. O **depósito** refere-se à transformação do dinheiro físico na sua representação digital numa conta bancária, trata-se de uma receção de fundos. A **transferência** refere-se ao movimento e conversão dos fundos entre a conta do emissor e recetor. O **levantamento** refere-se à transformação do dinheiro digital que se encontra na conta em dinheiro físico, ou seja, extrair dinheiro em numerário.

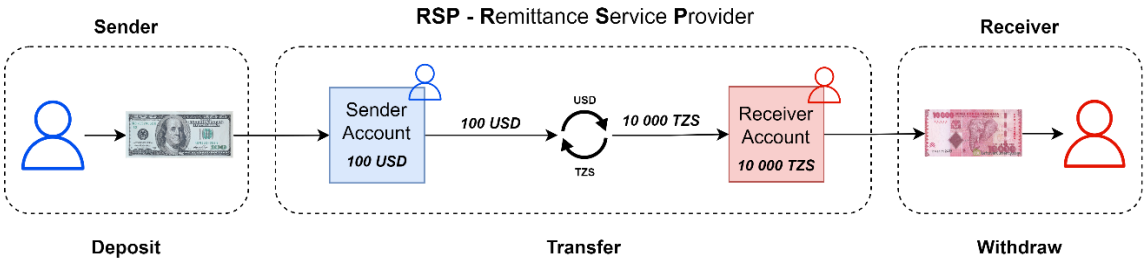


Figura 38 - Representação dos três principais passos envolvidos numa transferência no âmbito do estágio.

Uma análise a trezentos e cinquenta e quatro corredores[38] para o envio de remessas internacionais no primeiro trimestre de 2022, concluiu sobre a existência de dois montantes mais significativos enviados: **duzentos** dólares e **quinhentos** dólares. A significância destes valores tem por base a consideração por parte do *World Bank* (constituído por 189 países membro) como os valores que melhor representam o montante típico enviado numa remessa [4].

A média global do custo para o envio de duzentos dólares situa-se nos **6.09%**, enquanto para um montante no valor de quinhentos dólares, o custo associado é de **4.09%** (primeiro trimestre de 2022) [4]. A solução desenvolvida só apresenta viabilidade económica se o custo total associado (*Depósito + Transferência + Levantamento*) for inferior em pelo menos um destes montantes mais significativos.

[38] Corredor - Neste contexto, refere-se a um grupo de países emissor-recetor específico numa transferência monetária.

4.5.1 Custo de Depósito

De forma aumentar os fundos de uma conta no protótipo é necessário adquirir a criptomoeda nativa da rede Stellar (XLM) e garantir que é depositada no endereço da carteira digital associada. Para tal, são utilizados os serviços fornecidos por empresas de câmbio de criptomoedas. O processo de depósito divide-se assim em duas etapas fundamentais: **compra de XLM** e **envio para a wallet**.

Na figura 39, pode ver-se respetivamente, as duas etapas envolvidas no depósito através da empresa de câmbio Coinbase. De notar que neste caso, a compra de criptomoedas apresenta um custo associado (3.84 euros), mas o envio das mesmas para a carteira digital não (0.0 XLM).

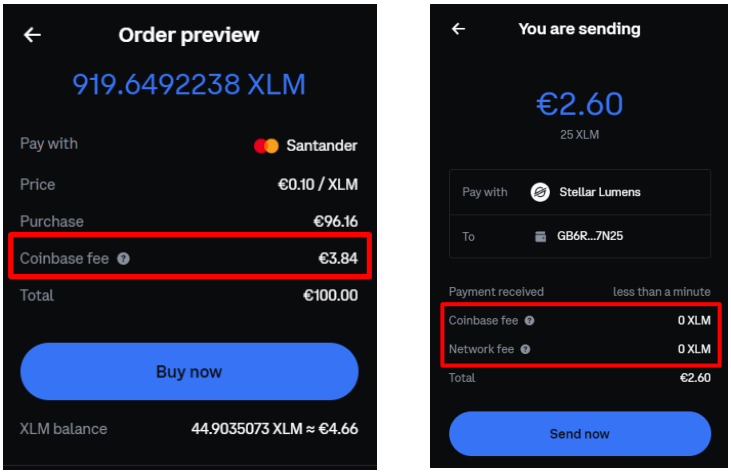


Figura 39 - Capturas de ecrã para as duas etapas envolvidas no deposito através da Coinbase.

Na tabela 8, pode ver-se os custos associados à compra e envio de XLM para a carteira digital do utilizador para as empresas de câmbio mais populares [140]. Verifica-se que o custo percentual varia bastante e torna-se essencial selecionar a empresa que fornece o serviço ao custo mais baixo. Na figura 40, pode ver-se uma outra representação dos dados. Verifica-se tanto na tabela como na figura os benefícios de utilizar os serviços da Binance na compra e envio de XLM para a carteira digital.

Tabela 8 - Comparação dos custos das empresas de câmbio mais populares na compra e envio de XLM para a carteira digital na solução.

Empresa de Câmbio	Montante Enviado (dólar)	Compra de XLM (dólar)	Envio para Wallet (dólar)	Custo Total (dólar)	Custo Total (%)
Coinbase	200	7.62	0.0	7.62	**3.81**
	500	19.05	0.0	19.05	**3.81**
Binance	200	2.25	0.002	2.252	**1.13**
	500	7.00	0.002	7.002	**1.4**
Kraken	200	10.59	0.001	10.591	**5.29**
	500	26.11	0.001	26.111	**5.22**

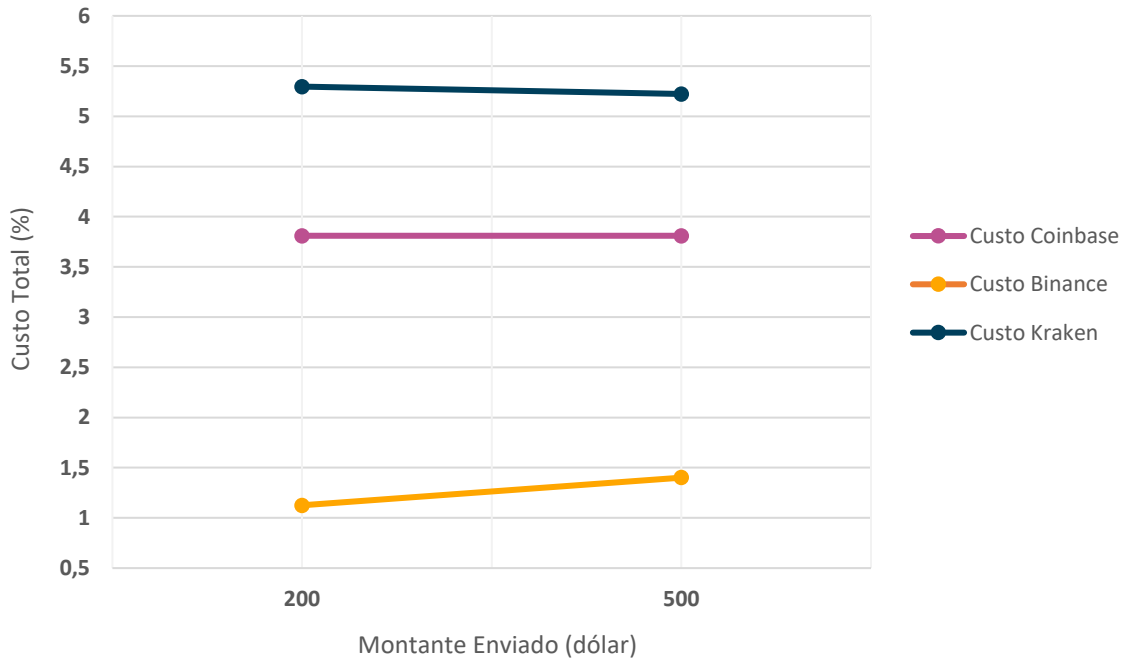


Figura 40 - Gráfico comparativo dos custos percentuais dos diferentes montantes enviados para as três empresas de câmbio mais populares.

4.5.2 Custo de Transferência

Depois de garantir que a carteira dentro da solução possui fundos ao menor custo possível, é necessário concretizar o próximo passo, a transferência entre contas. Neste passo, considerando o âmbito da solução, existem dois tipos de custos que totalizam no custo total de transferência: **custo de conversão** e **taxa de transação da rede**.

Na figura 41, pode respetivamente ver-se o rácio de conversão entre criptomoedas dentro de rede Stellar que ocorre quando uma operação de transação com conversão é realizada. Para 1964.7 XLM (equivalente a 200 dólares) o mercado da rede converte com uma perda de 0.2%[39].

À direita encontra-se representado parte do código presente no ficheiro *application.properties* que contém uma definição da taxa base máxima que a solução permite o utilizador pagar em *stroops*[40]. Numa transação direta o valor é o dobro da base definida (2050 *Stroops*, equivalente a 0.0205 XLM ou 0.0021 dólares), enquanto numa transação com conversão é o triplo (3075 Stroops, equivalente a 0.03075 XLM ou 0.0031 dólares).

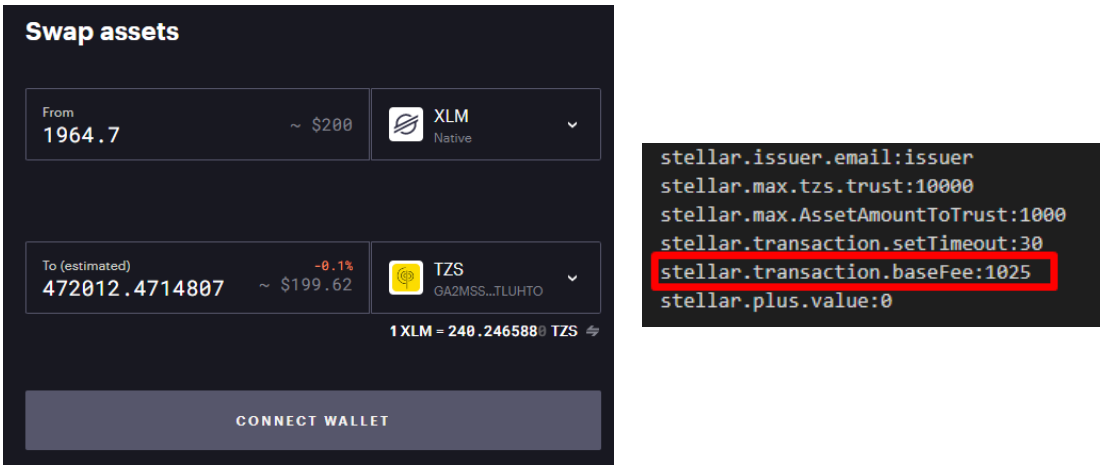


Figura 41 – À direita rácio de conversão de XLM pelo token de Xelim Tanzaniano no simulador da Stellar X [141]. À esquerda o valor da variável de propriedades global da solução que dita a taxa associada.

Na tabela 9, pode ver-se os custos associados à transferência de fundos entre contas com conversão da criptomoeda nativa da rede (XLM) para o token TZS (Xelim tanzaniano). Verifica-se que o custo total percentual para o valor de montante enviado varia em apenas 0.01307%, sendo ligeiramente superior para o montante de 500 dólares enviados. Este aumento deve-se essencialmente ao livro de ordens da rede Stellar (analisado na subsecção 3.2.2). A figura 42 pretende representar visualmente os dados relativos à tabela num gráfico de modo a facilitar a interpretação.

[39] A figura 37 apresenta uma perda percentual de 0.1% quando na realidade é uma perda de 0.19%, resultado da operação: *1 – (199.62 / 200.0) * 100.*

[40] Stroops – Unidade que representa 0.00001 XLM na rede Stellar, ou seja, 0.000001 dólares.

Tabela 9 – Custo de conversão e transação na rede de acordo com o montante enviado.

Montante Enviado (dólar)	Custo de conversão (dólar)	Custo de transação (dólar)	Custo Total (dólar)	Custo Total (%)
200	0,92	0,0031	0,9231	**0,46155**
500	2,37	0,0031	2,3731	**0,47462**

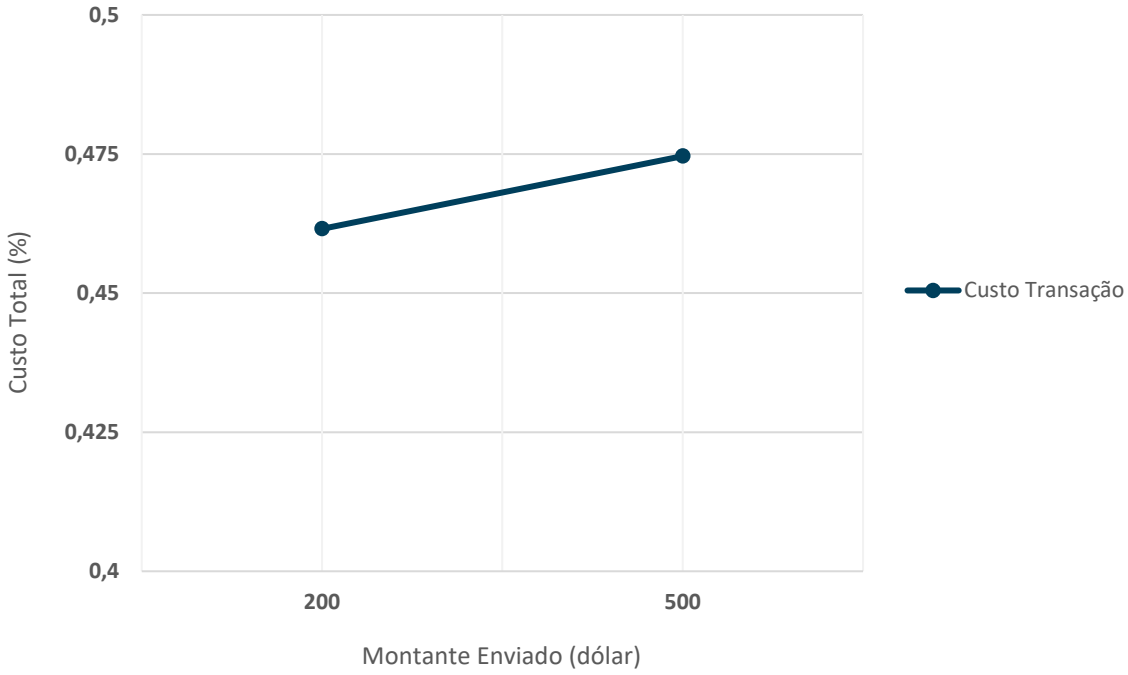


Figura 42 – Gráfico com o custo total percentual face ao montante enviado em dólar.

4.5.3 Custo de Levantamento

Inserindo-se num dos objetivos principais da solução é necessário garantir que o Xelim Tanzaniano (TZS) presente na conta do recetor pode ser transferido para uma conta bancária ou de *mobile money*. Para isto, existe na rede Stellar um único Anchor (definição na subsecção 3.2.2), sobre o controlo da empresa tanzaniana ClickPesa, que converte os tokens que representam TZS na moeda correspondente. Para análise do custo de levantamento existe esta limitação na oferta do serviço.

Neste último passo estão incluídos dois custos**: custo de transferência** entre a conta com os fundos e a conta da entidade da ClickPesa que irá realizar a conversão para a conta bancária e/ou de *mobile money* e ainda o custo relacionado com a **taxa do serviço**.

Na tabela 10, pode ver-se uma comparação dos custos associados ao levantamento de fundos pelo serviço fornecido pela ClickPesa de acordo com o montante e método selecionado para realizar a operação. Verifica-se um benefício de custo ao utilizar o método ACH para uma conta bancária, no entanto, é relevante relembrar que na Tanzânia existe uma falta de acesso a infraestrutura bancária e por isso o método mais comum é o levantamento para uma conta de *mobile money*. A figura 43 pretende representar visualmente os dados relativos à tabela num gráfico de modo a facilitar a interpretação.

Considerações Adicionais

A operação de levantamento foi implementada com sucesso na solução enquanto operava sobre a rede de testes da Stellar. Posteriormente foi realizada a migração para a rede real e requerido à empresa acolhedora do estágio dados bancários reais da Tanzânia de modo a testar a funcionalidade. No entanto, verificou-se que os serviços relacionados com o token TZS (xelim tanzaniano) da entidade ClickPesa se encontravam em manutenção. Os serviços mantiveram-se inoperacionais até à data atual (agosto de 2022) o que impediu que fosse realizado um levantamento na rede real. Os valores apresentados na tabela foram obtidos através de uma tabela de custos fornecida pela empresa ClickPesa que resultou de uma comunicação direta que ocorreu via e-mail entre o autor e a entidade (em anexo, no sexto apêndice).

Tabela 10 - Comparação dos custos totais para o levantamento do token TZS (Xelim Tanzaniano) através do serviço fornecido pela ClickPesa.

Método de Levantamento	Montante Enviado (dólar)	Custo de Transferência (dólar)	Taxa do Serviço (dólar)	Custo Total (dólar)	Custo Total (%)
Conta de Mobile Money	200	0.001	4.59	4.591	**2.2955**
	500	0.001	5.36	5.361	**1.0722**
Conta Bancária (ACH[41])	200	0.001	2.15	2.151	**1.0755**
	500	0.001	2.15	2.151	**0.4302**
Conta Bancária (RTGS[42])	200	0.001	8.58	8.581	**4.2905**
	500	0.001	8.58	8.581	**1.7162**

[41] Automated Clearing House (ACH) – Rede para transferência de fundos (maior detalhe na subsecção 2.1.1).

[42] Real-Time Gross Settlement (RTGS) – Sistema continuo de transferência de fundos. O processamento da operação ocorre quando é recebido [164].

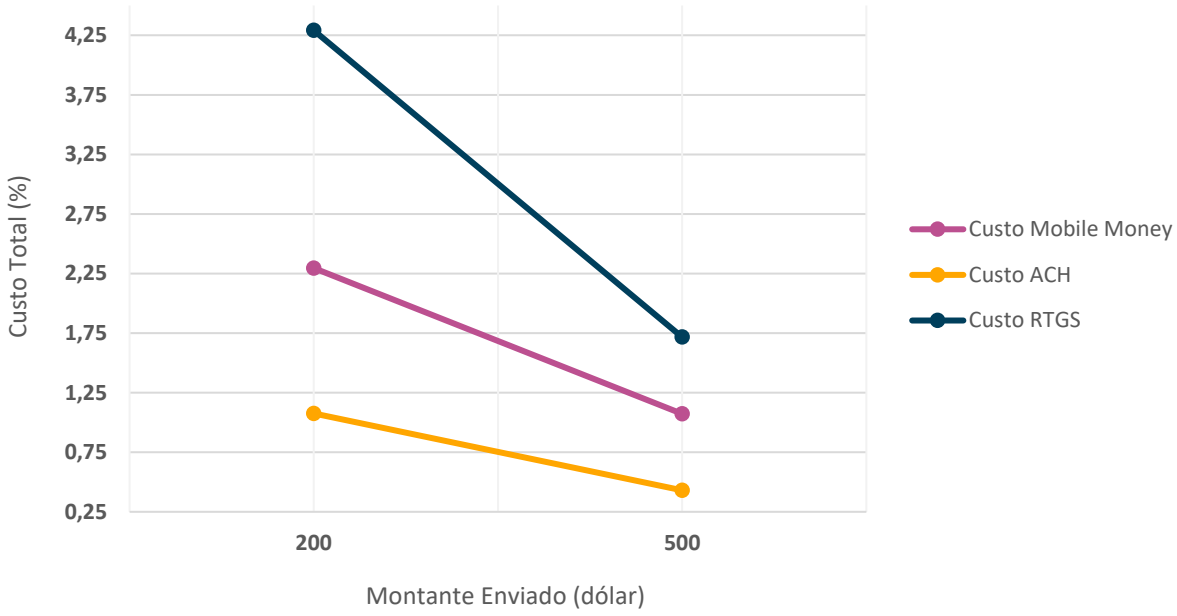


Figura 43 - Gráfico representativo da diferença dos custos de levantamento em relação ao montante enviado e ao método escolhido.

4.5.4 Custo Final da Solução

Após uma análise aos custos de cada componente (depósito, transferência e levantamento) que constitui o custo total da solução, torna-se possível prosseguir com uma análise final de custo onde se procura a melhor combinação de forma a obter a maior viabilidade económica.

Na tabela 11, pode ver-se numa única tabela, todas as combinações de todas as variáveis envolvidas no processo de envio de remessa através da solução criada. Na figura 40, estes dados encontram-se representados de uma forma simplificada para facilitar a interpretação. De notar que existe uma consideração adicional pelo método de levantamento ser para uma conta de *mobile money*, a isto deve-se o facto da sua popularidade na Tanzânia, contando atualmente com 35.7 milhões de contas registadas [142] de um total de população de 63.7 milhões [143]. De tal modo, deve assim ser o único método considerado relevante para a análise final de custo e por isso a sua distinção de cores tanto na tabela 9, como na figura 44.

Verifica-se que de entre os dados apresentados, o custo percentual mais baixo face aos montantes mais frequentes para a atividade das remessas (200 e 500 dólares) é originado através de um depósito feito pela Binance, apresentando respetivamente o custo total de **3.882776%** e **2.947572%.**

Tabela 11 - Comparação dos custos totais da solução com base nas diferentes combinações possíveis em cada componente.

Método de Levantamento	Empresa de Câmbio	Montante Enviado	Custo Depósito	Custo Transferência	Custo Levantamento	Custo Total	Custo Total (%)
Mobile Money	Coinbase	200	7,62	0,9231	4,591	13,1341	**6,56705**
		500	19,05	2,3731	5,361	26,7841	**5,35682**
	Binance	200	2,251451	0,9231	4,591	7,765551	**3,882776**
		500	7,003761	2,3731	5,361	14,73786	**2,947572**
	Kraken	200	10,59101	0,9231	4,591	16,10511	**8,052555**
		500	26,11101	2,3731	5,361	33,84511	**6,769022**
Local Bank Transfer (ACH)	Coinbase	200	7,62	0,9231	2,151	10,6941	**5,34705**
		500	19,05	2,3731	2,151	23,5741	**4,71482**
	Binance	200	2,251451	0,9231	2,151	5,325551	**2,662776**
		500	7,003761	2,3731	2,151	11,52786	**2,305572**
	Kraken	200	10,59101	0,9231	2,151	13,66511	**6,832555**
		500	26,11101	2,3731	2,151	30,63511	**6,127022**
Local Bank Transfer (RTGS)	Coinbase	200	7,62	0,9231	8,581	17,1241	**8,56205**
		500	19,05	2,3731	8,581	30,0041	**6,00082**
	Binance	200	2,251451	0,9231	8,581	11,75555	**5,877776**
		500	7,003761	2,3731	8,581	17,95786	**3,591572**
	Kraken	200	10,59101	0,9231	8,581	20,09511	**10,04756**
		500	26,11101	2,3731	8,581	37,06511	**7,413022**
	Média de Mercado	200	-	-	-	-	**6,09**
		500	-	-	-	-	**4,09**

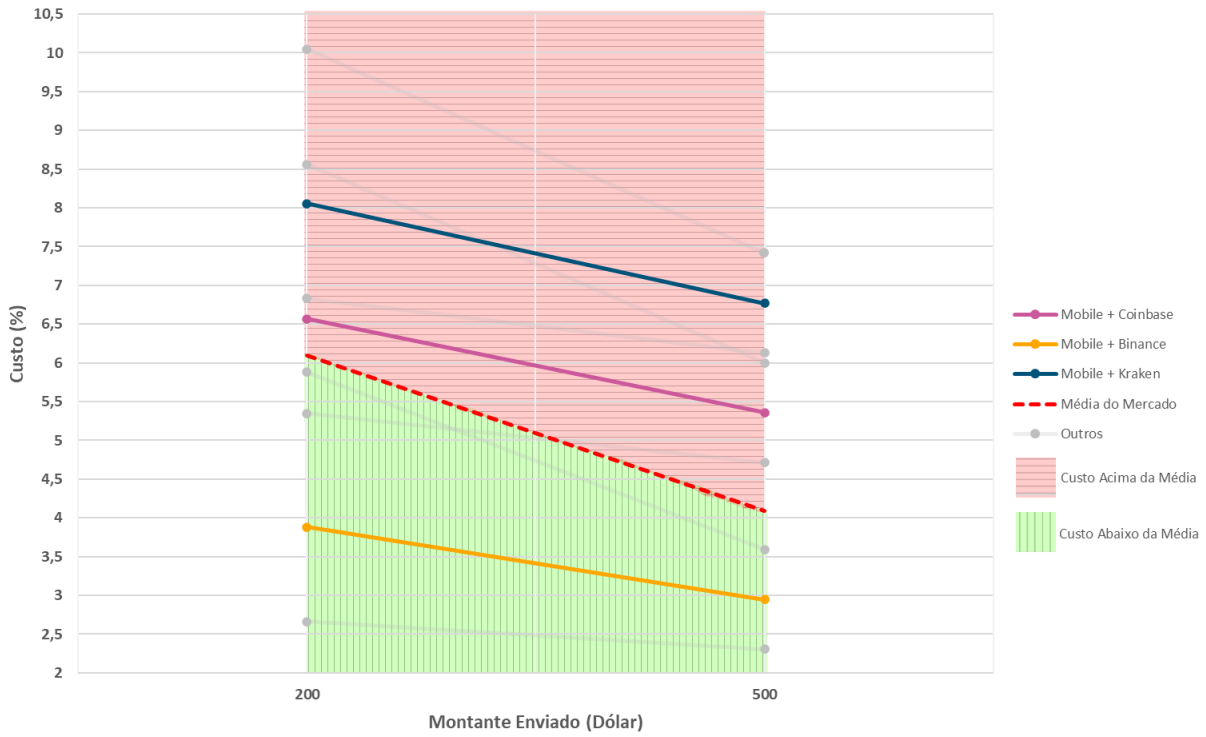


Figura 44 - Gráfico com os diferentes custos percentuais com base nas diferentes combinações possíveis em cada componente.

Capítulo 5
Planeamento

Esta secção pretende apresentar de uma forma resumida as ferramentas e metodologias usadas para gerir o projeto. Para além disso, será ainda apresentado o planeamento das tarefas criado para o primeiro e para o segundo semestre de estágio com as devidas divergências entre o planeado e o executado justificadas. Maior detalhe pode ser encontrado em anexo no primeiro apêndice.

No primeiro semestre era esperado uma carga de esforço semanal equivalente a 16 horas. A decisão foi tomada pelo autor e pela empresa que acolheu o estágio tendo em consideração as recomendações do Departamento de Engenharia Informática para esta unidade curricular. No segundo semestre, era esperada uma carga de esforço semanal equivalente a 40 horas. O regime de trabalho era de livre escolha do autor, sendo que foi tomado um regime mais presencial ao deslocar-se à empresa em Coimbra, pelo menos 2 vezes por semana e nos restantes dias ao Departamento de Engenharia Informática (DEI).

5.1 Primeiro Semestre

O primeiro semestre iniciou a 20 de setembro de 2021 e terminou no dia de entrega do relatório intermédio, a 17 de janeiro de 2022. Dado que, em simultâneo com a dissertação/estágio ainda existia a carga de esforço proveniente de outras 3 unidades curriculares, os objetivos para este semestre seriam mais relacionados com a familiarização da tecnologia e dos conceitos relacionados com a proposta.

A comunicação com orientador, tutor e analista de negócios da empresa ocorreram maioritariamente de forma remota através de e-mail, Skype e Zoom. Semanalmente era marcada uma reunião com os mesmos de forma a validar o trabalho realizado no decorrer da semana e planear o trabalho a realizar para a semana seguinte. Mensalmente decorria ainda uma reunião entre autor, orientador da empresa e orientador do departamento de forma a validar o estado atual do trabalho, rever o planeamento e abordar outros assuntos relacionados com o estágio.

Na figura 45, pode ver-se um esquema simplificado do planeamento para o primeiro semestre. A **tarefa de contextualização** teve a duração de uma semana e serviu para compreender a proposta e ser apresentado ao contexto da empresa e funcionamento do estágio. A **tarefa de pesquisa**, com duração de quatro semanas, serviu inicialmente para interiorizar e compreender os conceitos onde a proposta assentava. Posteriormente o material era agrupado de forma a começar a escrita de capítulos para a dissertação. A **tarefa de dissertação** teve a duração de nove semanas e

encontra-se relacionada com a escrita da mesma, onde depois da conclusão de cada capítulo, o conteúdo era revisto pelo orientador. A **tarefa de requisitos** teve a duração de uma semana e foi dedicada à criação do documento de especificação dos requisitos de software. **A tarefa de arquitetura** teve a duração de uma semana e foi dedicada à criação do documento de arquitetura de software. A **tarefa de requisitos** e **arquitetura** foram tarefas essenciais para suportarem o desenvolvimento no segundo semestre. Adicionalmente, não estando representado na figura, ocorreram duas reuniões internas à empresa, onde era pedido uma apresentação com o trabalho desenvolvido no último mês e o trabalho a desenvolver no próximo semestre de forma que a empresa tivesse conhecimento do progresso do estágio (dia 24 de novembro e dia 5 de janeiro). Para maior detalhe acerca do planeamento, pode ser consultado em anexo o primeiro apêndice.

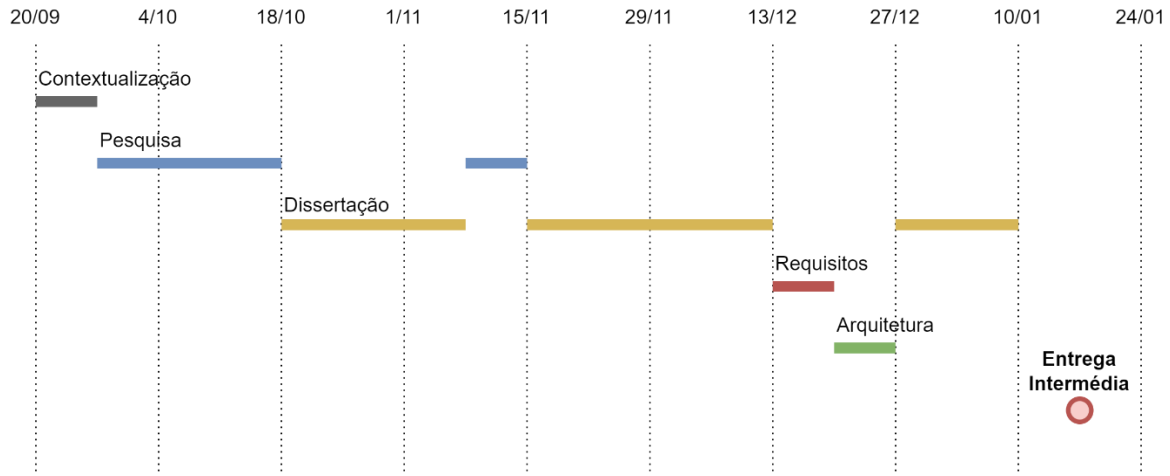


Figura 45 - Planeamento do primeiro semestre.

Plano Executado

O plano de trabalho executado no decorrer do primeiro semestre do estágio divergiu do plano originalmente criado. Na figura 46, pode ver-se que a diferença mais notável consistiu no surgimento da **tarefa de documentação**. Esta tarefa englobou a criação de um documento de *benchmark* que foi essencial na escolha da rede blockchain para construir a solução. Foi ainda criado um documento com base em experimentação na rede blockchain escolhida (Stellar) através do laboratório online de testes (*laboratory.stellar.org*) de modo a ganhar uma maior familiarização com os termos e conceitos próprios da rede. Devido a esta tarefa adicional de documentação, a tarefa de escrita do documento de requisitos e arquitetura não ficou terminada a tempo e teve de ser concluída posteriormente numa semana diferente da originalmente planeada.

Outro importante fator que influenciou na divergência que existiu entre o planeado e o executado foram as alterações que decorreram na proposta original. À medida que se obteve um conhecimento mais detalhado da tecnologia foram feitas mudanças no âmbito e nos objetivos propostos, que posteriormente foram sujeitas a

discussão e aprovação de ambos os orientadores. A proposta final foi aprovada a 21 de fevereiro de 2022 com o seguinte conteúdo escrito pelo autor:

"Desenvolver um protótipo que efetua conversão e transferência de dinheiro em cima de uma rede blockchain. Não procura entre várias redes blockchain (utiliza apenas o necessário) e as transferências internacionais ocorrem entre contas bancárias. Não depende, nem utiliza, nenhuma funcionalidade do M-Pesa. Depois de concluído, será explorado a possibilidade de outros canais de entrada/saída de dinheiro, nomeadamente contas mobile money e dinheiro físico.

***O foco será**: Transferências de EUR/USD/GBP para Tanzânia.*

Quando o protótipo estiver funcional e terminado, será analisado uma possível integração com o ambiente da M-Pesa. Adicionalmente, é importante analisar a forma de implementar noutros países em africa (ex: Congo, Quénia, ...). Indicar o que seria necessário alterar para colocar em funcionamento nesses mercados."

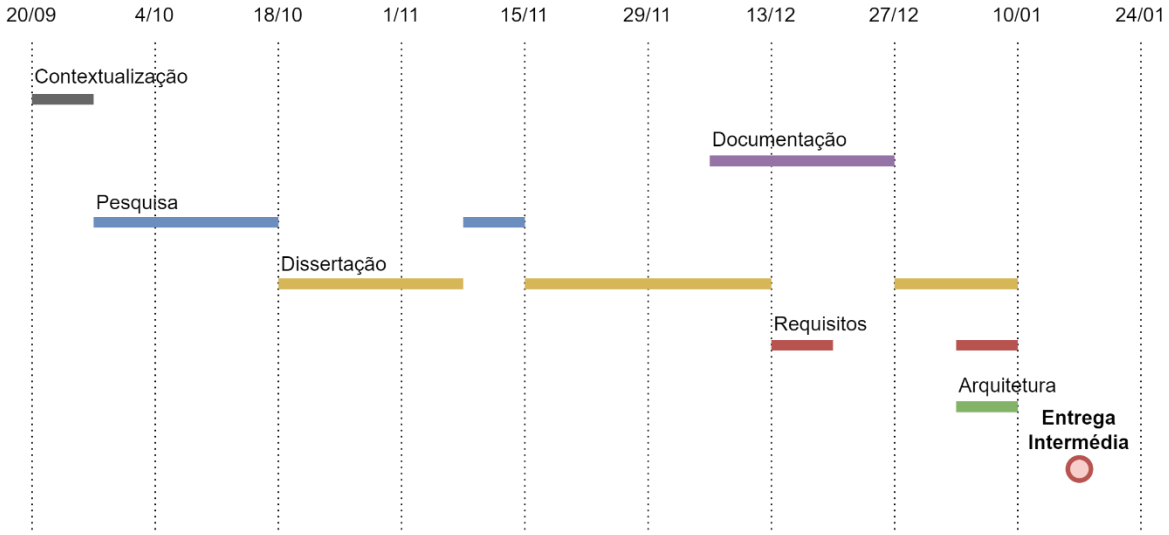


Figura 46 - Plano executado no primeiro semestre.

5.2 Segundo Semestre

O segundo semestre teve início após a defesa intermédia que ocorreu no dia 17 de fevereiro de 2022 e terminou no dia da entrega do relatório final em época especial, no dia 5 de setembro de 2022. Dado que, era a única unidade curricular do semestre a dedicação passou a ser total, com uma carga de esforço semanal de 40 horas.

A comunicação com a equipa de orientação da empresa (orientador, tutor e analista de negócios) manteve-se de forma remota através dos mesmos meios de comunicação mencionados para o primeiro semestre, sendo que esporadicamente havia discussões presenciais dado o retomar do regime presencial de trabalho. Foi seguida uma framework agile de gestão de projectos (SCRUM) onde cada sprint tinha a duração de uma semana e para gerir as tarefas utilizou-se o programa *trello* (Figura 47). Existiram reuniões diárias no início do dia com pelo menos um dos membros da equipa de orientação da empresa. Sendo que o primeiro dia da semana servia para validar o planeamento para a *sprint* e o último dia da semana servia para demonstração do trabalho realizado naquele *sprint*. A reunião mensal entre autor, orientador da empresa e orientador do departamento manteve-se.

Relativamente ao código produzido, este era guardado num repositório *git,* atualizando a versão sempre que uma funcionalidade nova e relevante fosse adicionada. Assim que uma nova versão era publicada no repositório, o tutor da empresa revia e transmitia o comentário relativo à mesma.

Na figura 47, pode ver-se a captura de ecrã do programa trello utilizado para gerir as tarefas para o *sprint*. As colunas representavam o estado onde se encontrava determinada tarefa. A coluna *backlog* representava tarefas a alocar para os *sprints*, a coluna *ready to dev* representava tarefas para o sprint a decorrer, a coluna de *in progress* representava tarefas a ser desenvolvidas e a coluna *done* representava as tarefas concluídas. Foi utilizado um esquema de *tags* com cores diferentes de forma a distinguir o sprint ao qual pertence uma tarefa e rapidamente compreender quando é que a execução de uma tarefa tinha sido prolongada para outro sprint.

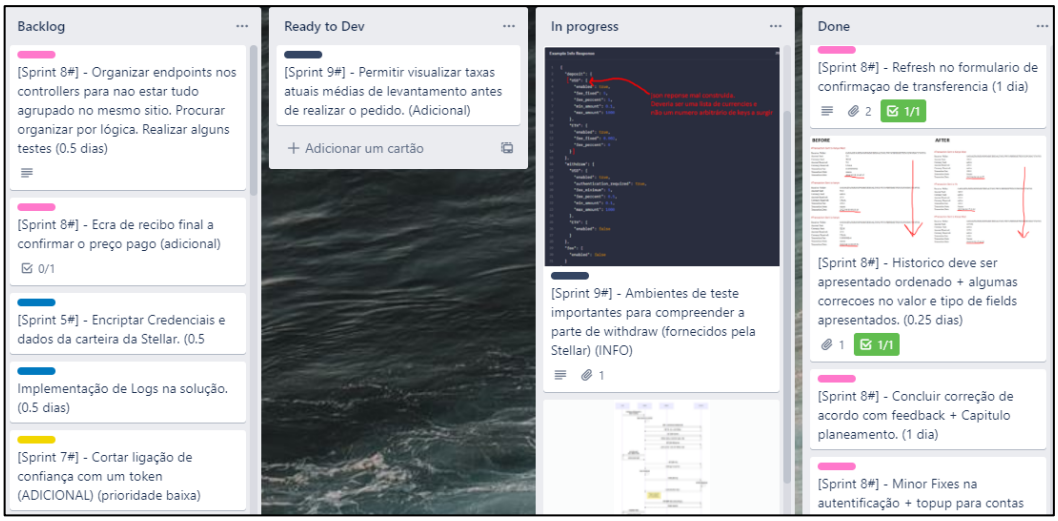


Figura 47 - Captura de ecrã do programa utilizado para gerir tarefas, trello.

Na figura 48, pode ver-se um esquema simplificado do planeamento para o segundo semestre. Apesar do segundo semestre ter começado na semana de dia 21, não se encontra representado na figura. Tratou-se de uma semana de arranque onde se refez o planeamento e se preparou todo o ambiente para o desenvolvimento. Para a **tarefa de análise e experimentação da tecnologia** planearam-se quatro semanas não consecutivas para explorar os *endpoints* da rede e realizar algumas interações fundamentais como a criação de conta, transferências com e sem conversão de moeda. A **tarefa de documentação** consistia no desenvolvimento de documentos de suporte à solução, como o refazer do documento de arquitetura e requisitos, mas também documentos como o de especificação dos *endpoints*. Para a **tarefa de desenvolvimento** estimaram-se dez semanas de trabalho. Estas semanas consistiam no desenvolvimento de toda a solução que incluía revisões de código e correções de acordo com os comentários do orientador e tutor. A **tarefa de validação** teria a duração de cinco semanas e serviria para validar componentes já desenvolvidas, realizando alguns testes unitários e de integração. A **tarefa de dissertação** consistia na escrita do documento e teria a duração total do semestre com uma dedicação mínima de 8h por semana. Adicionalmente, não estando representado na figura, ocorreram quatro reuniões internas à empresa, onde era solicitado uma apresentação com o trabalho desenvolvido no último mês e o trabalho a desenvolver de forma que a empresa tivesse algum conhecimento do progresso do estágio (dia 14 de março, dia 4 de abril, dia 11 de maio e dia 8 de junho). Para maior detalhe acerca do planeamento pode ser consultado em anexo no primeiro apêndice.

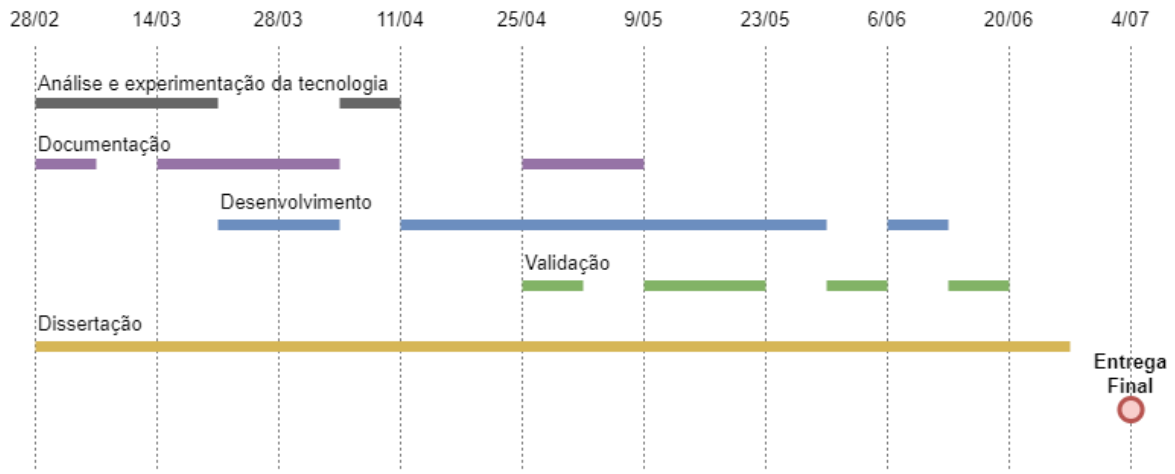


Figura 48 - Planeamento para o segundo semestre.

Plano Executado

O plano de trabalho executado no decorrer do segundo semestre do estágio divergiu substancialmente do plano originalmente criado, obrigando à entrega do documento em época especial. Na figura 49, pode ver-se que a diferença mais notável é o desaparecimento da **tarefa de validação** e o aparecimento de duas novas tarefas relacionadas com a componente de **interação com o utilizador**. A tarefa de validação foi sendo feita à medida que as funcionalidades eram implementadas e não existiu nenhum momento dedicado a testes unitários e de integração. A componente de interface da solução (*front-end*[43]) não foi inicialmente considerada como um objetivo de sucesso para o estágio e por isso não foi integrada no planeamento inicial. No entanto com o avançar da componente prática e da crescente complexidade da solução, tornou-se importante facilitar as demonstrações de forma a transpor mais valor para o estágio através de uma componente de *front-end*. Existiram ainda dois momentos no decorrer do semestre, onde o computador principal de trabalho teve indisponível durante alguns dias devido a problemas de software, o que obrigou à sua formatação, originando em atrasos no desenvolvimento. A decisão de entregar em época especial foi sendo avaliada à medida que a entrega de época normal se aproximava e o conteúdo e qualidade do documento de dissertação se mantinham aquém das expectativas, o que obrigou ao adiamento.

[43] Front-end – Refere-se à componente da interface que o utilizador interage [161].

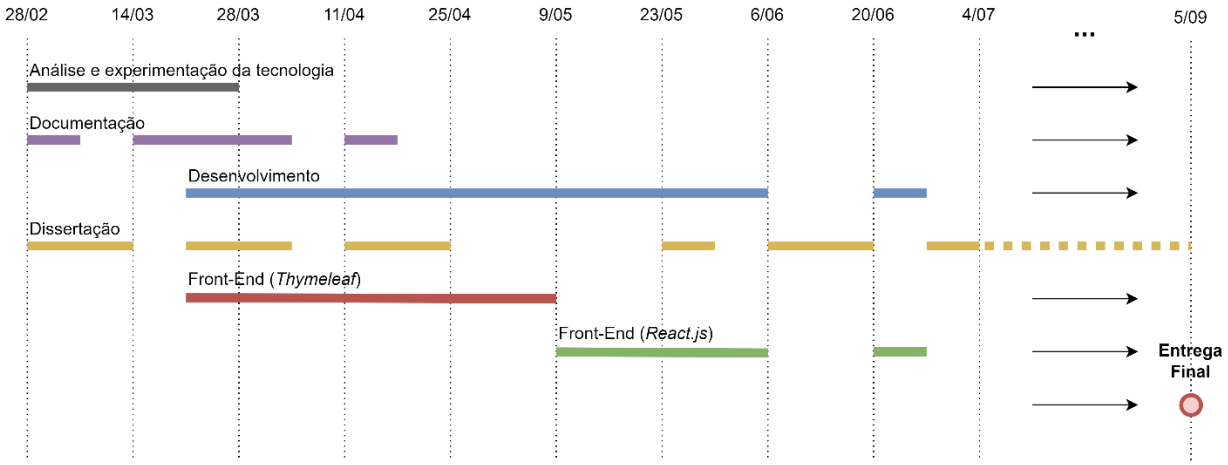


Figura 49 - Plano executado no segundo semestre.

Esta página foi intencionalmente deixada em branco

Capítulo 6
Conclusão

O principal objetivo deste estágio consistia no desenvolvimento de uma solução capaz de operar na atividade de envio de remessas para o mercado da Tanzânia de forma económica. Torna-se relevante para algo que pode impactar diretamente a vida da população em países em desenvolvimento, proporcionando melhores condições. O objetivo proposto foi atingido de uma forma significativa face a média de custos globais, sendo que para uma transferência de 200 dólares e uma transferência de 500 dólares apresenta uma redução de custos a rondar os 36.24% e 27.93%, respetivamente.

A solução desenvolvida é mais económica que a média do mercado, no entanto existiu uma falta de consideração na análise ao mercado de outros países onde também poderia vir a ser impactante. Para além disto, uma das grandes limitações deve-se à volatilidade do mercado de criptomoedas [144], que pode até colocar em causa tanto a viabilidade económica da solução como o funcionamento do serviço (ex: A entidade que fornece o serviço de levantamento de tokens de TZS pode deixar de operar caso os preços sejam demasiados baixos).

Apesar destas considerações, a solução desenvolvida neste estágio continua a ser valiosa para o corredor económico da Tanzânia devido aos baixos custos que apresenta. Para outros corredores, seria necessário uma análise e adaptação da solução a esses mercados de forma a usufruírem dos benefícios.

Para trabalho futuro seria importante integrar o depósito de fundos na carteira do utilizador através de um serviço que permitisse ao utilizador aumentar o saldo da sua conta sem ser obrigado a utilizar uma empresa de câmbio (ex: Coinbase ou Binance). Uma possível solução seria utilizar, da mesma forma que atualmente se realiza o levantamento dos tokens, um *Anchor*[44] para concretizar o depósito.

[44] Anchor – Uma entidade existente na rede blockchain da Stellar responsável pela conversão de dinheiro em tokens e vice-versa (maior detalhe na subsecção 3.2.2).

Esta página foi intencionalmente deixada em branco

Referências

[1] The Citizen, “Inside Tanzania’s remittance business,” *The Citizen*, Jan. 22, 2022.

[2] S. Gold, “World Bank projects 7.3% spike in 2021 remittances,” *Devex*, Nov. 2021.

[3] D. Ratha, “What are Remittances?,” *International Monetary Fund*, 2017, Accessed: Mar. 28, 2022. [Online]. Available: https://www.imf.org/external/pubs/ft/fandd/basics/pdf/ratha-remittances.pdf

[4] The World Bank, “Remittance Prices Worldwide Quarterly,” Mar. 2022. Accessed: Jul. 11, 2022. [Online]. Available: https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q122_final.pdf

[5] M. Lansisti and K. Lakhani, “The Truth About Blockchain,” *Harvard Business Review*, 2017. https://hbr.org/2017/01/the-truth-about-blockchain#:~:text=Blockchain%E2%80%94a%20peer%2Dto%2D,transferring%20ownership%2C%20and%20confirming%20transactions. (accessed Jul. 18, 2022).

[6] N. Gundaniya, “International remittance in times of COVID-19: Challenges, opportunities, and solutions,” *digipay*, 2020.

[7] Remitr, “What is Remittance and How Does it Work?,” *Remitr*, Jan. 28, 2020.

[8] IFAD, “11 reasons why remittances are important,” *IFAD*, 2021. https://www.ifad.org/en/web/latest/-/11-reasons-why-remittances-are-important (accessed Jan. 14, 2022).

[9] P. Vasconcelos, “Sending Money Home - World Remittance Flows to Developing and Transition Countries,” *IFAD*, 2017.

[10] R. Ruhmann, S. Konda, P. Horrocks, and N. Taka, “CAN BLOCKCHAIN TECHNOLOGY REDUCE THE COST OF REMITTANCES?,” *OEDC*, 2020, Accessed: Jan. 18, 2022. [Online]. Available: https://www.oecd-ilibrary.org/docserver/d4d6ac8f-en.pdf?expires=1642528149&id=id&accname=guest&checksum=747D811D451F682015F724E229FFDB55

[11] E. Simone, “Blockchain will lead the revolution in the banking sector,” *Worldline*, 2017.

[12] P. Shumsky, “How Blockchain Is Going To Change The Remittance In 2020,” *Finextra*, 2020.

[13] C. Vargas-Silva, “Migration and Development,” *The Migration Observatory*, 2012. https://migrationobservatory.ox.ac.uk/resources/primers/migration-and-development/ (accessed Jun. 21, 2022).

[14] Western Union, “This is the Fee Table,” 2022. Accessed: Jan. 14, 2022. [Online]. Available: https://www.westernunion.com/content/dam/wu/EU/EN/feeTableRetailEN-ES.PDF

[15] Money Banking, “The Stubbornly High Cost of Remittances,” *Money Banking*, Feb. 2018. https://www.moneyandbanking.com/commentary/2018/2/18/the-stubbornly-high-cost-of-remittances (accessed Jun. 21, 2022).
[16] World Bank, “Remittance Prices Worldwide,” *World Bank*, 2022. https://remittanceprices.worldbank.org/en (accessed Jan. 14, 2022).
[17] J. Dridi, T. Gursoy, H. Perez-Saiz, and M. Bari, “The Impact of Remittances on Economic Activity: The Importance of Sectoral Linkages,” *IMF Working Paper*, 2019, Accessed: Jan. 14, 2022. [Online]. Available: https://www.imf.org/en/Publications/WP/Issues/2019/08/16/The-Impact-of-Remittances-on-Economic-Activity-The-Importance-of-Sectoral-Linkages-47091
[18] C. Murphy, “Remittance,” *Investopedia*, 2021. https://www.investopedia.com/terms/r/remittance.asp (accessed Jan. 14, 2022).
[19] Ebanx, “Remittance,” *Ebanx*, 2021. https://business.ebanx.com/en/resources/payments-explained/remittance (accessed Jan. 14, 2022).
[20] inPay, “How to make receiving international bank cheques easier for your recipients,” *inPay*, 2022. https://www.inpay.com/cross-border-insights/how-to-make-international-bank-cheques-easier-for-your-recipients/ (accessed Apr. 26, 2022).
[21] R. Lake, “ACH Transfers: What Are They and How Do They Work?,” *Investopedia*, 2021. https://www.investopedia.com/ach-transfers-what-are-they-and-how-do-they-work-4590120 (accessed Jan. 15, 2022).
[22] Ebanx, “Electronic Funds Transfer (EFT),” *Ebanx*, 2022, Accessed: Apr. 26, 2022. [Online]. Available: https://business.ebanx.com/en/resources/payments-explained/electronic-funds-transfer-eft#:~:text=An%20electronic%20funds%20transfer%20(EFT,place%20independently%20from%20bank%20employees.
[23] GoCardless, “Difference Between EFT and Wire Transfer,” *GoCardless*, 2021. https://gocardless.com/en-au/guides/posts/difference-between-eft-and-wire-transfer/#:~:text=They%20both%20offer%20secure%2C%20convenient,is%20the%20speed%20of%20transaction. (accessed Apr. 26, 2022).
[24] J. Kagan, “Wire Transfer,” *Investopedia*, 2021. https://www.investopedia.com/terms/w/wiretransfer.asp (accessed Jan. 15, 2022).
[25] Wise, “How to pay by bank transfer,” *Wise*, 2021. https://wise.com/help/articles/2559761/how-to-pay-by-bank-transfer (accessed Jan. 18, 2022).
[26] S. Ross, “Correspondent Banks vs. Intermediary Banks: What’s the Difference?,” *Investopedia*, Mar. 2022. https://www.investopedia.com/ask/answers/062515/what-difference-between-correspondent-bank-and-intermediary-bank.asp (accessed Jun. 21, 2022).
[27] The World Bank, “Remittance Flows Register Robust 7.3 Percent Growth in 2021,” *The World Bank*, Nov. 2021. https://www.worldbank.org/en/news/press-release/2021/11/17/remittance-flows-register-robust-7-3-percent-growth-in-2021 (accessed Aug. 16, 2022).

[28] M. Kituyi, “Cutting the Costs of Remittances: The Role of Mobile Money - Opening Remarks,” *UNCTAD*, 2014. https://unctad.org/osgstatement/cutting-costs-remittances-role-mobile-money-opening-remarks#:~:text=Increasing%20the%20amount%20of%20remittances,well%20as%20their%20development%20impact. (accessed Jan. 19, 2022).
[29] A. Twin, “6 Factors That Influence Exchange Rates,” *Investopedia*, 2021. https://www.investopedia.com/trading/factors-influence-exchange-rates/ (accessed Jan. 19, 2022).
[30] J. David, “Closing the Gaps Between Fintechs and Legacy Banks,” *IBM*, Feb. 2022. https://www.ibm.com/cloud/blog/closing-the-gaps-between-fintechs-and-legacy-banks (accessed Jun. 21, 2022).
[31] V. Vahromovs, “Legacy systems in banking: the major barrier for digital transformation,” *fintech futures*, Nov. 2021. https://www.fintechfutures.com/2021/11/legacy-systems-in-banking-the-major-barrier-for-digital-transformation/ (accessed Jun. 21, 2022).
[32] A. Graham, “Fintech and Banks: How Can the Banking Industry Respond to the Threat of Disruption?,” *Toptal*, 2017. https://www.toptal.com/finance/investment-banking-freelancer/fintech-and-banks (accessed Mar. 28, 2022).
[33] CompaniesMarketCap, “Market Cap,” *Companies Market Cap*, 2022. https://companiesmarketcap.com/western-union/marketcap/ (accessed Apr. 04, 2022).
[34] IFAD, “11 reasons why remittances are important,” *IFAD*, 2021. https://www.ifad.org/en/web/latest/-/11-reasons-why-remittances-are-important (accessed Mar. 28, 2022).
[35] The World Bank, “Remittance Prices Worldwide Quarterly,” 2021. Accessed: Jan. 19, 2022. [Online]. Available: https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q221.pdf
[36] SDSN, “10.c by 2030, reduce to less than 3% the transaction costs of migrant remittances and eliminate remittance corridors with costs higher than 5%,” *Indicators and a Monitoring Framework*, 2012. https://indicators.report/targets/10-c/ (accessed Aug. 24, 2022).
[37] P. Dupas, D. Karlan, J. Robinson, and D. Ubfal, “Banking the Unbanked? Evidence from Three Countries,” *American Economic Journal*, 2018, Accessed: Jul. 20, 2022. [Online]. Available: https://web.stanford.edu/~pdupas/BankingTheUnbanked.pdf
[38] M. Barreto, “Finanças descomplicadas: A importância do Mobile Money,” *Forbes Portugal*, Jan. 2021. https://www.forbespt.com/opiniao/financas-descomplicadas-a-importancia-do-mobile-money/ (accessed Jul. 18, 2022).
[39] S. Onyango, “Africa accounts for 70% of the world’s $1 trillion mobile money market,” *Quartz Africa*, 2022. https://qz.com/africa/2161960/gsma-70-percent-of-the-worlds-1-trillion-mobile-money-market-is-in-africa/ (accessed Jul. 20, 2022).
[40] GSMA, “Mobile money and international remittances: Enabling recovery during COVID-19,” *GSMA*, 2021. https://www.gsma.com/mobilefordevelopment/mobile-

money-4/mobile-money-and-international-remittances-enabling-recovery-during-covid-19/#:~:text=When%20using%20mobile%20money%2C%20remittances,during%20the%20COVID%2D19%20pandemic. (accessed Jul. 20, 2022).
[41] Compare Remit, “Mobile Money Transfer: Pros and Cons,” *Compare Remit*, 2022. https://www.compareremit.com/money-transfer-tips/mobile-money-transfer-pros-and-cons/ (accessed Jul. 20, 2022).
[42] J. Barton, “Youtap and MatchMove bringing open-loop mobile money payments to Africa and Asia,” *Developing Telecoms*, 2017. https://developingtelecoms.com/telecom-technology/financial-services/7130-youtap-and-matchmove-bringing-open-loop-mobile-money-payments-to-africa-and-asia.html (accessed Jul. 20, 2022).
[43] Liquid, “Future of Cross-Border Payments: Blockchain Remittance Explained,” *Liquid*, 2021. https://blog.liquid.com/remittance-blockchain-crypto#:~:text=Blockchain%20remittance%20is%20a%20financial,probably%20located%20in%20two%20countries. (accessed Jun. 21, 2022).
[44] CBInsights, “How Blockchain Could Disrupt Banking,” *CBInsights*, Feb. 11, 2021. https://www.cbinsights.com/research/blockchain-disrupting-banking/ (accessed Apr. 04, 2022).
[45] K. Gai, J. Guo, L. Zhu, and S. Yu, “Blockchain Meets Cloud Computing: A Survey,” *IEEE*, 2020.
[46] Porto Editora, “livro-diário,” *Infopédia*, 2022. https://www.infopedia.pt/dicionarios/lingua-portuguesa/livro-di%C3%A1rio (accessed Jun. 21, 2022).
[47] J. Frankenfield, “Distributed Ledger Technology (DLT),” *2021*, Aug. 27, 2021. https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp (accessed Apr. 04, 2022).
[48] P. Chateterjee, “Public vs private blockchains: How do they differ,” *Analytics India Mag*, Feb. 2022. https://analyticsindiamag.com/public-vs-private-blockchains-how-do-they-differ/#:~:text=Blockchain%20is%20divided%20into%20two,of%20access%20given%20to%20users. (accessed Jun. 22, 2022).
[49] E. Rutland, “Blockchain Byte,” *R3 Research*, 2021, Accessed: Oct. 26, 2021. [Online]. Available: https://www.finra.org/sites/default/files/2017_BC_Byte.pdf
[50] V. Buterin, “The Meaning of Decentralization,” *Medium*, Feb. 2017. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (accessed Jun. 22, 2022).
[51] G. Iredale, “6 Key Blockchain Features You Need To Know Now,” *101 Blockchain*, 2021. https://101blockchains.com/introduction-to-blockchain-features/ (accessed Jun. 22, 2022).
[52] B. Shrimali and H. B. Patel, “Blockchain state-of-the-art: architecture, use cases, consensus,challenges and opportunities,” *King Saud University –Computer and*

Information Sciences, 2021, Accessed: Oct. 13, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S131915782100207X?via%3Dihub
[53] A. Hayes, "Blockchain Explained," *Investopedia*, Jun. 2022. https://www.investopedia.com/terms/b/blockchain.asp (accessed Jun. 22, 2022).
[54] Y.-C. Liang, "Blockchain for Dynamic Spectrum Management," Jan. 2020, Accessed: Apr. 05, 2022. [Online]. Available: https://www.researchgate.net/figure/The-structure-of-a-Blockchain-A-block-is-composed-of-a-header-and-a-body-where-a-header_fig1_337306138#:~:text=A%20block%20is%20composed%20of%20a%20header%20and%20a%20body,stored%20in%20the%20block%20body.
[55] A. Yadav, "What is blockchain and how it is tamper proof?," *Medium*, May 18, 2020. https://levelup.gitconnected.com/what-is-blockchain-and-how-it-is-tamper-proof-f86744cb7787 (accessed Apr. 08, 2022).
[56] Y.-C. Liang, "Blockchain for Dynamic Spectrum Management," *Creative Commons Attribution 4.0 International*, 2020, Accessed: Dec. 25, 2021. [Online]. Available: https://www.researchgate.net/figure/The-structure-of-a-Blockchain-A-block-is-composed-of-a-header-and-a-body-where-a-header_fig1_337306138
[57] B. Academy, "What is Timestamp?," *Bit2Me Academy*, 2020. https://academy.bit2me.com/en/blockchain-timestamp/ (accessed Dec. 25, 2021).
[58] J. Frankenfield, "Nonce," *Investopedia*, 2020. https://www.investopedia.com/terms/n/nonce.asp (accessed Dec. 25, 2021).
[59] Wikipedia, "Cryptography," *Wikipedia*, 2021. https://en.wikipedia.org/wiki/Cryptography (accessed Dec. 24, 2021).
[60] J. Thakkar, "Types of Encryption: 5 Encryption Algorithms & How to Choose the Right One," *The SSL Store*, May 2020. https://www.thesslstore.com/blog/types-of-encryption-encryption-algorithms-how-to-choose-the-right-one/#:~:text=Symmetric%20Encryption-,Asymmetric%20Encryption,a%20simpler%20method%20of%20encryption. (accessed Jun. 22, 2022).
[61] J. Harmening, *Virtual Private Networks*, 3rd ed. 2017. Accessed: Jun. 22, 2022. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/symmetric-encryption#:~:text=Symmetric%20encryption%20is%20also%20called%20%E2%80%9Csecret%20key%E2%80%9D%20encryption%20because%20the,two%20parties%20may%20communicate%20securely.
[62] Kaspersky, "Cryptography Definition," *Kaspersky*, 2021. https://www.kaspersky.com/resource-center/definitions/what-is-cryptography (accessed Nov. 12, 2021).
[63] M. Sahu, "Cryptography in Blockchain: Types & Applications," *upGrad*, 2021. https://www.upgrad.com/blog/cryptography-in-blockchain/ (accessed Dec. 24, 2021).
[64] J. Lake, "Understanding cryptography's role in blockchains," *Comparitech*, 2019. https://www.comparitech.com/crypto/cryptography-blockchain/ (accessed Dec. 25, 2021).

[65] A. Rawat, “Blockchain Mining: Types and Uses,” *Analytic Steps*, 2021. https://www.analyticssteps.com/blogs/blockchain-mining-types-and-uses (accessed Dec. 26, 2021).
[66] Freeman Law, “Mining Explained,” *Freeman Law*, 2021. https://freemanlaw.com/mining-explained-a-detailed-guide-on-how-cryptocurrency-mining-works/ (accessed Nov. 12, 2021).
[67] Coin Market Cap, “Bitcoin,” *Coin Market Cap*, 2021. https://coinmarketcap.com/currencies/bitcoin/ (accessed Dec. 27, 2021).
[68] Bitcoin IT, “Pool Vs. Solo Mining,” *Bitcoin IT*, 2020. https://en.bitcoin.it/wiki/Pool_vs._solo_mining (accessed Dec. 27, 2021).
[69] D. Oyinloye, J. Teh, N. Jamil, and M. Alawida, “Blockchain Consensus: An Overview of Alternative Protocols,” *Symmetry (Basel)*, 2021, Accessed: Dec. 27, 2021. [Online]. Available: https://www.mdpi.com/2073-8994/13/8/1363/htm
[70] Bitcoin Wiki, “CPU mining,” *Bitcoin Wiki*, 2022. https://en.bitcoinwiki.org/wiki/CPU_mining (accessed Jun. 22, 2022).
[71] S. Seth, “GPU Usage in Cryptocurrency Mining,” *Investopedia*, Apr. 2022. https://www.investopedia.com/tech/gpu-cryptocurrency-mining/#:~:text=Key%20Takeaways,to%20their%20speed%20and%20efficiency. (accessed Jun. 22, 2022).
[72] C. Tardi, “Application-Specific Integrated Circuit (ASIC) Miner,” *Investopedia*, Mar. 2022. https://www.investopedia.com/terms/a/asic.asp#:~:text=An%20ASIC%20miner%20refers%20to,miner%20can%20mine%20only%20bitcoin. (accessed Apr. 15, 2022).
[73] Wikipedia, “Consensus (computer science),” *Wikipedia*, 2021. https://en.wikipedia.org/wiki/Consensus_(computer_science) (accessed Oct. 14, 2021).
[74] S. Zhang and J. Hyouk, “Analysis of the main consensus protocols of blockchain,” *KICS*, 2019. https://www.sciencedirect.com/science/article/pii/S240595951930164X (accessed Dec. 28, 2021).
[75] J. Huang, C. O’Neill, and H. Tabuchi, “Bitcoin Uses More Electricity than Many Countries. How is that possible?,” *The New York Times*, 2021. Accessed: Oct. 14, 2021. [Online]. Available: https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html
[76] C. Beekhuizen, “A country’s worth of power, no more!,” *EF Blog*, 2021. https://blog.ethereum.org/2021/05/18/country-power-no-more/ (accessed Oct. 16, 2021).
[77] J. Frankenfield, “Proof-of-Stake (PoS),” *Investopedia*, Jun. 2022. https://www.investopedia.com/terms/p/proof-stake-pos.asp#:~:text=Proof%2Dof%2Dstake%20is%20a,and%20keeping%20the%20database%20secure. (accessed Jun. 22, 2022).

[78] E. Hong, “How does Bitcoin mining work?,” *Investopedia*, Nov. 30, 2021. https://www.investopedia.com/tech/how-does-bitcoin-mining-work/ (accessed Dec. 04, 2021).
[79] Unibright, “Blockchain Evolution: From 1.0 to 4.0,” *Unibright.io*, 2017. https://unibrightio.medium.com/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666 (accessed Dec. 29, 2021).
[80] Alexandria, “Blockchain 1.0,” *Coin Market Cap*, 2021. https://coinmarketcap.com/alexandria/glossary/blockchain-1-0 (accessed Oct. 16, 2021).
[81] M. Haller Grønbæk, “Blockchain 2.0, smart contracts and challenges,” *Bird & Bird Copenhagen*, 2020, Accessed: Oct. 16, 2021. [Online]. Available: https://www.twobirds.com/~/media/pdfs/in-focus/fintech/blockchain2_0_martinvonhallergroenbaek_08_06_16.pdf
[82] The Blog, “What Is Blockchain 3.0? | A Guide to the Next Phase of DLT,” *Elev8*, 2019. https://www.elev8con.com/what-is-blockchain-3-0-a-guide-to-the-next-phase-of-dlt/ (accessed Oct. 16, 2021).
[83] Bytesoft, “What is blockchain 4.0 ?,” *Bytesoft*, 2021. https://bytesoft.vn/en/what-is-blockchain-4-0 (accessed Oct. 16, 2021).
[84] M. Kukkuru, “Smart Contracts: Introducing A Transparent Way To Do Business,” *Infosys*, 2021. https://www.infosys.com/insights/digital-future/smart-contracts.html (accessed Jan. 13, 2022).
[85] J. Frankenfield, “Cryptocurrency,” *Investopedia*, 2021. https://www.investopedia.com/terms/c/cryptocurrency.asp (accessed Jan. 06, 2022).
[86] D. Kurt, “How Currency Works,” *Investopedia*, May 2022. https://www.investopedia.com/articles/investing/092413/how-currency-works.asp (accessed Aug. 23, 2022).
[87] Coin Market Cap, “Today’s Cryptocurrency Prices by Market Cap,” *Coin Market Cap*, 2021. https://coinmarketcap.com/ (accessed Jan. 06, 2022).
[88] J. Craig, “Crypto Minting vs. Mining: What’s the difference?,” *Phemex*, 2021. https://phemex.com/blogs/crypto-minting-vs-crypto-mining (accessed Jan. 06, 2022).
[89] N. Reiff, “Bitcoin vs. Ripple: What’s the Difference?,” *Investopedia*, 2021. https://www.investopedia.com/tech/whats-difference-between-bitcoin-and-ripple/ (accessed Jan. 06, 2022).
[90] A. Zadikoff and A. Chiu, “Digital Assets: Cryptocurrencies vs. Tokens,” *Cryptopedia*, 2022. https://www.gemini.com/cryptopedia/cryptocurrencies-vs-tokens-difference (accessed Jul. 14, 2022).
[91] Global Cap, “What is Tokenization? – The Fundamentals Explained,” *Global Cap*, 2021. https://globacap.com/content-hub/learn/what-is-tokenization/ (accessed Jan. 11, 2022).
[92] Liquid, “Blockchain-based Remittance Service,” *Liquid*, 2021, Accessed: Jun. 08, 2022. [Online]. Available: https://blog.liquid.com/remittance-blockchain-crypto#:~:text=Blockchain%20remittance%20is%20a%20financial,probably%20located%20in%20two%20countries.

[93] Everex, “Everex,” *Everex*, 2022. https://everex.io/company/ (accessed Jun. 08, 2022).
[94] The Paypers, “News Everex provides blockchain-powered remittance services with challenger bank,” *The Paypers*, 2018. Accessed: Jun. 08, 2022. [Online]. Available: https://thepaypers.com/online-payments/everex-provides-blockchain-powered-remittance-services-with-challenger-bank--774172#
[95] UNCDF, “Myanmar - Country Monitor on Migration & Remittance,” *UNCDF*, Apr. 2021, Accessed: Jun. 08, 2022. [Online]. Available: https://migrantmoney.uncdf.org/wp-content/uploads/2021/10/country-monitor-on-migration-and-remittance-myanmar.pdf
[96] Blockdata, “List of Remittances companies,” *Blockdata*, 2022. https://www.blockdata.tech/markets/use-cases/remittances (accessed Jun. 08, 2022).
[97] D. Cox, “Bithumb Review 2022,” *CryptoNewsZ*, May 11, 2022. https://www.cryptonewsz.com/cryptocurrency-exchange/bithumb-review/ (accessed Jun. 13, 2022).
[98] CoinWire, “Bithumb Unites with BitPay to Compete in International Remittance Market,” *CoinWire*, 2019, Accessed: Jun. 13, 2022. [Online]. Available: https://www.coinwire.com/bithumb-unites-with-bitpay-to-compete-in-international-remittance-market
[99] W. Foxley, “Bithumb Global Launches Native Token for Exchange Ecosystem,” *CoinDesk*, 2019, Accessed: Jun. 13, 2022. [Online]. Available: https://www.coindesk.com/markets/2019/11/12/bithumb-global-launches-native-token-for-exchange-ecosystem/
[100] M. Govind, “BizDay: Improving Remittances in the World’s 2nd Largest Corridor, Digiledge,” *CordaCon*, 2019. https://www.slideshare.net/MarketingTeamr3/bizday-improving-remittances-in-the-worlds-2nd-largest-corridor-digiledge-193995812 (accessed Jun. 13, 2022).
[101] Digiledge, “Enterprise graded Blockchain Solutions for banking, insurance and supply chain using IoT & Artificial Intelligence,” *Digiledge*, 2022. http://www.digiledge.com/ (accessed Jun. 13, 2022).
[102] Satander, “Blockchain: security and transparency at the service of banking,” *Satander*, 2021, Accessed: Jun. 13, 2022. [Online]. Available: https://www.santander.com/en/stories/blockchain-security-and-transparency-at-the-service-of-banking
[103] N. DiCamillo, “ Santander to Connect Latin America to Ripple-Powered Remittance Service,” *CoinDesk*, 2019, Accessed: Jun. 13, 2022. [Online]. Available: https://www.coindesk.com/markets/2019/08/19/santander-to-connect-latin-america-to-ripple-powered-remittance-service/
[104] Satander, “What are smart contracts?,” *Satander*, 2022, Accessed: Jun. 13, 2022. [Online]. Available: https://www.santander.com/en/stories/smart-contracts
[105] IBM, “Banco Satander,” *IBM*, 2021, Accessed: Jun. 13, 2022. [Online]. Available: https://www.ibm.com/case-studies/banco-santander-ibm-blockchain
[106] Trading Economics, “Tanzania - Remittance Inflows To GDP,” *Trading Economics*, 2020. https://tradingeconomics.com/tanzania/remittance-inflows-to-gdp-percent-

wb-data.html#:~:text=Remittance%20inflows%20to%20GDP%20(%25),compiled%20from%20officially%20recognized%20sources. (accessed Aug. 16, 2022).
[107] The World Bank, “World Development Indicators,” *The World Bank*, 2022. https://datacatalog.worldbank.org/search/dataset/0037712 (accessed Aug. 16, 2022).
[108] V. Oluwole, “Tanzania, Uganda, and South Africa are the top African markets for remittance inflows in Kenya,” *Business Insider Africa*, 2022, Accessed: Jun. 13, 2022. [Online]. Available: https://africa.businessinsider.com/local/markets/tanzania-uganda-and-south-africa-are-the-top-african-markets-for-remittance-inflows/qcttsx3
[109] The Citizen, “Inside Tanzania’s remittance business,” *The Citizen*, 2022, Accessed: Jun. 13, 2022. [Online]. Available: https://www.thecitizen.co.tz/tanzania/news/business/inside-tanzania-s-remittance-business-3687354
[110] Coinbase, “How to buy XRP,” 2022. https://www.coinbase.com/pt/how-to-buy/xrp (accessed Jun. 14, 2022).
[111] XRP Ledger Services, “List of all Tokens on the XRP Ledger Mainnet,” 2022. https://xrpl.services/tokens (accessed Jun. 14, 2022).
[112] Team Ripple, “bKash and Mobile Money Connect Through RippleNet To Power Wallet-To-Wallet Remittances,” Jan. 2021. https://ripple.com/insights/bkash-and-mobile-money-connect-through-ripplenet-to-power-wallet-to-wallet-remittances/ (accessed Jun. 14, 2022).
[113] XRP Ledger, “Transaction Cost,” 2022. https://xrpl.org/transaction-cost.html (accessed Jun. 14, 2022).
[114] Ripple, “Ripple,” *Ripple*, 2022. https://ripple.com/xrp/ (accessed Jun. 14, 2022).
[115] A. Bada, C. Angelopoulos, A. Damianou, and V. Katos, “Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption,” 2021.
[116] Coinbase, “How to buy Stellar Lumens,” 2022. https://www.coinbase.com/how-to-buy/stellar (accessed Jun. 14, 2022).
[117] StellarX, “Swap Assets,” 2022. https://www.stellarx.com/swap/native/TZS:GA2MSSZKJOU6RNL3EJKH3S5TB5CDYTFQFWRYFGUJVIN5I6AOIRTLUHTO (accessed Jun. 14, 2022).
[118] Stellar, “Sep-24: Deposits & Withdrawals,” 2022. https://developers.stellar.org/docs/anchoring-assets/enabling-deposit-and-withdrawal/ (accessed Jun. 14, 2022).
[119] Stellar, “Fees,” 2022. https://developers.stellar.org/docs/glossary/fees/ (accessed Jun. 14, 2022).
[120] A. Takyar, “What is Stellar Blockchain? A complete guide for beguinners,” *Leewayhertz*, 2021, Accessed: Jun. 14, 2022. [Online]. Available: https://www.leewayhertz.com/what-is-stellar-blockchain/#:~:text=The%20Stellar%20database%20is%20decentralized,thousands%20of%20transactions%20per%20second.
[121] Coinbase, “How to buy Algorand,” 2022. https://www.coinbase.com/how-to-buy/algorand (accessed Jun. 14, 2022).

[122] Algo Explorer, “Algo Explorer,” 2022. https://algoexplorer.io/ (accessed Jun. 14, 2022).
[123] Bnex, “Bnext Announces Next-Generation Remittance Service Across Spain and Latin America with Blockchain-based Solution on Algorand,” *Algorand*, 2021. https://www.algorand.com/resources/ecosystem-announcements/bnext-announces-next-generation-remittance-service (accessed Jun. 14, 2022).
[124] Algorand, “Frequently Asked Questions,” *Algorand*, 2022. https://algorand.foundation/faq (accessed Jun. 14, 2022).
[125] Algorand, “Atomic Transfers,” 2022. https://developer.algorand.org/docs/get-details/atomic_transfers/#:~:text=An%20atomic%20transfer%20on%20Algorand,governed%20by%20Algorand%20Smart%20Contracts. (accessed Jun. 14, 2022).
[126] Algorand, “About Algorand Protocol,” *Algorand*, 2022. https://algorand.foundation/algorand-protocol/about-algorand-protocol (accessed Jun. 14, 2022).
[127] Coinbase, “Own Ethereum in just a few minutes,” 2022, Accessed: Jun. 14, 2022. [Online]. Available: https://www.coinbase.com/buy-ethereum
[128] Cryptoslate, “Ethereum Cryptos,” 2022, Accessed: Jun. 14, 2022. [Online]. Available: https://cryptoslate.com/blockchain/ethereum/
[129] KeeCash, “How to withdraw your cryptos to your Mobile Money?,” 2022, Accessed: Jun. 14, 2022. [Online]. Available: https://aide.keecash.com/en/article/withdraw-your-cryptocurrencies-to-your-mobile-money-jowc3t/
[130] ycharts, “Ethereum average transaction fee,” 2022. https://ycharts.com/indicators/ethereum_average_transaction_fee#:~:text=Ethereum%20Average%20Transaction%20Fee%20is,29.48%25%20from%20one%20year%20ago. (accessed Jun. 14, 2022).
[131] A. Sergeenkov, “How to Check Your Ethereum Transaction,” *CoinDesk*, 2021. https://www.coindesk.com/learn/how-to-check-your-ethereum-transaction/#:~:text=On%20average%2C%20it%20usually%20takes,network%20congestion%20at%20the%20time. (accessed Jun. 14, 2022).
[132] Coinbase, “How to buy Chia,” 2022. https://www.coinbase.com/how-to-buy/chia-network (accessed Jun. 15, 2022).
[133] Hashgreen, “First DEX on Chia. Secure. Anonymous,” *Hashgreen*, 2022. https://hash.green/ (accessed Jun. 15, 2022).
[134] XCHScan, “Average Transaction Fee Chart,” *XCHScan*, 2022. https://xchscan.com/charts/txn-fee (accessed Jun. 15, 2022).
[135] KryptoMine, “The Pros and cons of Chia,” *Chia Forum*, 2022. https://chiaforum.com/t/the-pros-and-cons-of-chia/15861 (accessed Jun. 15, 2022).
[136] Coinbase, “Stellar Lumens price,” *Coinbase*, 2022. https://www.coinbase.com/price/stellar (accessed Jun. 15, 2022).
[137] Stellar, “Stellar for Remittances,” *Stellar*, 2022. https://www.stellar.org/learn/stellar-for-remittances?locale=en#:~:text=UsMeridianEvents-,Stellar%20for%20Remittances,sent%20on%20a%20monthly%20basis. (accessed Jun. 15, 2022).

[138] Stellar, “Decentralized Exchange,” *Stellar*, 2022. https://developers.stellar.org/docs/glossary/decentralized-exchange/ (accessed Jun. 15, 2022).
[139] Stellar, “Anchor Basics,” *Stellar*, 2022. https://www.stellar.org/learn/anchor-basics?locale=en (accessed Jun. 15, 2022).
[140] T. Tepper and J. Schmidt, “The Best Crypto Exchanges Of July 2022,” *Forbes*, Jul. 2022. https://www.forbes.com/advisor/investing/cryptocurrency/best-crypto-exchanges/ (accessed Jul. 12, 2022).
[141] Stellar, “Stellar X,” *Stellar X*, 2022. https://www.stellarx.com/swap/native/TZS:GA2MSSZKJOU6RNL3EJKH3S5TB5CDYTFQFWRYFGUJVIN5I6AOIRTLUHTO (accessed Jul. 13, 2022).
[142] B. Materu, “Tanzania registers 3.2m new mobile money subscribers: report,” *The East African*, Jun. 2022, Accessed: Jul. 14, 2022. [Online]. Available: https://www.theeastafrican.co.ke/tea/business/tanzania-mobile-money-subscribers-3835552#:~:text=By%20BEATRICE%20MATERU-,Tanzania%20has%20registered%203.2%20million%20more%20mobile%20money%20subscribers%20in,in%20January%2C%20a%20report%20shows.
[143] Country Meters, “Tanzania Population,” *Country Meters*, 2022. https://countrymeters.info/en/Tanzania (accessed Jul. 14, 2022).
[144] A. Zadikoff and A. Chiu, “Healthy Volatility and Its Implications for Crypto Markets,” *Gemini*, Jun. 2022. https://www.gemini.com/cryptopedia/volatility-index-crypto-market-price (accessed Jul. 18, 2022).
[145] W. Kenton, “Fedwire,” *Investopedia*, 2021. https://www.investopedia.com/terms/f/fedwire.asp (accessed Jan. 15, 2022).
[146] Infopedia, “Produto Interno Bruto,” *Infopedia*, 2021. https://www.infopedia.pt/$produto-interno-bruto-(pib) (accessed Jan. 19, 2022).
[147] Z. Laub, “The Group of Eight (G8) Industrialized Nations,” *Council Foreign Relations*, 2014. https://www.cfr.org/backgrounder/group-eight-g8-industrialized-nations#:~:text=The%20Group%20of%20Eight%20(G8)%20refers%20to%20the%20group%20of,security%2C%20energy%2C%20and%20terrorism. (accessed Jan. 20, 2022).
[148] Wikipedia, “G20,” *Wikipedia*, 2022. https://en.wikipedia.org/wiki/G20 (accessed Jan. 20, 2022).
[149] Kaspersky, “O que é smishing e como se proteger?,” *Kaspersky*, 2022. https://www.kaspersky.com.br/resource-center/threats/what-is-smishing-and-how-to-defend-against-it (accessed Jul. 20, 2022).
[150] Wikipedia, “Single point of failure,” *Wikipedia*, 2022. https://en.wikipedia.org/wiki/Single_point_of_failure (accessed Jul. 21, 2022).
[151] H. Fernandes, “O que é um sistema/aplicação Monolito/Monolítica?,” *Henrique Marques Fernandes*, 2020. https://marquesfernandes.com/tecnologia/o-que-e-um-sistema-aplicacao-monolito-monolitica/ (accessed Aug. 24, 2022).
[152] A. Zola, “Hashing,” *Tech Target*, 2022. https://www.techtarget.com/searchdatamanagement/definition/hashing (accessed Aug. 30, 2022).

[153] Wikipedia, “Binary Tree,” *Wikipedia*, 2021. https://en.wikipedia.org/wiki/Binary_tree#:~:text=In%20computer%20science%2C%20a%20binary,child%20and%20the%20right%20child.&text=It%20is%20also%20possible%20to,is%20an%20ordered%2C%20rooted%20tree. (accessed Dec. 26, 2021).
[154] Wikipedia, “Hardware,” *Wikipedia*, 2021. https://pt.wikipedia.org/wiki/Hardware (accessed Apr. 08, 2022).
[155] J. Chen, “Fiat Money,” *Investopedia*, 2021. https://www.investopedia.com/terms/f/fiatmoney.asp (accessed Dec. 27, 2021).
[156] Banco de Portugal, “O que é a emissão monetária?,” *Banco de Portugal*, 2022. https://bpstat.bportugal.pt/conteudos/publicacoes/1185#:~:text=A%20emiss%C3%A3o%20monet%C3%A1ria%20%C3%A9%20o,aceita%C3%A7%C3%A3o%20em%20pagamentos%20ou%20trocas. (accessed Aug. 23, 2022).
[157] Wikipedia, “Interoperabilidade,” *Wikipedia*, 2022. https://pt.wikipedia.org/wiki/Interoperabilidade (accessed Jun. 08, 2022).
[158] Wikipedia, “Unbanked,” *Wikipedia*, 2022. https://en.wikipedia.org/wiki/Unbanked (accessed Jul. 18, 2022).
[159] Airfocus, “What is a Mockup?,” *Airfocus*. https://airfocus.com/glossary/what-is-a-mockup/ (accessed Jul. 25, 2022).
[160] L. Rosencrance, “software development kit (SDK),” *WhatIs*, 2019. https://www.techtarget.com/whatis/definition/software-developers-kit-SDK#:~:text=A%20software%20development%20toolkit%20(SDK,their%20apps%20with%20their%20services. (accessed Jul. 01, 2022).
[161] Concepta, “What Is the Difference Between Front-End and Back-End Development?,” *Concepta*, 2022. https://www.conceptatech.com/blog/difference-front-end-back-end-development#:~:text=The%20term%20%E2%80%9Cfront%2Dend%E2%80%9D,deliver%20information%20to%20the%20user. (accessed Jun. 27, 2022).
[162] Wikipedia, “Template processor,” *Wikipedia*, 2022. https://en.wikipedia.org/wiki/Template_processor (accessed Jun. 28, 2022).
[163] B. Hufford, “What is a Mockup? (+How to Create a Mockup in 2022),” *Clique*, 2022. https://cliquestudios.com/mockups/#:~:text=A%20mockup%20is%20a%20static,each%20part%20of%20that%20definition. (accessed Jun. 28, 2022).
[164] Reserve Bank of India, “FREQUENTLY ASKED QUESTIONS,” *Reserve Bank of India*, 2021. https://m.rbi.org.in/scripts/FAQView.aspx?Id=65 (accessed Jul. 13, 2022).

Apêndices

Planeamento do Estágio

Neste apêndice, pode ver-se o planeamento criado para os dois semestres de estágio. Para o primeiro semestre foi usado o Excel como ferramenta para delinear as tarefas. No entanto, para o segundo semestre, de modo a planear com maior detalhe conservando a visibilidade de todas as tarefas em qualquer momento do estágio foi utilizado o Draw.io.

	September	October				November				December				January			
Task	Week 4	Week 1	Week 2	Week 3	Week 4	Week 1	Week 2	Week 3	Week 4	Week 1	Week 2	Week 3	Week 4	Week 1	Week 2	Week 3	Week 4
Internship Contextualization																	
Research																	
Planning																	
Blockchain																	
Remittances and Mobile Money																	
Experimentation																	
Benchmark																	
Pratical Experimentation																	
Thesis																	
Technology Background																	
State of the Art																	
Requeriments																	
Quality Review																	
Other																	
Internal Presentation																	
Intermediary Delivery																	

Figura 50 – Esquematização do planeamento para o primeiro semestre.

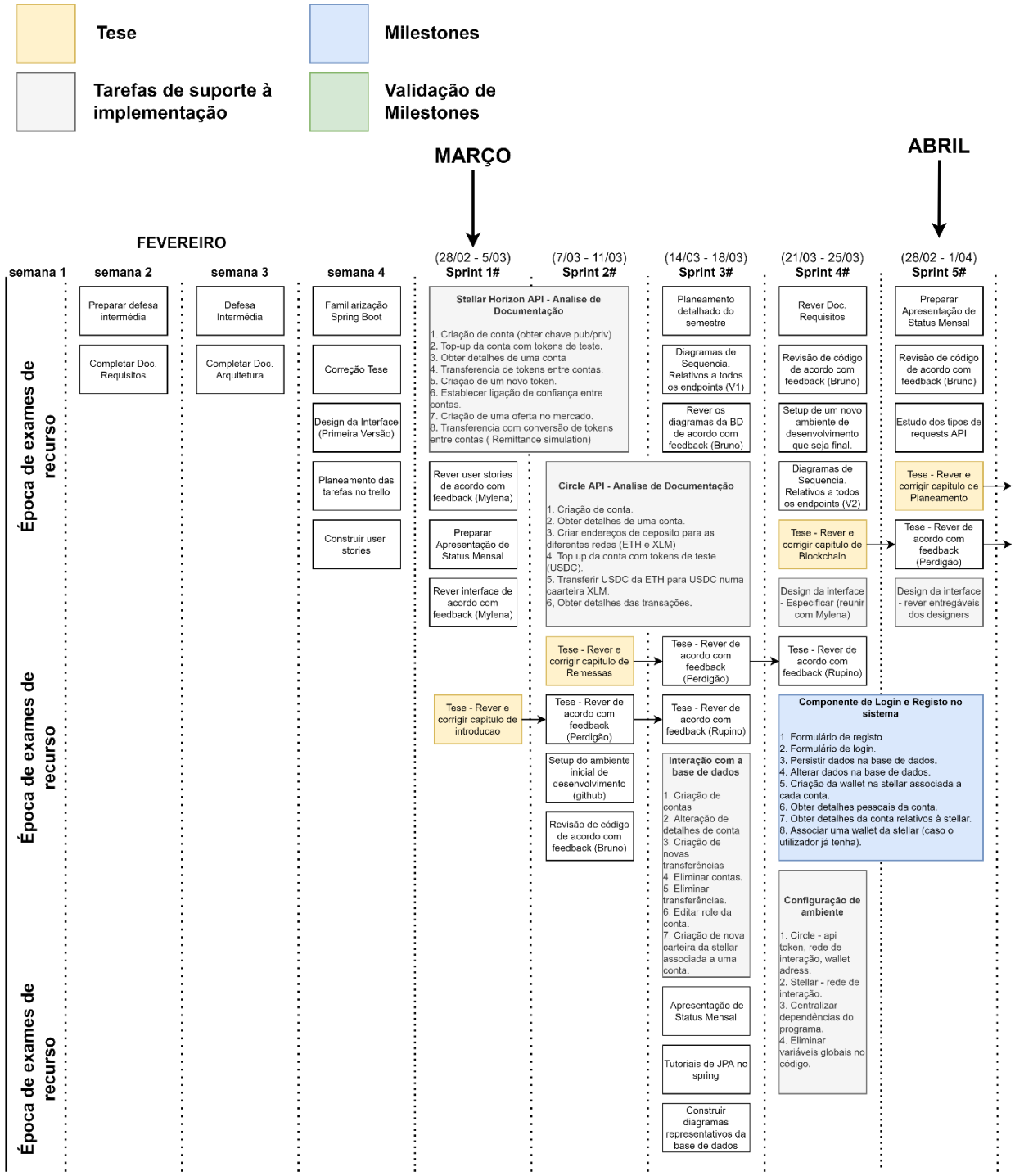


Figura 51 - Primeira parte do planeamento para o segundo semestre.

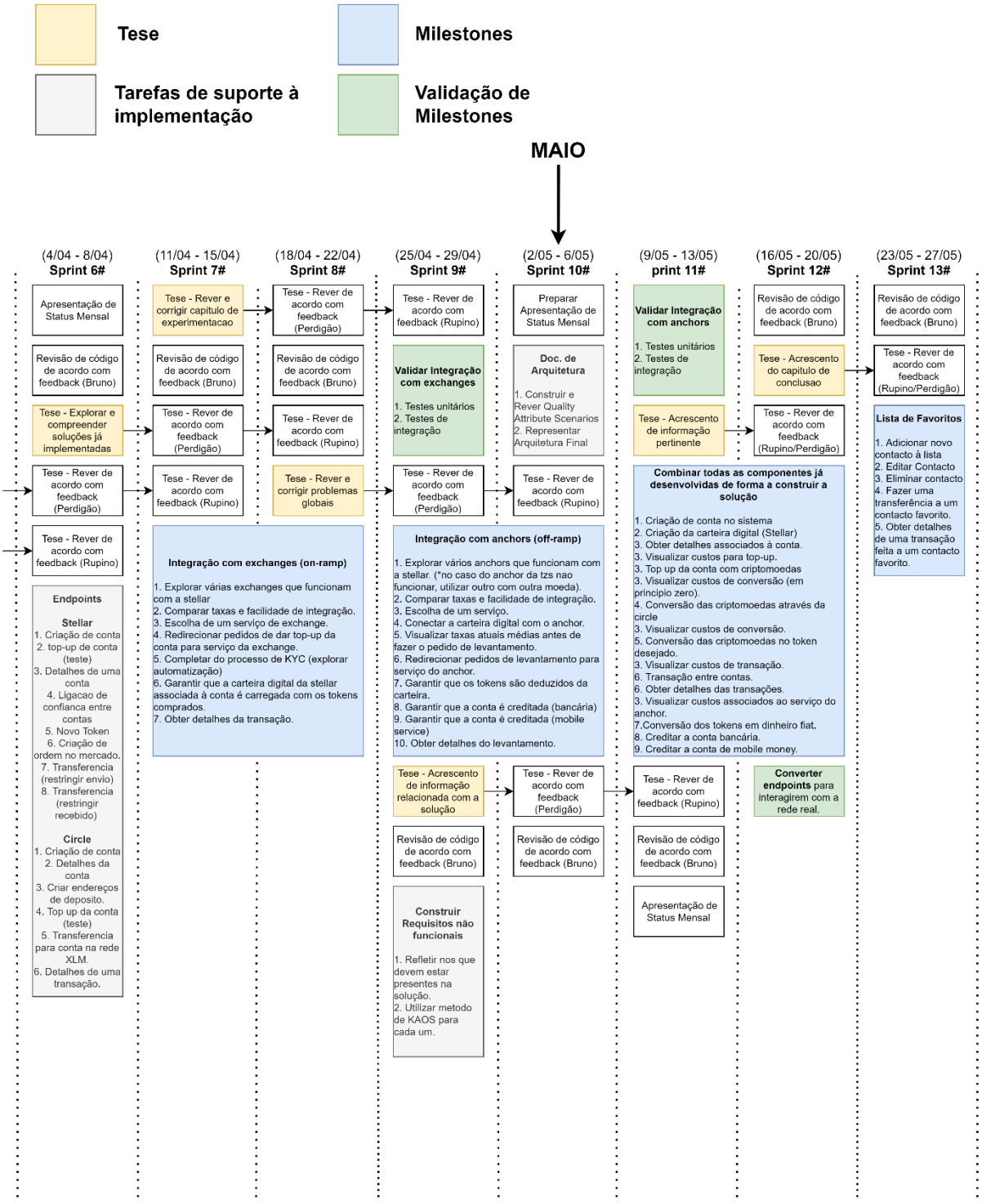


Figura 52 - Segunda parte do planeamento para o segundo semestre.

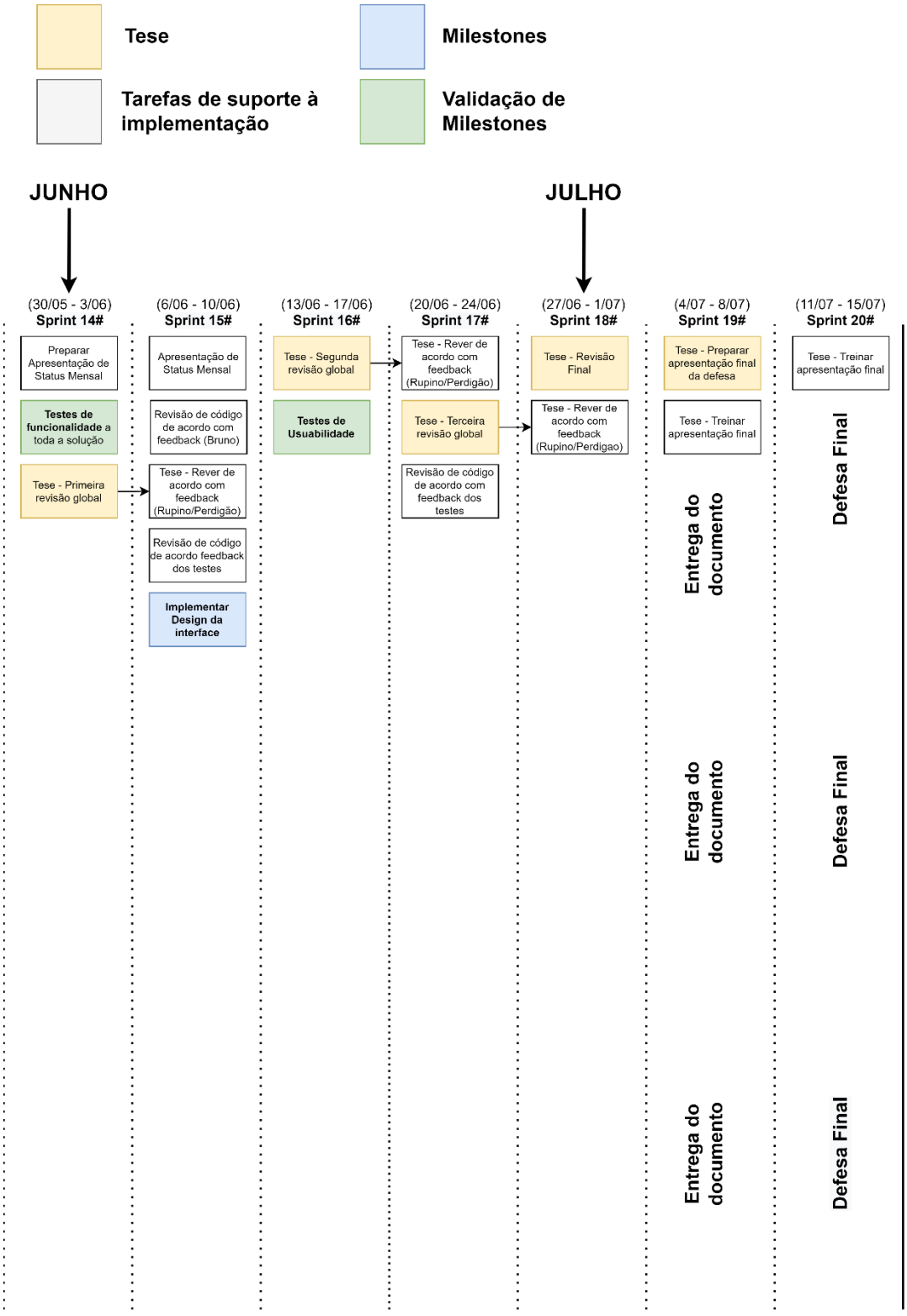


Figura 53 - Terceira e última parte do planeamento para o segundo semestre.

Descrição do Design da Aplicação

Neste apêndice, pode ver-se a transcrição do documento de descrição do design da aplicação fornecido à equipa da WIT. Este documento foi construído com apoio da analista de negócio Mylena.

1. Feature: Landing Page, Register e Login

Problem Statement:

Currently there is no way to onboard at the system.

Feature Hypothesis:

The aim of this feature is to allow users to register themselves and then login in the application in order to be able to send/receive money, check history, check account profile and managing favorites.

Benefit Hypothesis:

Better user experience in sending money internationally

Acceptance criteria:

- As user i need to be able to download the app and see the landing page with the following information's:
    1. - A commercial statement as title (such as: "The easiest way to send money")
    2. - Two buttons: One for registration and one for login.
    3. - Brand image / logo
- As user i should be able to click at "Register" and be redirected to a form screen to fulfill the following information:
    1. - Type of document (Passport or ID card) *
    2. - Document number *
    3. - First Name*; Last Name *
    4. - email (to be considered as the user login)*
    5. - password *
    6. - Phone number *
    7. - Bank account Identifier (optional)
    8. - Mobile money account identifier (optional)
    9. - Submit Button that can lead to two different scenarios:

        Error Scenario: Information inserted in form already present in database
        Success Scenario: Loading screen informing user that the crypto wallet has been created

- As user i should be able to click at "Login" and be redirected toa screen with:
    1. - 2 fields: Email; Password*
    2. - Recover Password
    3. - Submit button.*

- As user after log in successfully i should be able to see the homepage with the following options:
    1. - Account details (user profile, change password,)
    2. - Favorites
    3. - Send money
    4. - Withdraw
    5. - Transaction History

    Note: These features are only entry points to other screens that will be specified later on.

*Mandatory fields

2. Feature: Remessa Internacional (send money)

Problem Statement:

People working and living abroad who wish to send money to friends/family usually face some barriers and high costs to do that.

Feature Hypothesis:

The aim of this feature is to simplify the process of sending money and to reduce operation costs.

Benefit Hypothesis:

1. Better user experience
2. Help to reduce poverty levels by allowing users to send money internationally more frequently

Acceptance criteria:

- As user i should be able to click on the button “send money” at homepage and be redirected to a form screen with the following information:
  - Amount to be sent and its currency. (If amount is above funds in the account, a warning should appear and block user from continuing)
  - Receiver Information:
    - Choosing a contact from favorites
    - Insert manualy information:
      - Name*
      - Account Identifier*
      - Receivers Currency*
      - Submit Button.
- As user after clicking in the submit button i should be able to see “check and confirm screen”:
  - Sender Info:
    - Account Identifier
    - Amount to be send
    - Paying currency

  - Receiver Info
    - Name
    - Amount to be received.
    - Destination Currency
    - Account Identifier
  - Transaction info:
    - Total fees
    - Total costs

  Back Button

  Confirm Button that can lead to three different scenarios:

  Error Scenario 1#: Generic erro. Such as: “Something went wrong, please try again later”.

  Error Scenario 2#: Invalid receivers account id.

  Success Scenario: Transaction completed sucessfully followed by an “OK” button that lead user to homepage again.

Definição de Requisitos

Neste apêndice, pode ver-se uma transcrição do documento de definição dos requisitos para a solução criado no primeiro semestre.

1. Introdução

1.1. Objetivo

No âmbito do estágio é necessário desenvolver um protótipo que através de uma rede blockchain efetua uma conversão e transferência de dinheiro de uma conta bancária para outra conta bancária de um país localizado no continente africano. Nomeadamente com foco em reduzir custos nas transferências internacionais. Estará associado a uma aplicação móvel que mostrará, através de uma interface intuitiva, o estado da operação.

1.2. Âmbito

Que problema precisa de ser resolvido?

Em países em desenvolvimento a atividade de envio de remessas tem um enorme impacto no quotidiano, representando em média 33% de todo o dinheiro entrante nestas economias. De forma a aumentar o número de remessas enviadas é necessário procurar reduzir os custos associados a este tipo de operações.

Onde está o problema?

O problema encontra-se na organização responsável pela implementação de uma solução, a WIT Software.

De quem é o problema?

A resolução deste problema afeta os utilizadores em países desenvolvidos que procuram realizar transferências para países em desenvolvimento e utilizadores em países em desenvolvimento que pretendem ser recetores das remessas internacionais,

Porque é que o problema precisa de ser resolvido?

A atividade de envio de remessas tem um forte impacto económico no quotidiano da população em países em desenvolvimento, torna-se assim importante reduzir os custos para proporcionar melhores condições de vida. A comunidade internacional estabeleceu um objetivo até 2030 em reduzir os custos médios da

atividade de remessas até ao valor médio de 3% por transação, é importante contribuir para o concretizar deste objetivo de forma a estimular uma maior inclusão das economias dos países em desenvolvimento.

Como é que um sistema de software pode ajudar?

O processo pode ser alcançado através de uma interface gráfica para dispositivos móveis que, com uma boa componente de usabilidade, permite aos utilizadores finais realizar transferências internacionais de uma forma mais rápida e com menores custos do que serviços tradicionais disponíveis no mercado.

1. **Cenário:** A Neema encontra-se deslocada do seu país natal. Trabalha nos Estados Unidos da América há mais de 5 anos e conseguiu juntar algum dinheiro para apoiar na construção de uma nova casa para o seu pai Emmanuel. O Emmanuel precisa de pagar a primeira prestação ao engenheiro da obra em menos de 1 semana. A Neema, através da solução desenvolvida envia o dinheiro para o seu pai, com a garantia de que chega dentro do prazo a um custo baixo. O Emmanuel é notificado no momento de receção da transferência e consegue assim iniciar o processo de construção da casa.

Quando é que a solução tem que estar pronta?

Prazo final de entrega da dissertação, dia 5 de setembro de 2022.

O que pode impedir a resolução do problema?

Os fatores que mais podem dificultar a resolução deste problema são a falta de experiência do orientando nas tecnologias de desenvolvimento da solução, o prazo de entrega, uma alteração drástica dos custos das operações através da rede blockchain e a possível carência de nós na rede o que pode conduzir a um serviço mais lento ou até não operacional.

1.3. Definições, acrónimos e abreviaturas

Termo	Definição
Emissor	Utilizador que usa a solução para realizar transferências de dinheiro de um país desenvolvido para um país em desenvolvimento.
Recetor	Utilizador que usa a solução para ser notificado no momento de receção de dinheiro na sua conta bancária.
Utilizador Final	Emissor e Recetor de remessas internacionais através da solução.
WIT Software	Empresa que abriga o orientando no âmbito do estágio.
#Nxx	Id de um {use case} relativo a um utilizador não autenticado.
#Uxx	Id de um {use case} relativa a um utilizador.

2. Descrição Geral

2.1. Perspetiva do Produto

Este produto pretende permitir o envio de remessas internacionais de uma forma rápida e com custos baixos, através de uma aplicação móvel que irá informar o utilizador final do estado do processo de envio da remessa.

2.2. Funções do Produto

Nesta subsecção está presente, de uma forma simplificada, uma lista de funções disponíveis pelo sistema de forma a suportar o seu objetivo.

1. **Transferência internacional:** O emissor pode enviar dinheiro para outro país com uma moeda diferente da do recetor. Será garantido que o dinheiro irá ser creditado na conta recetora e disponível para ser gasto depois do concluir do processo de envio.
2. **Câmbio de Moeda:** A solução deve proporcionar uma forma de realizar a troca da moeda original enviada, por uma moeda que o utilizador pretenda que chegue ao destino. Limitado e de acordo com uma lista pré-definida.
3. **Taxas:** O utilizador final tem a habilidade de visualizar as taxas associadas ao serviço antes e depois de ter iniciado e realizado a transferência.

2.3. Características dos Utilizadores

Os utilizadores da plataforma são:

Emissor: Utilizador que usa a solução para enviar dinheiro de um país desenvolvido para alguém de um país em desenvolvimento, realizando uma conversão de moeda no processo.

Recetor: Utilizador que usa a solução para introduzir dados que o identificam no realizar da transferência. Pretende visualizar o estado da operação e ser notificado quando o processo é concluído.

3. Requisitos Específicos

3.1. Diagramas

Os diagramas desta secção ilustram o uso da plataforma e a interação entre os vários tipos de utilizador e o sistema.

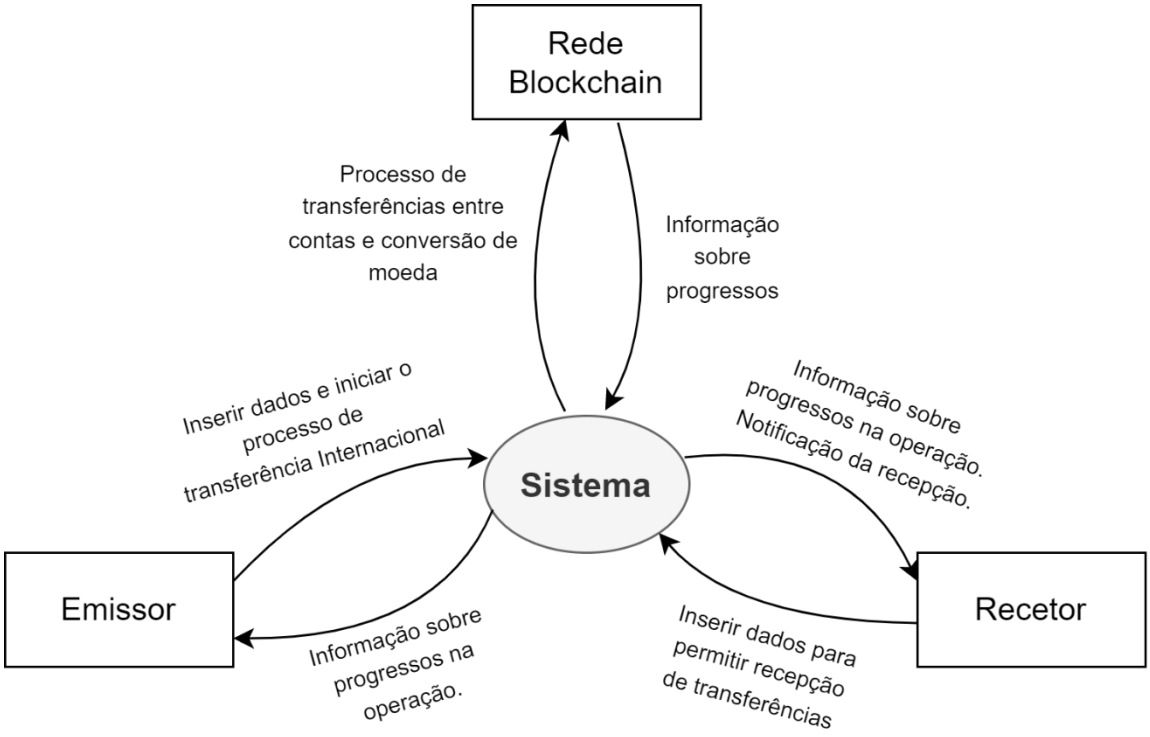


Figure 1 - Diagrama top level.

Na figura 1, pode ver-se as interações principais que o sistema irá ter com os diferentes atores e com a rede de blockchain. O sistema da solução deverá através dos dados inseridos pelo emissor iniciar o processo de transferência internacional do dinheiro, interagindo com a rede blockchain escolhida de forma transferir o dinheiro entre contas e converter a moeda para a desejada. A rede blockchain disponibiliza informação sobre o progresso da operação. O sistema deverá tratar desta informação e transmiti-la tanto para o recetor como para o emissor da remessa. O recetor deve inserir os dados necessários no sistema de forma a permitir o realizar da transferência para a sua conta bancária.

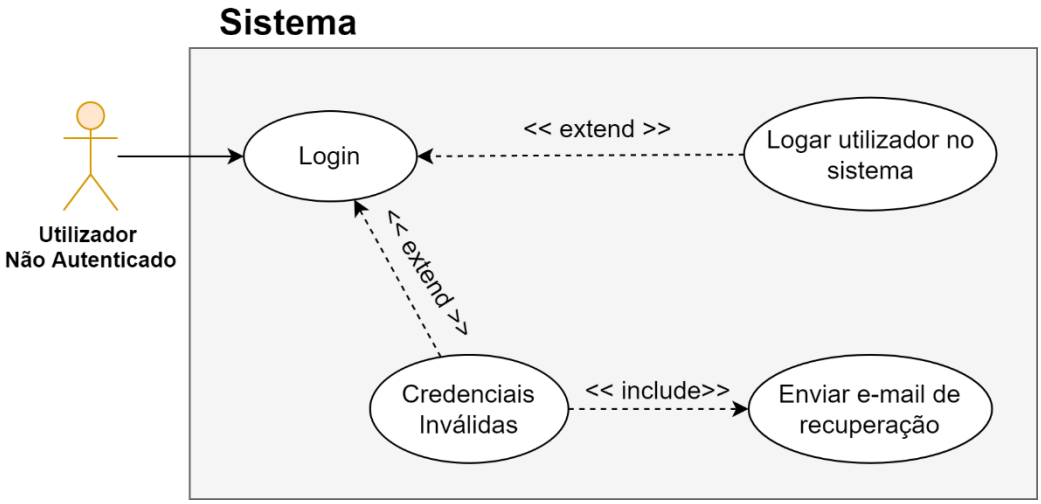


Figure 2 - Uso da plataforma por um utilizador não autenticado.

Na figura 2, pode ver-se o diagrama de caso-uso para um utilizador não autenticado da solução. O sistema irá proporcionar uma forma de autenticar todos os utilizadores de uma forma segura e protegida, sendo que apenas utilizadores autenticados devem interagir com o sistema. Caso o utilizador não se recorde das suas credenciais de acesso, através de um e-mail de recuperação, será possível alterá-las.

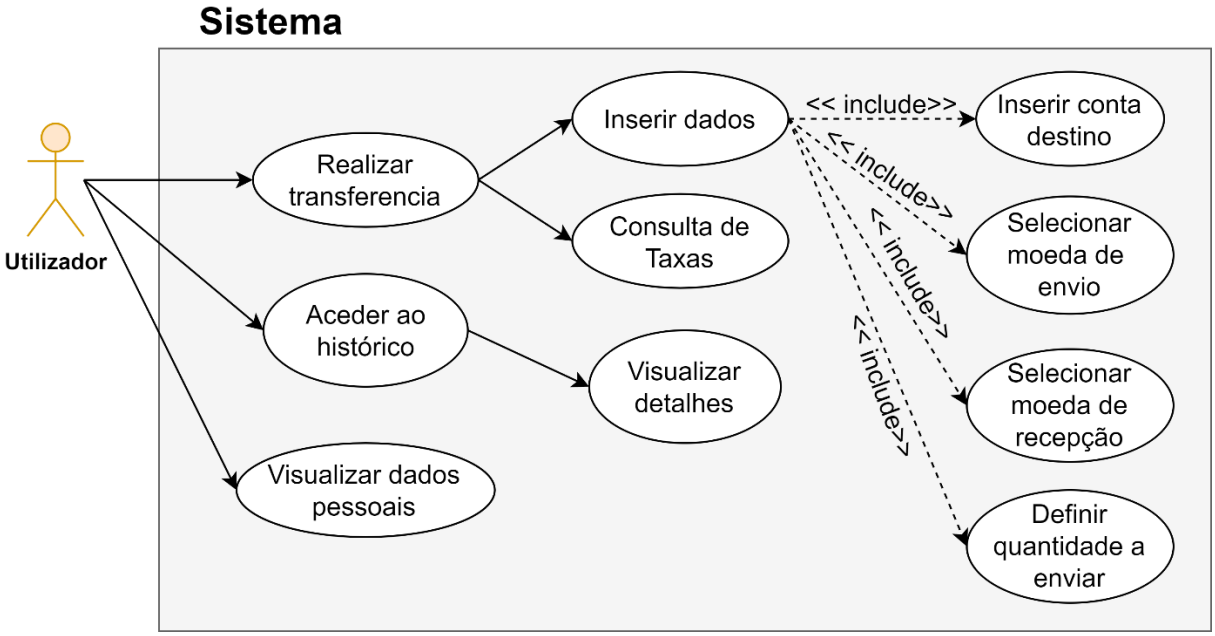


Figure 3 - Uso da plataforma por um utilizador.

Na figura 3, pode ver-se o diagrama de caso-uso para um utilizador da solução. Para o realizar de uma transferência internacional, o emissor deve inserir dados que permitam garantir o sucesso da operação, o que inclui inserir a informação relativa à conta bancária destino, selecionar da moeda e quantidade a enviar e selecionar da moeda que pretende que o recetor receba. As taxas e custos serão apresentados ao emissor de uma forma transparente até que este confirme a transação. O sistema irá permitir ao utilizador consultar o seu histórico de transferências de forma a visualizar toda a informação associada e no caso de a operação ainda não estar concluída, apresentar o progresso da operação. Será ainda possível ao utilizador visualizar e editar os seus dados pessoais, que incluem informação básica de identificação pessoal e da sua conta bancária, tanto para o recetor como para o emissor da remessa.

3.2. Requisitos Funcionais

3.2.1. Utilizador não autenticado

3.2.1.1. Use Case #N1: Fazer login

Primary Actor: Utilizador não autenticado

Scope: Aplicação móvel para transferências

Level: User Goal

Stakeholders and Interests:

Emissor – Quer realizar transferências internacionais de forma rápida e com custos baixos, visualizando todos os progressos para cada operação concretizada.

Recetor – Quer receber transferências internacionais na sua moeda local.

Precondition:

O utilizador tem acesso a um dispositivo móvel com internet.

Minimal Guarantee:

O estado do sistema não é alterado.

Success Guarantee:

O utilizador faz login no sistema e consegue aceder à sua página pessoal.

Main Success Scenario:

1. O utilizador acede à página de login da aplicação.
2. O utilizador introduz as credenciais.
3. O sistema devolve a página pessoal do utilizador.

Extensions:

1a. Existe uma quebra na conexão entre o dispositivo e o sistema.

1a1. O sistema fica inacessível e espera que haja uma reconexão do dispositivo.

2a. O utilizador não se lembra das suas credenciais.

2a1. O sistema envia um e-mail para recuperar as credenciais.

3.2.2. Utilizador

3.2.2.1. Use Case #U1: Emissor

Primary Actor: Emissor

Scope: Aplicação móvel para transferências

Level: User Goal

Stakeholders and Interests:

Emissor – Quer realizar transferências internacionais de forma rápida e com custos baixos, visualizando todos os progressos para cada operação concretizada.

Recetor – Quer receber transferências internacionais na sua moeda local.

Precondition:

O utilizador já fez login no sistema.

Minimal Guarantee:

O estado do sistema não é alterado. Não há alterações nos fundos da conta.

Success Guarantee:

O utilizador realiza a transferência. Os fundos são descontados da conta do emissor e creditados na conta do recetor.

Main Success Scenario:

1. O utilizador acede à página para realizar uma transferência internacional.
1.1. Insere a informação da conta recetora.
1.2. Escolhe a moeda a enviar, a moeda a receber e a quantidade.
2. Visualiza o total das taxas aplicadas.
3. Sistema devolve a informação resumida da transferência.
4. Utilizador confirma transferência.
5. Sistema devolve a página inicial da aplicação.

Extensions:

1a. Existe uma quebra na conexão entre o dispositivo e o sistema.

1a1. O sistema guarda a informação para uma nova tentativa. Não existem deduções ou creditações nos fundos de nenhuma conta.

2a. Cliente não tem saldo suficiente na conta para realizar a transferência.

2a1. Não existem deduções ou creditações nos fundos de nenhuma conta.

3.2.2.2. Use Case #U2: Recetor

Primary Actor: Recetor

Scope: Aplicação móvel para transferências

Level: User Goal

Stakeholders and Interests:

Emissor – Quer realizar transferências internacionais de forma rápida e com custos baixos, visualizando todos os progressos para cada operação concretizada.

Recetor – Quer receber transferências internacionais na sua moeda local.

Precondition:

O utilizador já fez login no sistema.

Minimal Guarantee:

O estado do sistema não é alterado. Não há alterações nos fundos da conta.

Success Guarantee:

O utilizador é notificado da receção de dinheiro na conta. Os fundos são creditados na sua conta bancária.

Main Success Scenario:

1. O utilizador recebe uma notificação no seu dispositivo móvel.
2. Pressiona na notificação e é redirecionado para uma página de informação relativa à transferência.
3. Confirma a receção.

4. O sistema devolve a página inicial da aplicação.

Extensions:

1a. Existe uma quebra na conexão entre o dispositivo e o sistema.

1a1. O sistema guarda a informação para uma nova tentativa. Não existem deduções ou creditações nos fundos de nenhuma conta.

2a. Cliente não tem saldo suficiente na conta para realizar a transferência.

2a1. Não existem deduções ou creditações nos fundos de nenhuma conta.

Esta página foi propositadamente deixada em branco

Especificação de Endpoints

Neste apêndice, pode ver-se uma transcrição do documento de especificação de endpoints criado com auxílio do programa PostMan de forma a enviar pedidos e captar respostas para cada um dos quinze endpoints desenvolvidos:

Autenticação

1. Registo
2. Login

Stellar

3. Criação de uma carteira
4. Associação de uma carteira
5. Desassociar uma carteira
6. Transferência (com conversão)
7. Estabelecer ligação de confiança (trustline)
8. Ativos disponíveis para levantamento
9. Informação relativa a um Anchor
10. Submeter pedido de levantamento
11. Obter preço de uma transação (sem conversão)
12. Obter preço de uma transação (com conversão)

Outros

13. Informação HomePage
14. Histórico
15. Informação sobre a carteira digital

1. Autenticação

1.1. Registo

Descrição: Endpoint para registo de novos utilizadores no sistema. É necessário enviar um pedido Json com estrutura correspondente ao objeto RegisterRequest.

Url: /react/register
Request: RegisterRequest.java
Response: HttpEntity<BaseResponse>
Http Verb: POST

Request Body:

Field Name	Type	Description
Email	String	Unique user email. (primary key in database)
ccNumber	String	Document Identifier
firstName	String	First Name
lastName	String	Last Name
password	String	Must follow certain rules. At least: One upper case, one lower case, one number.
phoneNumber	String	Phone number
accountStatus	Enum	Automatically filled. Can be changed later. {ACTIVE, BLOCKED, DELETED}
accountRole	Enum	Automatically filled. Can be changed later. {ADMIN, USER}
bankAccountId	String	Bank Account ID
mobileMoneyAccountId	String	Mobile money Account ID

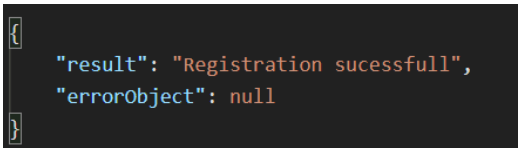
Request Body (Example):

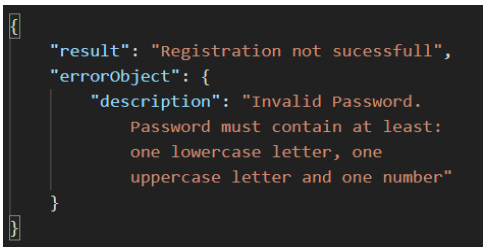
```
{
"email":"newUser@gmail.com",
"ccNumber":"asd1231das",
"firstName":"Marshall",
"lastName":"Mathers",
"password":"Slimshady1",
"phoneNumber":"+351 312 233 111",
"accountStatus":"",
"accountRole":"",
"bankAccountId":"",
"mobileMoneyAccount":""
}
```

Response Body:

Field Name	Type	Description
Header.HttpStatus	String	Http Status Code (meaning: https://www.restapitutorial.com/httpstatuscodes.html)
Body.result	String	Result of the sucess/failure in operation.
Body.ErrorObject. Description	String	Description of the reason why operation failed

Response (example):





1.2. Login

Descrição: Endpoint para autenticar utilizadores no sistema e forma a permitir com que estes usufruam das funcionalidades do sistema. É necessário enviar um pedido Json com estrutura correspondente ao objeto LoginRequest.

Url: /auth/login2
Request: LoginRequest.java
Response: HttpEntity<BaseResponse>
Http Verb: POST

Request Body:

Field Name	Type	Description
Email	String	Unique user email. (primary key in database).
password	String	Must follow certain rules. At least: One upper case, one lower case, one number.

Request Body (Example):

```
{
    "email": "yeeeesgmail.com",
    "password": "hhhh12T"
}
```

Response Body:

Field Name	Type	Description
Header.HttpStatus	String	Http Status Code (meaning: https://www.restapitutorial.com/httpstatuscodes.html)
Body.result	String	Result of the sucess/failure in operation.
Body.ErrorObject.Description	String	Description of the reason why operation failed

Response (example):

```
{
    "result": "Login sucessfull",
    "errorObject": null
}
```

```
{
    "result": "Login not sucessfull",
    "errorObject": {
        "description": "Invalid credentials"
    }
}
```

2. Stellar

2.1. Criação de uma carteira

Descrição: Endpoint que permite a utilizadores autenticados criar uma carteira digital da Stellar que ficará associada à sua conta. É necessário enviar um pedido Json com estrutura correspondente ao objeto createWalletRequest.

Url: /react/createWallet
Request: CreateWalletRequest.java
Response: HttpEntity<BaseResponse>
Http Verb: POST

Request Body:

Field Name	Type	Description
Email	String	Unique user email. (primary key in database).
password	String	Must follow certain rules. At least: One upper case, one lower case, one number.

Request Body (Example):

```
{
    "email": "sam@outlook.com",
    "password": "Qwerty123"
}
```

Response Body:

Field Name	Type	Description
Header.HttpStatus	String	Http Status Code (meaning: https://www.restapitutorial.com/httpstatuscodes.html)
Body.result	String	Result of the sucess/failure in operation.
Body.ErrorObject.Description	String	Description of the reason why operation failed

Response (example):

```
{
    "result": "New wallet created with sucess",
    "errorObject": null
}
```

```
{
    "result": "Login not sucessfull",
    "errorObject": {
        "description": "Invalid credentials"
    }
}
```

2.2. Associação de uma carteira

Descrição: Endpoint que permite a utilizadores autenticados associar uma carteira digital da Stellar que já tenham previamente. É necessário enviar um pedido Json com estrutura correspondente ao objeto ConnectWalletRequest.

Url: /react/connectWallet
Request: ConnectWalletRequest.java
Response: HttpEntity<BaseResponse>
Http Verb: POST

Request Body:

Field Name	Type	Description
Email	String	Unique user email. (primary key in database).
password	String	Must follow certain rules. At least: One upper case, one lower case, one number.
secretKey	String	Secret seed associated with user wallet. Necessary to reconstruct the object Keypair that will be used to sign transactions.

Request Body (Example):

```
{
    "email": "u@hotmail.com",
    "password": "turimS123",
    "secretKey":"SBCEQD7UFFEP5RK4XNHVLCHTDFUAU3RITQHB
        ISZSELI3YGL73T23BQ3G"
}
```

Response Body:

Field Name	Type	Description
Header.HttpStatus	String	Http Status Code (meaning: https://www.restapitutorial.com/httpstatuscodes.html)
Body.result	String	Result of the sucess/failure in operation.
Body.ErrorObject.Description	String	Description of the reason why operation failed

Response (example):

```
{
    "result": "New wallet created with sucess",
    "errorObject": null
}
```

2.3. Desassociar de uma carteira

Descrição: Endpoint que permite a utilizadores autenticados desassociar uma carteira digital da Stellar que já tenham previamente associado no sistema. É necessário enviar um pedido Json com estrutura correspondente ao objeto DeleteWalletRequest.

Url: /react/deleteWallet
Request: DeleteWalletRequest.java
Response: HttpEntity<BaseResponse>
Http Verb: POST

Request Body:

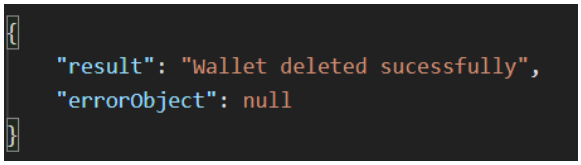
Field Name	Type	Description
Email	String	Unique user email. (primary key in database).
password	String	Must follow certain rules. At least: One upper case, one lower case, one number.

Request Body (Example):

Response Body:

Field Name	Type	Description
Header.HttpStatus	String	Http Status Code (meaning: https://www.restapitutorial.com/httpstatuscodes.html)
Body.result	String	Result of the sucess/failure in operation.
Body.ErrorObject.Description	String	Description of the reason why operation failed

Response (example):



2.4. Transferência

Descrição: Endpoint que permite a utilizadores realizar transferências que podem ou no envolver câmbio de moeda. É necessário enviar um pedido Json com estrutura correspondente ao objeto PathTransactionRequest.

Url: /react/sendPathTransaction
Request: PathTransactionRequest.java
Response: HttpEntity<BaseResponse>
Http Verb: POST

Request Body:

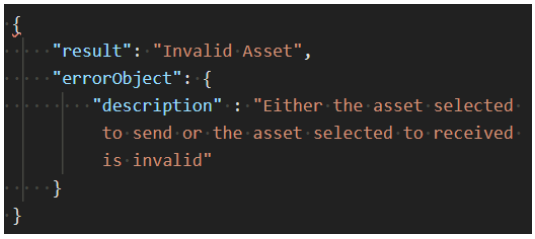
Field Name	Type	Description
senderEmail	String	Unique user email. (primary key in database).
currencySent	String	Name of currency sent
maxSentAmount	Float	Max amount use is willing to pay for transaction
currencyReceived	String	Name of currency user wants receiver to get
amontOfCurrencyReceived	String	Amount of currency user wants receiver to get
receiverName	String	Transaction name of receiver
receiverWalletAddr	String	Identifier for digital wallet of receiver
transactionFee	String	(*filled later) transaction network cost
transactionCost	String	(*filled later) the amount user has to pay
transactionDate	String	(*filled later) Date and time of transaction

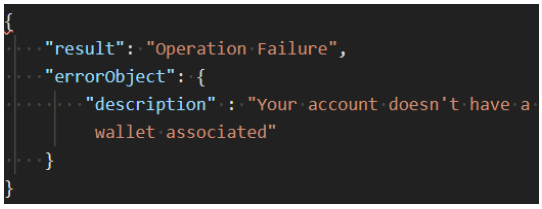
Request Body (Example):

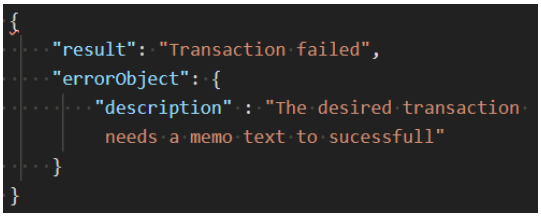
Response Body:

Field Name	Type	Description
Header.HttpStatus	String	Http Status Code (meaning: https://www.restapitutorial.com/httpstatuscodes.html)
Body.result	String	Result of the sucess/failure in operation.
Body.ErrorObject.Description	String	Description of the reason why operation failed

Response (example):







2.5. Establecer uma ligação de confiança (trustline)

Descrição: Endpoint que permite a utilizadores estabelecer uma ligação de confiança com determinado token, simbolizando a confiança que este tem no mesmo, ou seja, encontra-se recetível e aceita o seu valor. É necessário enviar um pedido Json com estrutura correspondente ao objeto TrustlineRequest.

Url: /react/establishTrustline
Request: TrustlineRequest.java
Response: HttpEntity<BaseResponse>
Http Verb: POST

Request Body:

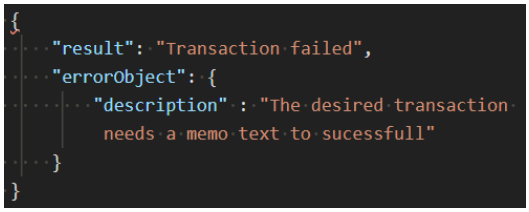
Field Name	Type	Description
email	String	Unique user email. (primary key in database).
assetName	String	Name of currency to trust

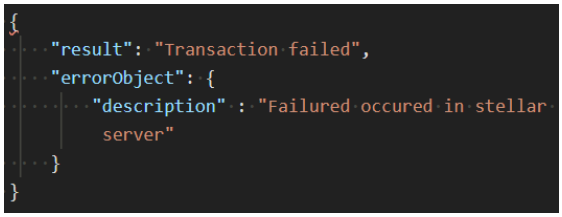
Request Body (Example):

Response Body:

Field Name	Type	Description
Header.HttpStatus	String	Http Status Code (meaning: https://www.restapitutorial.com/httpstatuscodes.html)
Body.result	String	Result of the sucess/failure in operation.
Body.ErrorObject.Description	String	Description of the reason why operation failed

Response (example):





2.6. Ativos disponíveis para levantamento

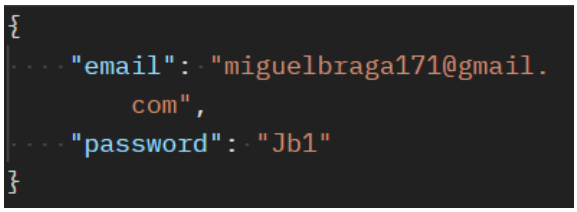
Descrição: Endpoint que devolve à aplicação uma lista de ativos passiveis a levantamento para uma conta *mobile money* ou conta bancária dentro da lista de ativos que o utilizador possui.

Url: /react/assetsToWithdraw
Request: TrustlineRequest.java
Response: HttpEntity<AccountAssetList>
Http Verb: POST

Request Body:

Field Name	Type	Description
email	String	Unique user email. (primary key in database).
assetName	String	Name of currency to trust

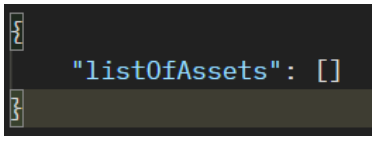
Request Body (Example):

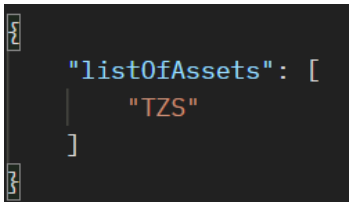


Response Body:

Field Name	Type	Description
listOfAssets	List<String>	List of current user assets that can be withdrawn

Response (example):





2.7. Informação relativa a um Anchor

Descrição: Endpoint que devolve toda a informação de uma entidade Anchor na rede Stellar para permitir que o processo de levantamento seja concretizável.

Url: /react/ fetchAnchorInfo
Request: WithdrawRequest.java
Response: HttpEntity<Sep6KycRequest>
Http Verb: POST

Request Body:

Field Name	Type	Description
amount	String	Amount of currency to withdraw
asset	String	Name of currency to withdraw
email	String	Unique user email. (primary key in database).
type	String	Identifies if account to withdraw is a Bank or mobile money
destination	String	Bank/Mobile Money account identifier
bankRounting	String	In case of a bank account, bank rounting is needed

Request Body (Example):

```
{
    "amount": "10",
    "asset": "TZS",
    "email": "rodrigo@gmail.com",
    "type": "bank",
    "destination": "9122331",
    "bankRounting": "12312321"
}
```

Response Body:

Field Name	Type	Description
kycFields	List<String>	List of KYC fields that Anchor needs to validate user.
kycValues	String[]	List of KYC values that Anchor needs to validate user.
email	String	Unique user email. (primary key in database).
authToken	String	Authentication token used in comunication between use rand anchor.
sep6Url	String	Anchor endpoint to send withdraw requests
anchorOrgName	String	Anchor official organization name
kycUrl	String	Anchor endpoint to validate user KYC values
kycNeeded	Boolean	“True” if it is the first time user comunicates with anchor.
amount	String	Amount of currency to withdraw
asset	String	Name of currency to withdraw
type	String	Identifies if account to withdraw is a Bank or Mobile money
destination	String	Bank/Mobile Money account identifier
totalSent	String	Total amount sent to bank/mobile account after fees
fee	String	Anchor fees
bankRouting	String	In case of a bank account, bank rounting is needed

Response (example):


```
{
    "kycFields":["mobile_number","first_name"],
    "kycValues":["+351911713676","José"],
    "email": "rodrigo@gmail.com",
    "authToken":"56GDDSASTTHHTSSASD",
    "sep6Url":"https://connect.clickpesa.com/sep6",
    "anchorOrgName":"ClickPesa Limited",
    "kycUrl":"https://connect.clickpesa.com/sep12",
    "kycNeeded":"False",
    "amount": "25",
    "asset": "TZS",
    "type": "bank",
    "destination": "9122331",
    "totalSent":"20",
    "fee":"5",
    "bankRounting": "12312321"
}
```

2.8. Submeter pedido de levantamento

Descrição: Endpoint para realizar um levantamento de um ativo.

Url: /react/submitWithdrawRequest
Request: Sep6KycRequest.java
Response: HttpEntity<BaseResponse>
Http Verb: POST

Request Body:

Field Name	Type	Description
kycFields	List<String>	List of KYC fields that Anchor needs to validate user.
kycValues	String[]	List of KYC values that Anchor needs to validate user.
email	String	Unique user email. (primary key in database).
authToken	String	Authentication token used in comunication between use rand anchor.
sep6Url	String	Anchor endpoint to send withdraw requests
anchorOrgName	String	Anchor official organization name
kycUrl	String	Anchor endpoint to validate user KYC values
kycNeeded	Boolean	“True” if it is the first time user comunicates with anchor.
amount	String	Amount of currency to withdraw
asset	String	Name of currency to withdraw
type	String	Identifies if account to withdraw is a Bank or Mobile Money
destination	String	Bank/Mobile Money account identifier
totalSent	String	Total amount sent to bank/mobile account after fees
fee	String	Anchor fees
bankRouting	String	In case of a bank account, bank rounting is needed

Request Body (Example):

```
{
    "kycFields":["mobile_number","first_name"],
    "kycValues":["+351911713676","José"],
    "email": "rodrigo@gmail.com",
    "authToken":"56GDDSASTTHHTSSASD",
    "sep6Url":"https://connect.clickpesa.com/sep6",
    "anchorOrgName":"ClickPesa Limited",
    "kycUrl":"https://connect.clickpesa.com/sep12",
    "kycNeeded":"False",
    "amount": "25",
    "asset": "TZS",
    "type": "bank",
    "destination": "9122331",
    "totalSent":"20",
    "fee":"5",
    "bankRounting": "12312321"
}
```

Response Body:

Field Name	Type	Description
Header.HttpStatus	String	Http Status Code (meaning: https://www.restapitutorial.com/httpstatuscodes.html)
Body.result	String	Result of the sucess/failure in operation.
Body.ErrorObject. Description	String	Description of the reason why operation failed

Response (Example):

```
{
    "result": "Withdraw was sucessfull",
    "errorObject": null
}
```

```
{
    "result": "Not enought funds",
    "errorObject": {
        "description": "Not enought TZS to withdraw"
    }
}
```

2.9. Obter preço de uma transação (sem conversão)

Descrição: Endpoint para obter preço de uma transação direta que não envolve conversão de moeda.

Url: /react/fetchDirectSendCost
Request: PathTransactionRequest.java
Response: HttpEntity<PathTransactionRequest>
Http Verb: POST

Request Body:

Field Name	Type	Description
senderEmail	String	Unique user email. (primary key in database).
currencySent	String	Name of currency sent
maxSentAmount	Float	(empty)
currencyReceived	String	(empty)
amontOfCurrencyReceived	String	(empty)
receiverName	String	Transaction name of receiver
receiverWalletAddr	String	Identifier for digital wallet of receiver
transactionFee	String	(*filled later) transaction network cost
transactionCost	String	(*filled later) the amount user has to pay
transactionDate	String	(*filled later) Date and time of transaction

Request Body (Example):

```
{
    "senderEmail": "miguelbraga171@gmail.com",
    "currencySent":"XLM",
    "maxSentAmount":"10.5",
    "currencyReceived":null,
    "amountOfCurrencyReceived":null,
    "receiverName":"Rodrigo",
    "receiverWalletAddr":"GALN3WBCXZXFEQRBP4V57JDPF44KWHBO7R3ZF7
        RDEEDEZG5L7U6SPGOY",
    "transactionFee":null,
    "transactionCost":null,
    "transactionDate":null
}
```

Response Body:

Field Name	Type	Description
senderEmail	String	Unique user email. (primary key in database).
currencySent	String	Name of currency sent
maxSentAmount	Float	(empty)
currencyReceived	String	(empty)
amontOfCurrencyReceived	String	(empty)
receiverName	String	Transaction name of receiver
receiverWalletAddr	String	Identifier for digital wallet of receiver
transactionFee	String	Transaction network cost
transactionCost	String	Amount user has to pay (total cost)
transactionDate	String	Date and time of transaction

Response (Example):


```
{
    "senderEmail": "miguelbraga171@gmail.com",
    "currencySent":"XLM",
    "maxSentAmount":"10.5",
    "currencyReceived":null,
    "amountOfCurrencyReceived":null,
    "receiverName":"Rodrigo",
    "receiverWalletAddr":"GALN3WBCXZXFEQRBP4V57JDPF44KWHBO7R3ZF7
        RDEEDEZG5L7U6SPGOY",
    "transactionFee":"10.50001025",
    "transactionCost":"1025",
    "transactionDate":"2022/06/24 15:41:37"
}
```

2.10. Obter preço de uma transação (com conversão)

Descrição: Endpoint para obter preço de uma transação que envolve conversão de moeda.

Url: /react/fetchPathSendCost
Request: PathTransactionRequest.java
Response: HttpEntity<PathTransactionRequest>
Http Verb: POST

Request Body:

Field Name	Type	Description
senderEmail	String	Unique user email. (primary key in database).
currencySent	String	Name of currency sent
maxSentAmount	Float	Maximum cost of the operation
currencyReceived	String	Name of currency received
amontOfCurrencyReceived	String	Amount of currency received
receiverName	String	Transaction name of receiver
receiverWalletAddr	String	Identifier for digital wallet of receiver
transactionFee	String	(*filled later) transaction network cost
transactionCost	String	(*filled later) the amount user has to pay
transactionDate	String	(*filled later) Date and time of transaction

Request Body (Example):

```
{
    "senderEmail": "miguelbraga171@gmail.com",
    "currencySent":"XLM",
    "maxSentAmount":"25",
    "currencyReceived":"TZS",
    "amountOfCurrencyReceived":"150",
    "receiverName":"Rodrigo",
    "receiverWalletAddr":"GALN3WBCXZXFEQRBP4V57JDPF44KWHBO7R3ZF7
        RDEEDEZG5L7U6SPGOY",
    "transactionFee":"null",
    "transactionCost":"null",
    "transactionDate":"null"
}
```

Response Body:

Field Name	Type	Description
senderEmail	String	Unique user email. (primary key in database).
currencySent	String	Name of currency sent
maxSentAmount	Float	Maximum cost of the operation
currencyReceived	String	Name of currency received
amontOfCurrencyReceived	String	Amount of currency received
receiverName	String	Transaction name of receiver
receiverWalletAddr	String	Identifier for digital wallet of receiver
transactionFee	String	Transaction network cost
transactionCost	String	Amount user has to pay (total cost)
transactionDate	String	Date and time of transaction

Response Body (Example):


```
{
    "senderEmail": "miguelbraga171@gmail.com",
    "currencySent":"XLM",
    "maxSentAmount":"25",
    "currencyReceived":"TZS",
    "amountOfCurrencyReceived":"150",
    "receiverName":"Rodrigo",
    "receiverWalletAddr":"GALN3WBCXZXFEQRBP4V57JDPF44KWHBO7R3ZF7
        RDEEDEZG5L7U6SPGOY",
    "transactionFee":"3075",
    "transactionCost":"12.0003075",
    "transactionDate":"2022/06/24 15:41:37"
}
```

3. Outros

3.1. Informação da HomePage

Descrição: Endpoint que permite obter toda a informação relativa a um utilizador de forma a construir o ecrã de homepage.

Url: /react/home
Request: SessionRequest.java
Response: HttpEntity<HomeResponse>
Http Verb: POST

Request Body:

Field Name	Type	Description
Email	String	Unique user email. (primary key in database).
password	String	Must follow certain rules. At least: One upper case, one lower case, one number.

Request Body (Example):

```
{
    "email": "sam@outlook.com",
    "password": "Qwerty123"
}
```

Response Body:

Field Name	Type	Description
isAdmin	Boolean	Determines if current user has admin privileges
hasWallet	Boolean	Determines if current user has an wallet associated
accountAssets	List<AccountAssets>	List of assets with corresponding amounts.

Response Body (Example):

3.2. Histórico

Descrição: Endpoint que permite obter todo o histórico

Url: /react/history
Request: SessionRequest.java
Response: HttpEntity<TransactionHistory>
Http Verb: POST

Request Body:

Field Name	Type	Description
Email	String	Unique user email. (primary key in database).
password	String	Must follow certain rules. At least: One upper case, one lower case, one number.

Request Body (Example):

Response Body:

Field Name	Type	Description
listOfTransactions	List<SystemTransaction>	List of all user transactions
accountId	String	User wallet address

Response Body (Example):


```
"listOfTransactions": [
    {
        "id": 1,
        "amountSent": 0.65,
        "currencySent": "XLM",
        "amountReceived": 0.65,
        "transactionFee": 1025.0,
        "currencyReceived": "XLM",
        "transactionDate": "2022/06/24 15:41:37",
        "receiverName": "Rodrigo",
        "receiverWalletAddr":
            "GDY4A3FJXOK3OSOWIQYHT6SBPXN5LJZZOMVGTX34ITQM46Z
            4GZ6EGW5T",
        "transactionState": "Sucessfull transaction",
        "userEmail": "miguelbraga171@gmail.com",
        "user": null
    }
```


3.3. Informação da Carteira Digital

Descrição: Endpoint que permite obter toda a informação da carteira digital do utilizador.

Url: /react/walletData
Request: SessionRequest.java
Response: HttpEntity<walletData>
Http Verb: POST

Request Body:

Field Name	Type	Description
Email	String	Unique user email. (primary key in database).
password	String	Must follow certain rules. At least: One upper case, one lower case, one number.

Request Body (Example):


```
{
    "email": "sam@outlook.com",
    "password": "Qwerty123"
}
```

Response Body:

Field Name	Type	Description
accountId	String	User wallet address
publicKey	String	User wallet public key
privateKey	String	User wallet private key
createdAt	String	Creation date of wallet

Response Body (Example):


```
{
    "accountId":
        "GB6R75ZGHM2EJWIBR3HOJGJLX4AMOEE6POPMXGCTCG3TOPQW6WZH7N2
        5",
    "publicKey": "fR/3Jjs0RNkBjs7kmSu/AMcQnnuey5hTEbc3Phb1sn8=",
    "privateKey":
        "SB5TXVFCRVD4R3FJH2VYOWZ5ZYU32DQK2O4QWWZYJZWVQCWAUFMKSXZ
        L",
    "createdAt": "2022/06/24 12:45:45"
}
```

Diagramas de Sequência

Neste apêndice, pode ver-se os diagramas de sequência que descrevem todas as operações possíveis de realizar na solução desenvolvida:

1. Login.
2. Registo.
3. Criar carteira digital.
4. Associar carteira digital.
5. Desassociar carteira digital.
6. Visualizar histórico.
7. Estabelecer uma ligação de confiança com um token (trustline).
8. Transferência.
9. Levantamento.

1. Login

Na figura 50, pode ver-se o diagrama de sequência para a operação login que segue os seguintes passos:

- Utilizador submete um formulário com as suas credências.
- Verifica-se se existe uma correspondência das credenciais na base de dados.
- Caso exista, o utilizador é autenticado. Caso contrário, uma mensagem de erro surge ao utilizador.

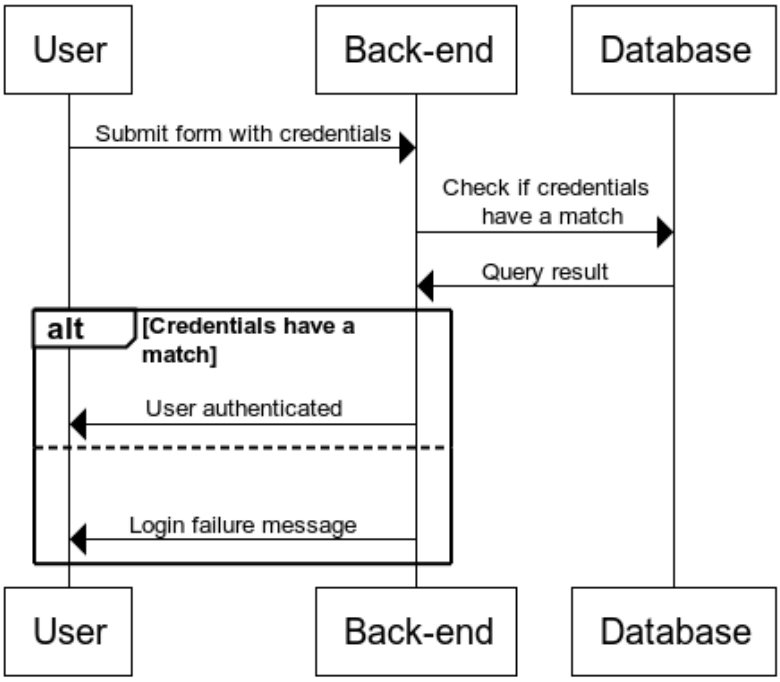


Figura 54 - Diagrama de sequência para o login.

2. Registo

Na figura 51, pode ver-se o diagrama de sequência para a operação de registo que segue os seguintes passos:

- Utilizador submete um formulário com a informação de registo.
- Os valores submetidos são validados (ex: Garantir que o número inserido é válido, garantir que não existem valores nulos). Se isto não se verificar, uma mensagem de erro surge ao utilizador.
- Como o email é utilizado como identificador único na solução é verificado se existe um duplicado na base de dados.
- Caso seja único, o registo é realizado com sucesso. Caso contrário, uma mensagem de erro surge ao utilizador.

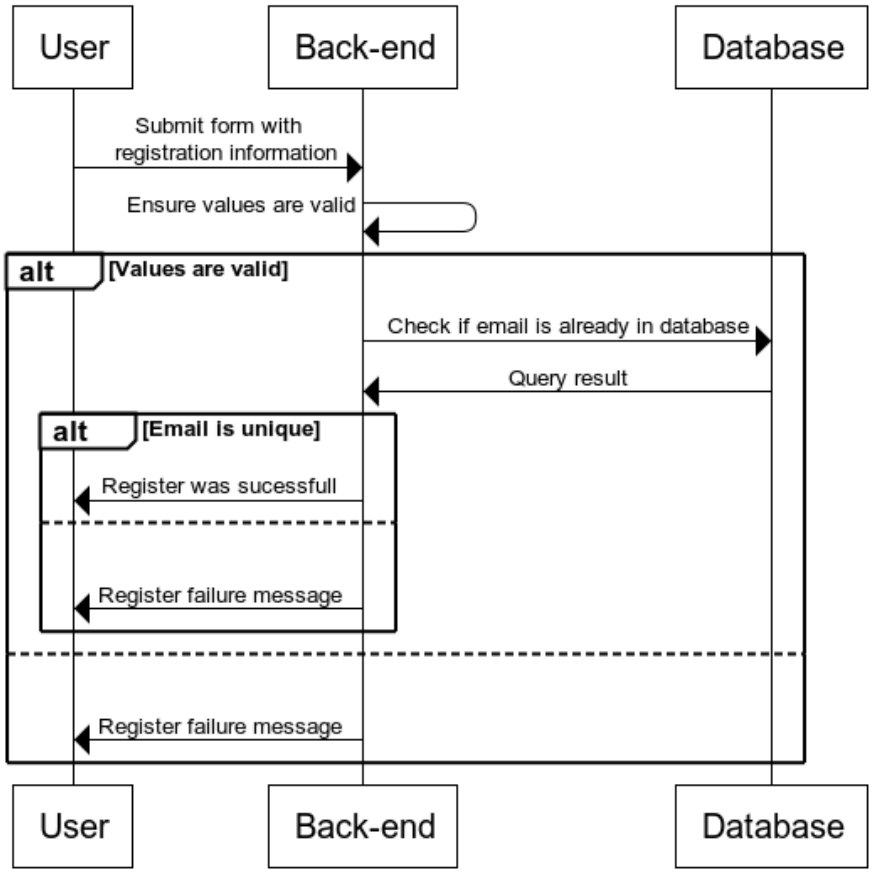


Figura 55 - Diagrama de sequência para o registo.

3. Criar uma carteira digital

Na figura 52, pode ver-se o diagrama de sequência para a operação de criação de uma carteira digital que segue os seguintes passos:

- O utilizador envia o pedido de criação para a sua carteira digital.
- O back-end utiliza o SDK para criar uma carteira digital na rede Stellar.
- A rede devolve as informações relativas à carteira criada.
- As informações são persistidas na base de dados e uma mensagem de sucesso na operação é transmitida ao utilizador.

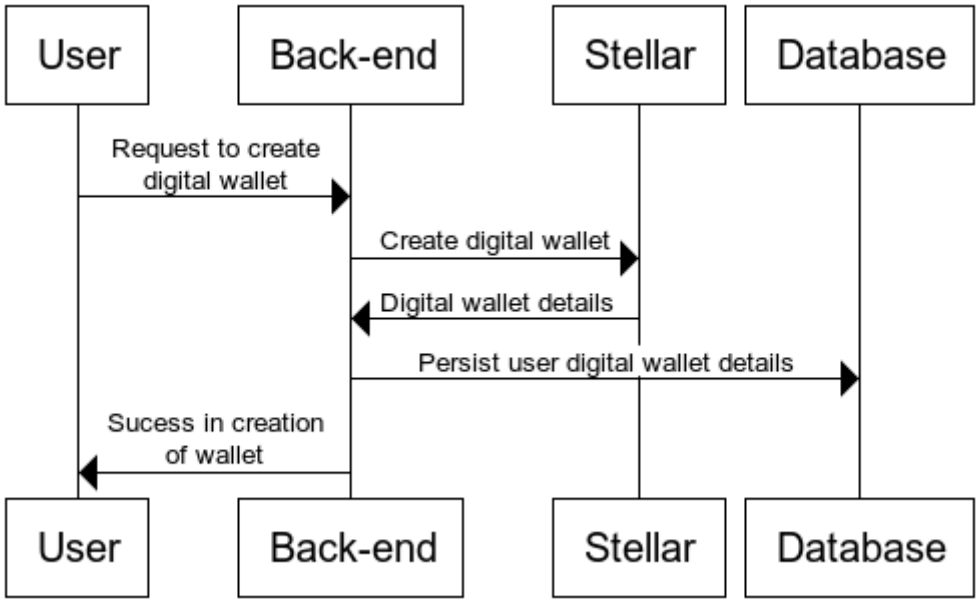


Figura 56 - Diagrama de sequência para a criação de uma carteira digital.

4. Associar uma carteira digital

Na figura 53, pode ver-se o diagrama de sequência para a operação de associar uma carteira digital que segue os seguintes passos:

- Utilizador submete a chave privada da carteira digital previamente existente.
- Um pedido é enviado à rede Stellar para verificar se a chave possui correspondência.
- Caso haja correspondência, a restante informação da carteira é enviada e persistida na base de dados. Caso contrário, uma mensagem de erro surge ao utilizador.

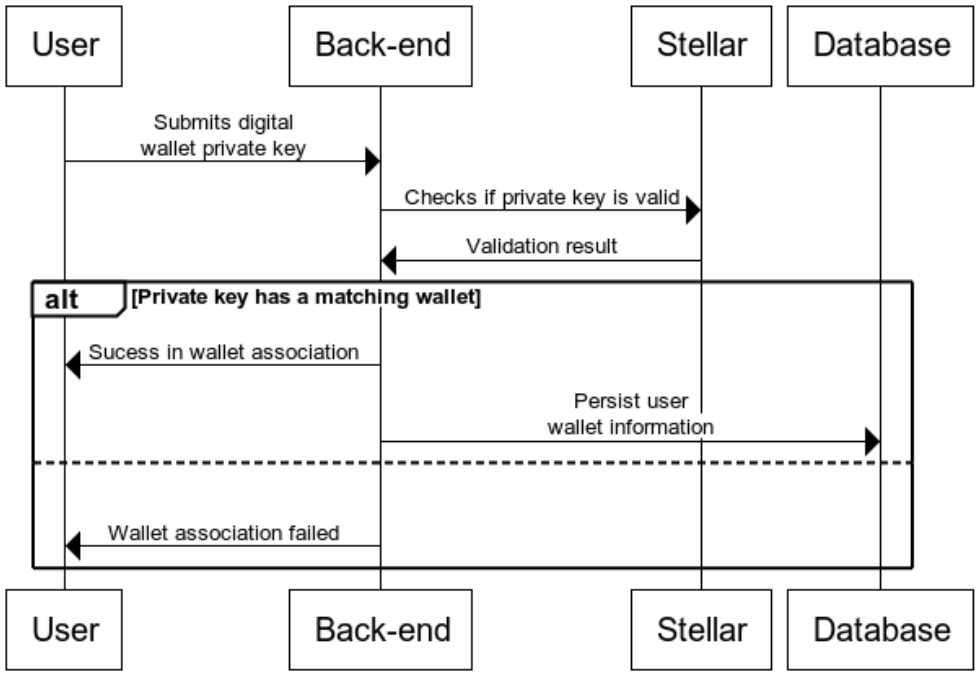


Figura 57 - Diagrama de sequência para associar uma carteira digital.

5. Desassociar uma carteira digital

Na figura 54, pode ver-se o diagrama de sequência para a operação de desassociação de uma carteira digital que segue os seguintes passos:

- O utilizador envia um pedido para desassociar a sua carteira digital da solução.
- Os valores presentes na base de dados relativos à carteira digital do utilizador são eliminados.
- Uma mensagem de sucesso surge ao utilizador.

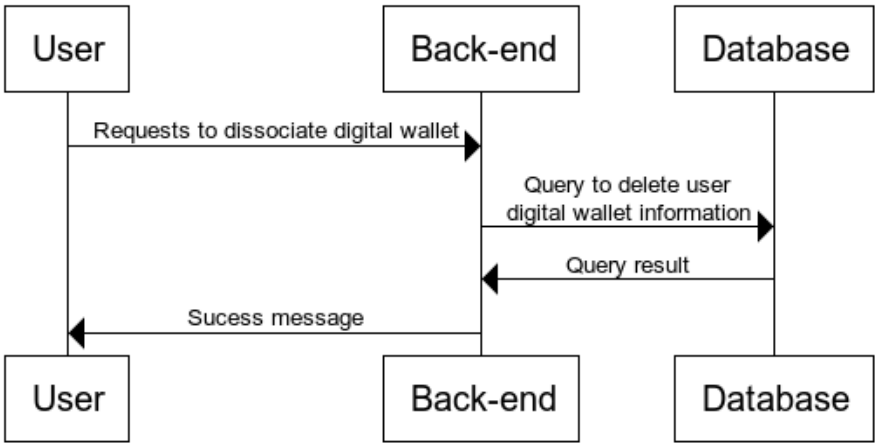


Figura 58 - Diagrama de sequência para desassociar uma carteira digital.

6. Visualizar histórico

Na figura 55, pode ver-se o diagrama de sequência para a operação de visualização do histórico que segue os seguintes passos:

- O utilizador faz um pedido para visualizar o seu histórico de transações.
- É feita uma pesquisa na base de dados por todas as transações que envolvem o utilizador.
- A lista resultado é devolvida ao utilizador.

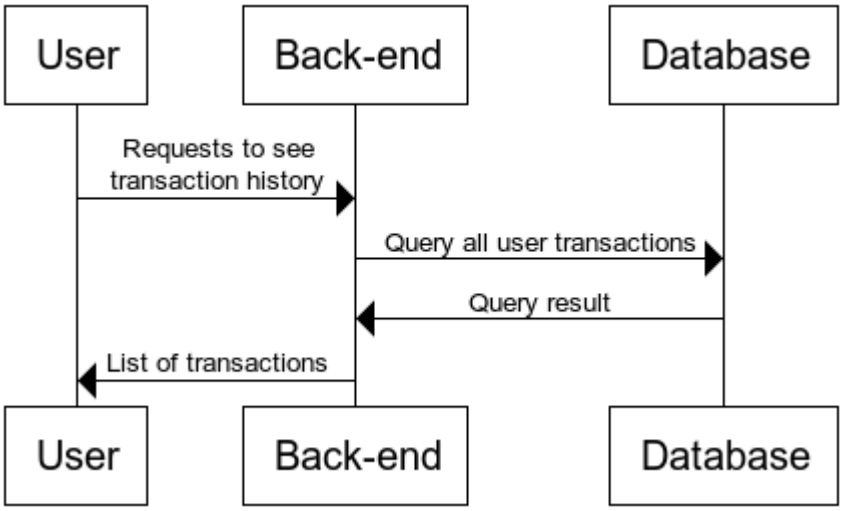


Figura 59 - Diagrama de sequência para visualizar histórico.

7. Estabelecer uma ligação de confiança com um token (trustline)

Na figura 56, pode ver-se o diagrama de sequência para a operação para estabelecer uma ligação de confiança com um token (trustline) que segue os seguintes passos:

- Utilizador realiza um pedido para confiar num token.
- A existência do token na rede a partir do identificador enviado pelo utilizador é validado na rede Stellar que posteriormente devolve um resultado.
- Caso o token seja válido, é realizada uma operação para estabelecer a ligação de confiança (trustline) e submetida à rede. A resposta é transmitida ao utilizador. Caso contrário, surge ao utilizador uma mensagem de erro.

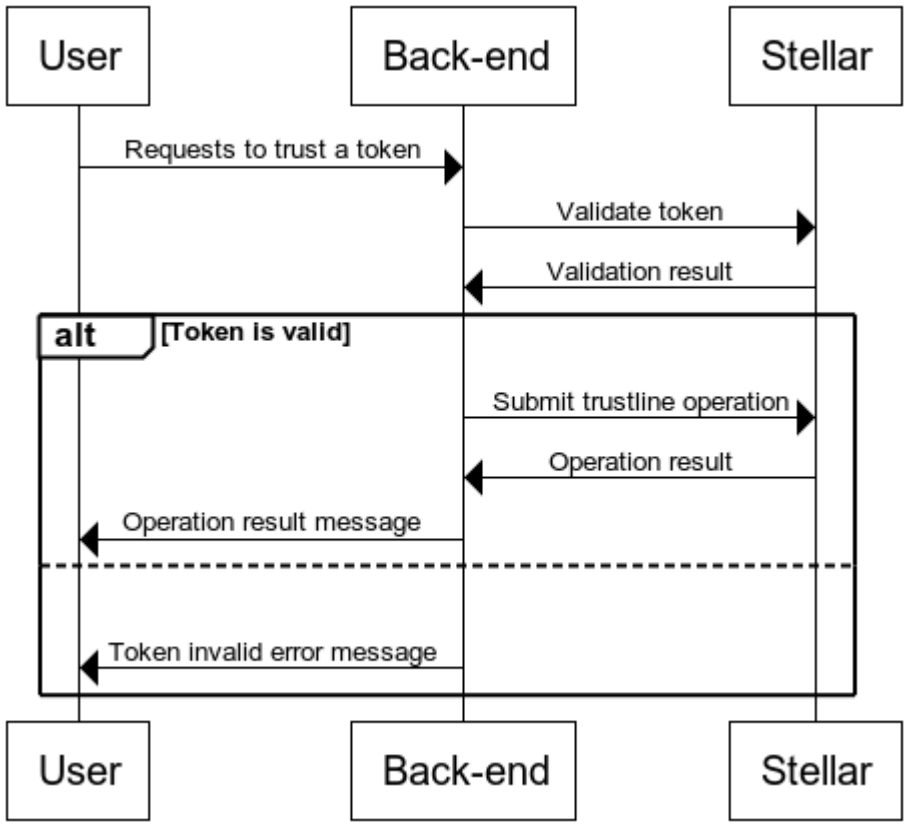


Figura 60 - Diagrama de sequência para estabelecer uma ligação de confiança com um token.

8. Transferência

Na figura 57, pode ver-se o diagrama de sequência para a operação de transferência de fundos que segue os seguintes passos:

- Preenchimento e submissão de um formulário pelo utilizador onde lhe é pedido que insira os valores associados à transferência.
- É gerado um pedido composto pelos valores preenchidos e enviado para o endpoint no back-end.
- É realizada uma validação inicial de forma a garantir que não se encontram presentes valores nulos ou inválidos. Caso o formulário esteja nos conformes, é que o processo de transferência continua e são enviados vários pedidos à rede Stellar de forma a validar os valores no formulário.
- Caso todas as condições sejam validadas, um pedido final é realizado à rede Stellar para obter o custo da operação. O custo é depois apresentado ao utilizador.
- Com esta informação, o utilizador pode ou não confirmar o pedido. Caso confirme, o *back-end* do sistema constrói a transação, submete na rede Stellar e os dados relativos à mesma são persistidos na base de dados.
- No final, o utilizador é informado do sucesso da operação.

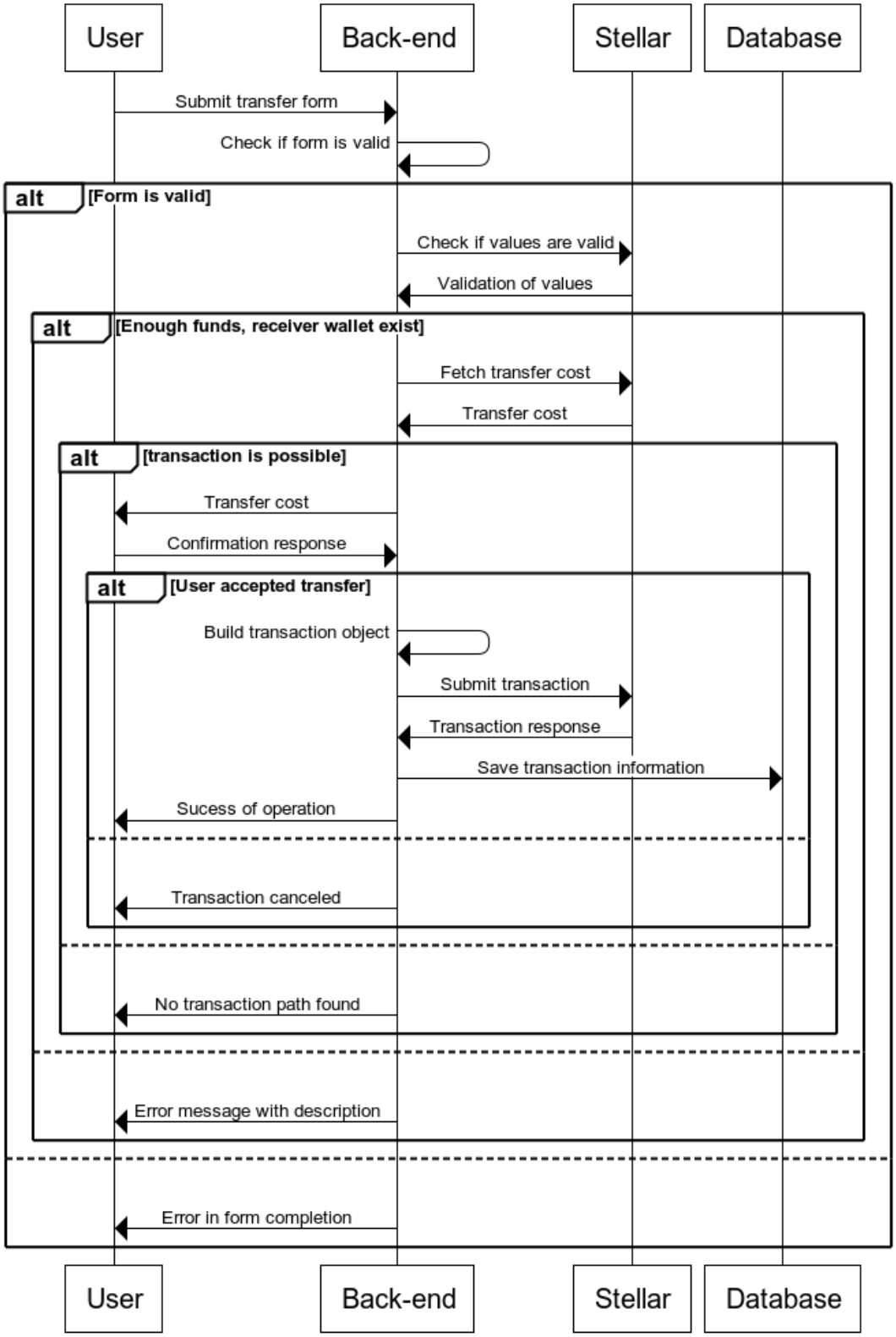


Figura 61 - Diagrama de sequência para uma transferência.

9. Transferência

Na figura 58, pode ver-se o diagrama de sequência para a operação de levantamento de fundos que segue os seguintes passos:

- Utilizador seleciona o montante e ativo para realizar o levantamento.
- Back-end realiza um pedido à rede para obter mais informações sobre a entidade responsável por realizar o levantamento (anchor). Esta informação consiste essencialmente nos endpoints que serão usados para progredir na operação de levantamento.
- Back-end pede o token de autenticação ao anchor para garantir que a comunicação é feita em segurança e depois realiza um novo pedido ao anchor para validar se o utilizador necessita ou não de enviar dados para o KYC.
- Caso o utilizador nunca tenha realizado o KYC com o anchor, os valores a preencher serão pedidos ao anchor, um formulário é gerado para o utilizador preencher e a resposta é submetida. Caso contrário, prossegue com os próximos passos na operação.
- É feito um novo pedido ao anchor para obtenção do preço da operação de levantamento que será de seguida mostrado ao utilizador.
- Caso o utilizador não aceite o preço apresentado, a operação é cancelada. Caso contrário, uma transferência é realizada para a carteira digital do anchor com os fundos a levantar de modo que este envie os fundos para a conta bancária do utilizador.
- Depois da operação estar terminada, o utilizador é informado e os dados da mesma são persistidos para a base de dados.

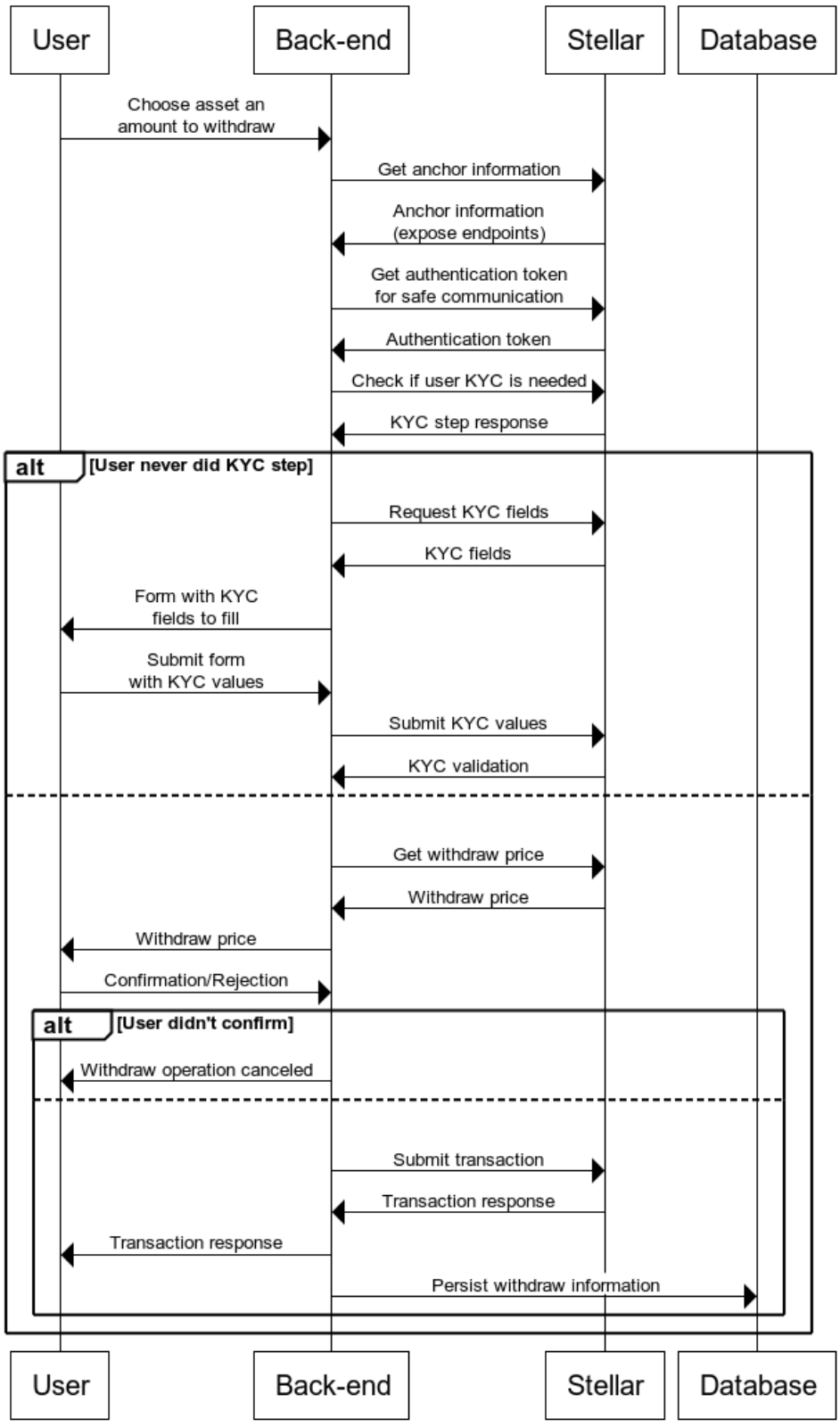


Figura 62 - Diagrama de sequência para uma operação de levantamento.

Tabela de Custos ClickPesa

Neste apêndice, pode ver-se a tabela de custos associados ao serviço de levantamento de token TZS por parte da entidade ClickPesa.

Tabela 12 - Tabela de custos associados ao levantamento de tokens TZS por parte da ClickPesa.

CHARGES & TRANSACTION VALUES COMMERCIALS **Withdraw Fees (TZS)**				
Mobile Money				
I TigoPesa I Mpesa I AirtelMoney I			**Settlement Time**	1 - working day
Minimum	**Maximum**	**Charge**	**New charges**	
1,000	4,999	1,800		
5,000	9,999	2,100		
10,000	19,999	2,700		
20,000	29,999	4,000		
30,000	39,999	5,300		
50,000	49,999	7,100		
100,000	199,999	7,700		
200,000	299,999	8,300		
300,000	399,999	9,100		
400,000	499,999	10,700		
500,000	999,999	12,000		
1,000,000	2,500,000	12,500		
Local Bank Transfer **Automated Clearing House (ACH)**				
ACH			**Settlement Time**	3 - working Days
Minimum	**Maximum**	**Charge**	**New charges**	
1,000	20,000,000	5,000		
Local bank transfer **Real Time Gross Settlement System (RTGS)**				
RTGS			**Settlement Time**	1 - Working day
Minimum	**Maximum**	**Charge**	**New charges**	
1,000	200,000,000	20,000		