

Superando Barreiras de Usabilidade em Aplicações DeFi

Uma Análise de Interação Humano-Computador em Redes Compatíveis com EVMs

Emanuele L. M. Martins¹, Bryan K. Ferreira¹

¹Instituto de Tecnologia e Liderança (INTELI)
Av. Prof. Almeida Prado, 520 - Butantã, São Paulo - SP, 05508-070 - Brazil

emanuele.martins@sou.inteli.edu.br, bryan@ime.usp.br

Resumo. Esse trabalho tem como objetivo principal analisar e superar as barreiras de usabilidade que dificultam a adoção em massa de aplicações financeiras descentralizadas (DeFi) construídas sobre tecnologia blockchain, especialmente em redes compatíveis com a Ethereum Virtual Machine (EVM).

1. Introdução

Nos últimos anos, o avanço das tecnologias de blockchain tem possibilitado o surgimento de um novo paradigma financeiro, no qual a intermediação é substituída por contratos inteligentes que operam de maneira autônoma e transparente. Dentro desse contexto, as aplicações de finanças descentralizadas (DeFi) se consolidaram como um dos pilares mais promissores da Web3, oferecendo instrumentos financeiros acessíveis, auditáveis e globais. Contudo, a promessa de democratização trazida por tais sistemas tem sido limitada por um fator frequentemente subestimado: a usabilidade. Apesar do rigor técnico e da robustez criptográfica dessas soluções, o processo de interação com carteiras digitais, a assinatura de transações e o gerenciamento de chaves privadas ainda impõem barreiras consideráveis, especialmente para usuários iniciantes. Essa complexidade técnica, aliada à falta de padronização de fluxos e de terminologias consistentes, contribui para uma experiência fragmentada que restringe a adoção em larga escala, evidenciando a necessidade de investigar a interação entre humanos e sistemas descentralizados sob a ótica da Interação Humano-Computador (IHC).

Pesquisas recentes indicam que a experiência do usuário é um fator crítico para a consolidação das tecnologias descentralizadas. Estudos sobre o comportamento de usuários em plataformas DeFi apontam que dificuldades em tarefas aparentemente simples, como conectar uma carteira, compreender taxas de transação ou interpretar mensagens de erro, resultam em altos índices de abandono logo nas primeiras interações. Além disso, o excesso de confirmações e de etapas técnicas durante operações rotineiras gera o fenômeno conhecido como fadiga de operações, no qual o esforço cognitivo supera os benefícios percebidos do sistema, reduzindo o engajamento e a confiança do usuário. Tais evidências revelam que a segurança técnica, isoladamente, não é suficiente para promover a adoção, a segurança percebida e a fluidez da interação são igualmente determinantes para o sucesso de uma aplicação descentralizada. Nesse sentido, compreender como os usuários se comportam, interpretam e reagem a esses sistemas é essencial para alinhar o design de interfaces às suas expectativas e limitações cognitivas.

Diante desse cenário, este trabalho tem como objetivo analisar e propor formas de superar barreiras de usabilidade em aplicações DeFi, com foco na redução da fadiga operacional e na ampliação da compreensão do usuário sobre os processos envolvidos. Para isso, se desenvolveu uma metodologia experimental baseada em testes A/B com duas versões de uma mesma plataforma, uma construída segundo princípios heurísticos de usabilidade e outra propositalmente desprovida desses preceitos, mas ambas sustentadas pelo mesmo contrato inteligente. Essa abordagem permite isolar o impacto do design da interface sobre a experiência do usuário, mensurando diferenças em eficiência, eficácia e satisfação. O estudo busca, assim, contribuir para o avanço das práticas de design e avaliação de usabilidade em ambientes descentralizados, oferecendo evidências empíricas sobre como decisões de interface influenciam a confiança, o esforço cognitivo e o engajamento dos usuários em ecossistemas de finanças descentralizadas.

2. Fundamentação Teórica

Esta seção tem como objetivo apresentar e discutir os principais conceitos e estudos que fundamentam a análise sobre a eliminação de barreiras de usabilidade e a redução da fadiga operacional em aplicações *blockchain* voltadas para finanças descentralizadas. Serão abordados os fundamentos da tecnologia *blockchain* e os aspectos relacionados à usabilidade, buscando contextualizar os desafios e oportunidades para a adoção em massa dessas soluções.

2.1. Fundamentos de Blockchain

Uma rede *blockchain* pode ser definida como um sistema de registros compartilhados, distribuídos e imutáveis, em que as transações são gravadas de forma permanente e só podem ser alteradas mediante consenso de todas as partes envolvidas [Bashir 2018]. Além disso, esse sistema elimina a necessidade de intermediários, permitindo que as transações ocorram diretamente entre os participantes da rede [Bashir 2018].

2.1.1. Histórico e Evolução da Tecnologia

A ideia da criação do que hoje conhecemos como blockchain surgiu a partir do conceito de dinheiro eletrônico e da busca por formas de representar valores monetários na internet [Nakamoto 2008]. Desde os anos 1980, já existiam protocolos de dinheiro eletrônico baseados no modelo proposto por David Chaum. Entretanto, a primeira implementação prática de uma moeda digital descentralizada aconteceu através do Bitcoin [Bashir 2018].

O Bitcoin surgiu em 2008, quando um pseudônimo chamado Satoshi Nakamoto publicou o documento técnico “Bitcoin: A Peer-to-Peer Electronic Cash System” [Nakamoto 2008]. Satoshi combinou ideias anteriores, como b-money [Dai 1998] e HashCash [Back 2002], para criar um sistema de dinheiro eletrônico totalmente descentralizado, sem necessidade de uma autoridade central para emissão ou validação de transações [Antonopoulos 2014]. O grande avanço dessa rede foi usar um sistema de computação distribuída chamado Proof-of-Work para resolver o problema do gasto duplo, permitindo que a rede chegassem a um consenso global sobre o estado das transações sem confiar em uma entidade central [Antonopoulos 2014]. O Bitcoin não é controlado por nenhum governo ou empresa. Em vez disso, milhares de computadores espalhados

pelo mundo, formando a rede Bitcoin, como ilustrado na Figura 1, mantém o sistema funcionando continuamente, 24 horas por dia. Para utilizar o Bitcoin, não é necessário se cadastrar ou criar uma conta em nenhum lugar, basta ter acesso à internet e usar um programa, como um aplicativo no celular.

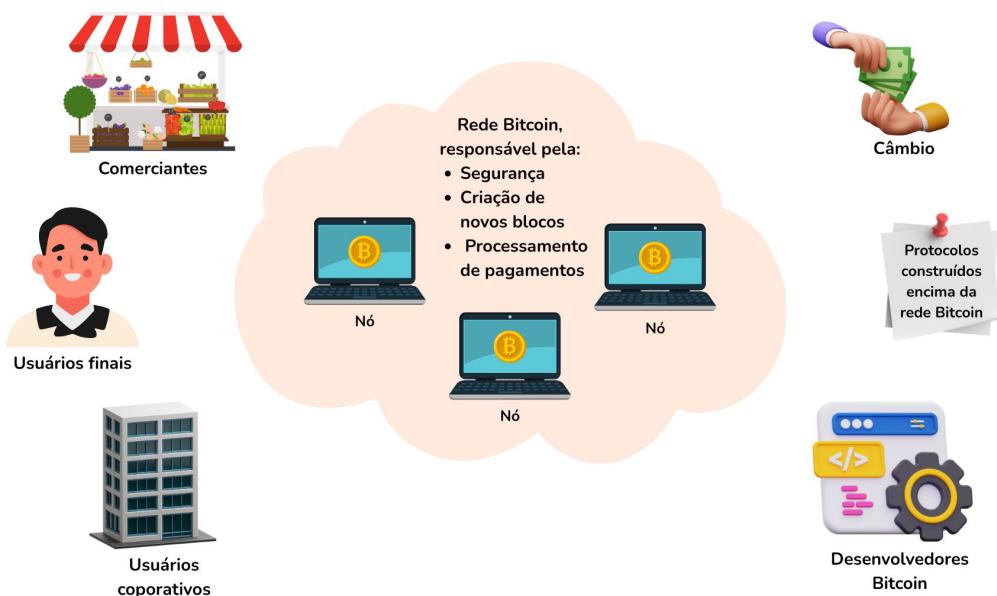


Figura 1. Participantes da rede. Fonte: Adaptado de [Rosenbaum 2019]

Ao longo do tempo, o *Bitcoin* demonstrou ser possível criar um sistema monetário digital descentralizado e resistente à censura, sem a necessidade de intermediários. Entretanto, sua arquitetura foi projetada especificamente para transações financeiras ponto a ponto, limitando sua capacidade de suportar aplicações além do registro e transferência de valor. Essa limitação motivou o surgimento de novas plataformas de blockchain, como o *Ethereum*, cuja proposta foi ampliar o escopo da tecnologia para uma infraestrutura de propósito geral, capaz de executar contratos inteligentes e aplicações descentralizadas (dApps) sob consenso distribuído [Buterin 2014][Antonopoulos and Wood 2018].

Vitalik Buterin propôs a criação de uma máquina mundial de estados globais, permitindo que qualquer pessoa implementasse códigos que detêm valor e regras de negócio, conhecidos como “contratos inteligentes” [Buterin 2014]. Esse projeto evoluiu e se tornou uma rede ativa em 2015, dando origem ao Ethereum, que abriu caminho para uma plataforma programável além da transferência de moeda [Antonopoulos and Wood 2018].

O coração dessa inovação é a *Ethereum Virtual Machine (EVM)*, uma máquina virtual descentralizada capaz de executar códigos de contratos inteligentes de forma segura e determinística em todos os nós da rede. A EVM garante que as regras programadas sejam seguidas fielmente e que as transições de estado ocorram de maneira idêntica em toda a *blockchain*, independentemente do participante [Antonopoulos and Wood 2018]. Na prática, o desenvolvimento desse novo conceito de rede mudou o foco do aspecto exclusivamente monetário para a infraestrutura em si. Dessa forma, o Ethereum permite a sincronização de transições de estado de qualquer tipo de dado, possibilitando a criação de *tokens*, aplicações financeiras, *stablecoins*, organizações autônomas descentralizadas

(*Decentralized Autonomous Organizations — DAOs*) e diversas outras inovações.

2.2. Arquitetura e Funcionamento

2.2.1. Estrutura do bloco

Um bloco na *blockchain* é uma estrutura responsável por registrar e organizar transações de forma segura e ordenada, e é composto por duas partes principais, o cabeçalho e o corpo. O corpo do bloco reúne todas as transações incluídas, enquanto o cabeçalho, conhecido como Block Header, contém informações essenciais para identificar e validar o bloco, como o horário de criação, o nonce, o hash do bloco anterior (*parentHash*) e o hash das transações, chamado de Merkle Root [Bashir 2018].

A Merkle Root é gerada por meio da árvore de Merkle, uma estrutura que combina todos os *hashes* das transações até chegar a um único hash final, funcionando como um resumo do bloco [Bashir 2018]. Esse mecanismo permite verificar rapidamente se uma transação faz parte do bloco e garante que qualquer alteração em uma transação modifique a Merkle Root, preservando a integridade do conjunto. O *nonce*, por sua vez, é um número ajustado durante o processo de mineração para que o hash do bloco atenda aos requisitos definidos pela rede. Já o hash do bloco, gerado a partir de seu conteúdo, utilizando funções como Keccak-256 [Wood 2014] no caso do Ethereum, funciona como uma impressão digital única do bloco.

Além disso, o *parentHash* presente no cabeçalho conecta cada bloco ao anterior, formando uma cadeia contínua. Essa ligação por *hashes* garante a integridade e a imutabilidade da *blockchain*, pois qualquer alteração em um bloco modifica seu hash, comprometendo a sequência e invalidando todos os blocos seguintes.



Figura 2. Exemplificação da estrutura de blocos na rede. Fonte: Autoria própria

2.2.2. Nós e Papéis na Rede

Para que uma rede descentralizada funcione corretamente, é necessário que diversos computadores, chamados de nós, executem o protocolo e se comuniquem entre si, formando uma infraestrutura robusta e distribuída. Esses nós desempenham diferentes funções, que, em conjunto, garantem a segurança, auditabilidade e acessibilidade da rede.

Os nós completos (*full nodes*) mantêm uma cópia local de todo o blockchain e do estado da rede, validando integralmente blocos e transações conforme as regras de consenso. Eles são fundamentais para a resiliência e verificabilidade do sistema, mas exigem considerável capacidade de armazenamento, largura de banda e tempo para sincronização [Bashir 2018].

Os clientes leves (*light clients*), por outro lado, não armazenam a cadeia completa nem reexecutam todas as transações. Eles verificam blocos utilizando apenas os cabeçalhos e provas de Merkle, confiando em nós completos para obter dados sob demanda. Por consumirem menos recursos, são ideais para carteiras digitais e dispositivos móveis, permitindo assinar e enviar transações de maneira eficiente [Antonopoulos and Wood 2018].

Além desses, existem os nós validadores, responsáveis por produzir e atestar blocos dentro do mecanismo de consenso da rede. Em sistemas Proof-of-Work (PoW), essa função é desempenhada por mineradores, que competem para encontrar o próximo bloco por meio de cálculos computacionais intensivos. Já em sistemas Proof-of-Stake (PoS), os validadores depositam (*stake*) o *token* nativo para participar da proposta e validação de blocos, recebendo recompensas pelo bom comportamento e podendo sofrer penalidades (*slashing*) em caso de conduta desonesta ou inatividade. Normalmente, os validadores operam nós completos com alta disponibilidade, boa conectividade e chaves privadas bem protegidas [Bashir 2018]. A atuação coordenada desses diferentes tipos de nós permite que a rede *blockchain* seja descentralizada, equilibrando segurança, auditabilidade e acessibilidade para todos os participantes.

2.2.3. Mecanismos de Consenso

Existem dois mecanismos de consenso mais conhecidos nas redes blockchain, o Proof-of-Work (PoW) e o Proof-of-Stake (PoS). Ambos desempenham o papel de garantir que apenas blocos válidos sejam adicionados à cadeia, mantendo a segurança e a descentralização da rede.

No PoW, mineradores competem para resolver um problema matemático, buscando um nonce que gere um hash válido para o bloco. Esse processo demanda grande poder computacional e consumo de energia, tornando ataques à rede caros e incentivando o comportamento honesto. Os mineradores são recompensados com moedas nativas e taxas de transação, mas precisam arcar com os custos de eletricidade e hardware. O objetivo principal do PoW não é apenas “minerar moedas”, mas sim proteger a rede contra manipulações e garantir sua integridade [Bashir 2018].

Já no PoS, validadores são selecionados para propor e votar em blocos conforme a quantidade de tokens que depositaram como garantia (“stake”). A seleção

dos validadores é aleatória, e aqueles que agem de maneira desonesta podem perder parte ou todo o valor em stake (slashing). As recompensas são distribuídas proporcionalmente ao stake e ao comportamento honesto dos participantes. Uma das principais vantagens do PoS é a eficiência energética, além de reduzir barreiras de entrada e incentivar maior descentralização, tornando o sistema mais inclusivo e sustentável [Antonopoulos and Wood 2018].

O Ethereum, por exemplo, inicialmente utilizava o PoW como mecanismo de consenso, mas migrou para o PoS visando maior sustentabilidade e segurança, além de promover uma rede mais descentralizada e menos suscetível a ataques.

2.2.4. Criptografia e segurança.

Em redes blockchain, a segurança não depende de logins e senhas, mas sim de criptografia. O processo começa com funções de hash, que convertem qualquer dado em um resumo de tamanho fixo e aparentemente aleatório. No ecossistema Ethereum, o algoritmo utilizado para gerar esse hash é o Keccak-256, como mencionado anteriormente [Bashir 2018].

O resultado de uma função de hash é pseudoaleatório, embora seja totalmente determinístico, ou seja, a mesma entrada sempre gera o mesmo resultado, qualquer alteração mínima na entrada produz uma saída completamente diferente e imprevisível. A identidade dos usuários na rede é definida por um par de chaves geradas a partir da curva elíptica secp256k1, uma chave privada, que é basicamente um número aleatório de 256 bits, e sua respectiva chave pública, obtida por multiplicação escalar na curva [Antonopoulos and Wood 2018]. Nesse sistema, quem possui a chave privada controla os fundos associados ao endereço, portanto, perder essa chave significa perder acesso aos ativos.

Para autorizar operações na rede, utilizam-se assinaturas digitais. A transação é serializada, processada por uma função de hash e assinada com a chave privada usando o algoritmo ECDSA. Isso garante que apenas o detentor da chave privada pode autorizar a transação e que os dados não foram alterados. Qualquer nó da rede pode verificar a assinatura utilizando a chave pública, confirmado a autenticidade da transação [Antonopoulos and Wood 2018].

Para simplificar o backup, carteiras modernas adotam a seed phrase (BIP-39), uma sequência mnemônica de 12 ou 24 palavras que codifica entropia de alta qualidade. Essa seed é convertida em uma chave-mestra, da qual podem ser derivadas milhares de chaves privadas e endereços diferentes, seguindo os padrões BIP-32/BIP-44 [Antonopoulos and Wood 2018].

2.3. Princípios de Interação Humano-Computador (IHC)

2.3.1. Definição de Interação Humano-Computador (IHC)

Interação Humano-Computador (IHC) é uma área multidisciplinar que reúne ciência da computação, psicologia e design com o objetivo de aprimorar a comunicação entre pessoas e máquinas. O foco principal está em desenvolver interfaces e sistemas que levem

em consideração as necessidades, limitações e expectativas dos usuários, tornando a tecnologia mais intuitiva e acessível [Nielsen 1994].

A IHC vai além do design de interfaces gráficas: ela abrange também a funcionalidade dos sistemas e o papel que desempenham ao lado dos seres humanos. Entre os princípios fundamentais estão a prevenção de erros, a facilidade para desfazer ações, a redução da carga de memória de curto prazo do usuário e a oferta de feedback informativo [Nielsen 1994].

A experiência do usuário (UX) é um fator decisivo para a adoção de sistemas. Aspectos afetivos, como expressividade, estética, frustração, agentes e antropomorfismo, influenciam diretamente a confiança, o engajamento e o retorno dos usuários. Por outro lado, uma UX pobre, marcada por erros obscuros, excesso de etapas e mensagens vagas, tende a causar abandono dos sistemas [Preece et al. 2002].

2.3.2. Affordance, visibilidade, carga cognitiva.

Alguns dos conceitos fundamentais na área de Interação Humano-Computador (IHC) são affordance, visibilidade e carga cognitiva. Esses princípios são amplamente reconhecidos e aplicados para orientar o desenvolvimento de interfaces mais intuitivas e eficientes.

Affordance se refere às pistas perceptíveis que indicam ao usuário que uma determinada ação é possível. Por exemplo, um botão que “convida” ao clique ou uma alça que sugere ser puxada. Em interfaces digitais, confiar apenas na imitação de objetos físicos nem sempre é suficiente, é essencial utilizar convenções, oferecer feedback claro e estabelecer restrições lógicas ou culturais para orientar o usuário de maneira eficaz [Preece et al. 2002].

A visibilidade, por sua vez, diz respeito à clareza com que as funções e o estado da interface são apresentados ao usuário. Uma interface bem projetada responde à pergunta “o que posso fazer agora?”, tornando evidentes as opções disponíveis e o resultado de cada ação. Isso envolve mapeamentos comprehensíveis entre controles e efeitos, além de feedback imediato para que o usuário entenda o impacto de suas escolhas [Preece et al. 2002].

Por fim, o conceito de carga cognitiva destaca a importância de minimizar o esforço mental exigido do usuário. Interfaces que dependem da memorização de passos, códigos ou comandos tendem a aumentar o risco de erros e a dificultar o uso. Para reduzir esse peso mental, recomenda-se priorizar o reconhecimento (por meio de menus, ícones e favoritos), manter consistência para que o contexto ajude a memória e promover a cognição externa. Sempre que possível, o sistema deve assumir tarefas mecânicas, como cálculos e rastreamento de progresso, permitindo que o usuário concentre sua atenção nas decisões relevantes [Preece et al. 2002].

2.3.3. Segurança Técnica vs. Segurança Percebida

No campo da Interação Humano-Computador (IHC), um dos conceitos centrais é o de segurança usável, que busca integrar a robustez técnica dos sistemas com a clareza e confiança transmitidas pela interface ao usuário [Preece et al. 2002]. Essa aproximação é

fundamental porque, muitas vezes, a segurança percebida pelo usuário é tão importante quanto a segurança técnica baseada em mecanismos como criptografia.

A segurança técnica se refere à implementação de algoritmos avançados que garantem a confidencialidade e integridade dos dados. No entanto, se a interface não comunica de maneira transparente o que está acontecendo, o sistema pode parecer inseguro mesmo sendo matematicamente robusto. Usuários tendem a depositar confiança no que veem na tela, e não nos processos invisíveis que acontecem no backend [Preece et al. 2002]. Essa discrepância é especialmente crítica em ambientes como blockchain, onde interfaces que ocultam informações ou apresentam mensagens vagas podem levar a decisões equivocadas, como autorizar transações maliciosas ou enviar valores para endereços errados.

No contexto de sistemas DeFi, a diferença entre segurança técnica e percebida se torna ainda mais relevante, pois erros podem resultar em perdas financeiras irreversíveis. Interfaces que não traduzem operações complexas em linguagem acessível podem induzir o usuário a conceder permissões amplas sem entender as consequências [Nielsen 1994]. Exemplos comuns incluem endereços truncados, pop-ups confusos, tokens falsos e propostas de governança ambíguas, todos explorando falhas de design de experiência do usuário (UX).

Além disso, a cultura de auto-custódia típica do universo blockchain exige que interfaces orientem o usuário de forma precisa sobre práticas de backup, uso de seed phrases e assinaturas fora da cadeia, qualquer ambiguidade pode abrir espaço para ataques como phishing. O paradoxo é que, quanto mais robusta e permissionless a infraestrutura, maior a superfície para erros humanos mediados por uma UX inadequada.

2.3.4. Modelos de Avaliação de Interface

A avaliação de interfaces desempenha um papel fundamental para assegurar que os sistemas interativos sejam eficazes, eficientes e satisfatórios para os usuários [Nielsen 1994]. Entre os principais modelos utilizados nesse processo, se destacam as dez heurísticas de usabilidade propostas por Jakob Nielsen, que servem como princípios amplamente reconhecidos para orientar tanto o design quanto a avaliação de interfaces. Essas heurísticas abordam pontos essenciais como a visibilidade do status do sistema, a correspondência entre a interface e o mundo real, o controle e a liberdade do usuário, a consistência, a prevenção de erros e a clareza nas mensagens de ajuda [Nielsen 1994]. Embora não sejam regras rígidas, funcionam como diretrizes que facilitam a identificação de problemas recorrentes na interação entre o usuário e o sistema.

Outro modelo relevante é o design centrado no usuário (DCU), que coloca as necessidades, características e limitações dos usuários no centro do processo de desenvolvimento. O DCU é caracterizado por sua abordagem iterativa, envolvendo ciclos de pesquisa, ideação, prototipagem e testes, o que permite o aprimoramento contínuo das soluções a partir do feedback real dos usuários [Preece et al. 2002]. Os testes de usabilidade são ferramentas essenciais para complementar esses modelos. Eles fornecem evidências concretas sobre como as pessoas interagem com a interface, por meio da observação direta de tarefas, coleta de métricas como tempo de execução, taxa de sucesso

e número de erros, além de questionários e entrevistas que captam percepções subjetivas dos usuários [Preece et al. 2002].

A combinação entre heurísticas de usabilidade, design centrado no usuário e testes de usabilidade garante que as interfaces desenvolvidas não apenas atendam aos requisitos técnicos, mas também ofereçam uma experiência positiva e alinhada às expectativas dos usuários.

3. Revisão da literatura

A adoção de aplicações de finanças descentralizadas (*DeFi*) esbarra em dois obstáculos recorrentes, a barreiras de usabilidade, que dificultam a formação de modelos mentais estáveis por usuários não especialistas [Jang et al. 2020], e a fadiga de operações, causada por sequências longas e pouco transparentes de passos, aprovações e confirmações [Saldivar et al. 2023]. A literatura recente em HCI para sistemas distribuídos argumenta que reduzir fricções instrumentais é fundamental para converter a curiosidade inicial em retenção e uso recorrente. Tecnologias emergentes dificilmente alcançam seu potencial sem um foco consistente em experiência do usuário, o que exige equilibrar inovação tecnológica com estratégias de design centrado no usuário [Glomann et al. 2019].

3.1. Barreiras de Usabilidade em DeFi

Ainda antes da realização de qualquer transação, o processo de onboarding já se configura como uma barreira significativa à adoção, afastando uma parcela relevante dos potenciais usuários. A configuração inicial frequentemente se revela complexa e carente de orientações claras, desde a criação de carteiras até a execução de operações básicas. Essa dificuldade se intensifica diante da necessidade de troca de dispositivo ou da perda da *seed phrase*, uma vez que muitos usuários não compreendem sua importância nem conhecem os procedimentos adequados para recuperação [Voskobojnikov et al. 2021]. A exigência de anotar, armazenar e posteriormente localizar uma sequência de palavras representa um ponto de fricção recorrente entre usuários e aplicações descentralizadas [Moniruzzaman et al. 2020].

Outro fator relevante é o desalinhamento entre o modelo mental herdado do sistema bancário tradicional e o funcionamento da blockchain. Usuários frequentemente apresentam dificuldades para compreender taxas, endereços e a irreversibilidade das operações. Muitos acreditam que as taxas são definidas pelo aplicativo, quando na realidade são determinadas pela rede, e esperam a possibilidade de cancelar ou reverter transações, expectativa que não se aplica ao contexto descentralizado [Voskobojnikov et al. 2021]. Esse descompasso é intensificado por interfaces pouco intuitivas, nas quais ações essenciais permanecem ocultas, mensagens de erro não contribuem para a resolução de problemas e, para usuários sem domínio do inglês, traduções incompletas ou inadequadas comprometem o entendimento em momentos críticos [Froehlich et al. 2021].

Paralelamente, o receio de perda de fundos é amplificado pela comunicação pouco clara durante transações, backups ou restaurações. A gestão de chaves, em especial, permanece pouco intuitiva e sujeita a erros, uma vez que a distinção entre chaves públicas e privadas é abstrata para a maioria dos usuários [Moniruzzaman et al. 2020].

Em síntese, é observada uma cadeia de fricções que se retroalimentam. As instabilidades técnicas minam a confiança inicial, dificuldade de onboarding e de recuperação de conta dificultam o retorno após contratemplos e compreensão insuficiente de conceitos fundamentais torna operações rotineiras arriscadas. Esse conjunto de fatores não apenas eleva o custo mental de cada ação, mas também transformam pequenos obstáculos em desistências definitivas, o que restringe o funil de adoção e impede que os usuários desenvolvam a fluência operacional necessária para sua permanência no ecossistema.

3.2. Fadiga de Operações

Pesquisas recentes apontam que usuários relatam frustração e fadiga ao lidar com sistemas que exigem muitos passos para realizar operações simples. A necessidade de múltiplas confirmações e verificações de segurança pode tornar o processo cansativo, especialmente para iniciantes [Albayati et al. 2021]. Além disso, sistemas que exigem navegação por múltiplas plataformas e possuem etapas pouco claras ou repetitivas geram ansiedade e preocupação nos usuários [Si et al. 2024]. A falta entendimento sobre o significado de cada etapa contribui para a sensação de insegurança e sobrecarga cognitiva. Para lidar com essa complexidade, alguns usuários inclusive adotam estratégias, como testar operações com valores pequenos antes de realizar transações maiores, para assim garantir que não irão se perder durante o processo e realizar transferências erradas [Si et al. 2024].

Outro ponto de preocupação comum entre usuários novatos é o tempo de espera entre a realização e o registro de uma transação no blockchain. Esse intervalo costuma ser maior do que em sistemas centralizados e, frequentemente, os usuários não recebem informações claras sobre quanto tempo devem aguardar. Como resultado, surgem insegurança, sensação de erro e abandono da tarefa [Jang et al. 2020]. Problemas de usabilidade também são relatados em relação à ausência de explicações sobre o que está acontecendo, o que cada botão faz ou por que certas ações são necessárias. Isso obriga o usuário a repetir etapas e buscar informações por tentativa e erro, aumentando o risco de desistência [Jang et al. 2020].

Esses desafios se confirmam em testes de usabilidade realizados com aplicações que utilizam a rede *EVM*. Mais de 70% do tempo total dos participantes foi consumido por etapas relacionadas ao uso do Metamask e da rede Ethereum, especialmente durante a instalação da carteira e criação da conta, momentos marcados por bloqueios e confusão [Saldivar et al. 2023]. Além disso, os termos técnicos apresentados nas janelas de transação, como *gas fee*, *gas price* e *gas limit*, foram considerados excessivamente complexos para pessoas com pouca experiência em blockchain, gerando ainda mais insegurança e dificultando o processo [Saldivar et al. 2023].

3.3. Padrões de Design para Reduzir Fricção

Estudos indicam que a redução da fricção na utilização de aplicações descentralizadas depende do alinhamento dos fluxos operacionais com modelos mentais já consolidados pelos usuários em bancos e corretoras, por meio da reutilização de termos e ícones familiares. Por exemplo, ao tratar a carteira como uma *conta*, com ações de *ver saldo* e *transferir*, evita-se a necessidade de reaprendizagem de operações básicas, promovendo uma navegação mais previsível [Jang et al. 2020]. Esta coesão com práticas tradicionais deve ser refletida em funcionalidades críticas, como mecanismos para lidar com transações pendentes, aproximando a experiência do que o usuário espera ao “alterar”

uma operação bancária. Da mesma forma, opções de backup em nuvem, com a seed-phrase cifrada e armazenada em serviço escolhido pelo usuário, reduzem o risco percebido na recuperação de acesso e replicam padrões já aceitos em aplicativos convencionais [Voskobojnikov et al. 2021].

Tal alinhamento é potencializado quando o onboarding inicial é transparente, guiando o usuário passo a passo na instalação, criação de conta e execução da primeira operação. Além de reduzir a incerteza das etapas iniciais, esse percurso pode ser simplificado com a integração de carteiras em um modelo *custodial-like*, no qual a aplicação abstrai a gestão de chaves e os detalhes de transação para iniciantes, sem impedir que usuários experientes conectem suas próprias carteiras e accessem configurações avançadas [Saldivar et al. 2023]. A interface pode ser adaptada ao nível de proficiência do usuário em que são feitos perfis simplificados para iniciantes, focados em tarefas essenciais, e visões avançadas para usuários experientes, incluindo ajuste fino de taxas e importação de chaves [Voskobojnikov et al. 2021]. Essa personalização deve ser acompanhada de orientação adequada, como tutoriais curtos e ambientes de teste, os quais auxiliam na explicação de conceitos como irreversibilidade, taxas e importância do backup. Por fim, a comunicação clara sobre sincronização, por exemplo, quando o saldo ainda não refletiu o último bloco, e sobre limitações do protocolo, como a impossibilidade de “cancelar” uma transação confirmada, previnem expectativas irrealistas e fortalecem a confiança [Voskobojnikov et al. 2021].

Paralelamente, é fundamental a diminuição do cansaço operacional imposto por confirmações repetitivas. Parte das autorizações pode ser agregada ou mediada por resumos de intenção, reduzindo cliques e diálogos redundantes sem comprometer a verificabilidade e a segurança [Saldivar et al. 2023]. No nível micro da interação, a simplificação dos fluxos atua de maneira decisiva. Operações comuns devem exigir o mínimo de etapas possível com confirmações apenas quando agregarem valor real à segurança ou à compreensão do risco [Si et al. 2024]. Cada etapa precisa fornecer feedback imediato e mensagens de erro devem sugerir ações corretivas, evitando a apresentação exclusiva de códigos técnicos [Si et al. 2024]. A transparência sobre o propósito de cada etapa e o que está sendo aprovado pode ser promovida por meio de resumos curtos e *tooltip* nos pontos críticos, como permissões de gasto e assinaturas de contratos, reduzindo ambiguidades sem sobrecarregar a interface [Si et al. 2024].

Por fim, a automação e o preenchimento inteligente desempenham papel relevante na aceleração de tarefas repetitivas e na redução do esforço exigido dos usuários, como a sugestão automática de endereços frequentemente utilizados e o resgate das últimas preferências configuradas. Simultaneamente, mecanismos de autenticação de baixo atrito, como biometria e *PIN*, contribuem para a preservação da segurança sem transformar cada ação em um obstáculo adicional. O princípio orientador nessas práticas é garantir que a proteção seja devidamente explicada e percebida pelo usuário, em vez de simplesmente imposta [Si et al. 2024].

4. Metodologia

Neste estudo, buscamos investigar formas de eliminar barreiras de usabilidade e reduzir a fadiga operacional em aplicações *DeFi* por meio de um experimento conduzido com duas versões de uma mesma plataforma. Ambas as versões oferecem funcionali-

lidades idênticas, se diferenciando apenas nos fundamentos de usabilidade aplicados. Em revisões recentes, foi apontado que, dentre as principais operações e categorias de serviços no âmbito de *DeFi*, se destacam stablecoins, troca de ativos e empréstimos de ativos. Segundo o relatório da *Wharton School* (2021), essas operações são centrais para a experiência do usuário e representam as principais interações típicas em ambientes *DeFi* [Gogel et al. 2021]. Por esse motivo, o desenvolvimento de *features* da plataforma para o cenário experimental se justifica por reunir características representativas dessas interações. Na plataforma desenvolvida, os usuários podem realizar o depósito e retirada de ativos, trocar ativos, enviar a outros usuários e realizar empréstimos, se alinhando às práticas observadas nos principais protocolos *DeFi* descritos na literatura.

Com base nesse desenho experimental, foram estabelecidas as seguintes hipóteses de pesquisa:

1. Maior usabilidade reduz o tempo de conclusão das tarefas e o número de cliques em comparação à versão sem princípios de usabilidade;
2. A versão com princípios de usabilidade aumenta a taxa de sucesso na conclusão de tarefas e a satisfação percebida em comparação à versão sem tais princípios;
3. O ganho proporcionado pela versão com princípios heurísticos é mais pronunciado entre usuários novatos do que entre usuários experientes;
4. A versão baseada em princípios heurísticos reduz a taxa de abandono de tarefas em comparação à versão sem esses fundamentos;

Para operacionalizar a comparação, as duas versões da aplicação foram implementadas com fundamentos distintos de usabilidade. A primeira seguiu princípios heurísticos consolidados, priorizando *feedback* imediato, terminologia clara e consistente, minimização da carga cognitiva e prevenção de erros [Nielsen and Molich 1990]. O fluxo de navegação foi projetado para ser intuitivo, com rótulos descritivos, mensagens de confirmação legíveis e indicadores visuais de progresso em cada etapa. Em contraste, a segunda versão foi construída sem a aplicação desses princípios, os rótulos utilizam linguagem técnica, há escassez de *feedback* visual, pouca consistência entre elementos da interface e mensagens genéricas de erro ou confirmação. Essa configuração representa um cenário menos amigável, próximo das barreiras de usabilidade ainda comuns em aplicações *DeFi* emergentes, sem comprometer a segurança ou a funcionalidade essencial do sistema.

[Adicionar imagem da plataforma 1 e 2 após ser construída]

4.1. Métricas do estudo

Para a construção das métricas deste estudo, serão utilizadas medidas objetivas e subjetivas para obtenção de dados quantitativos. Em pesquisas de usabilidade, métricas objetivas como tempo de execução, número de cliques e taxa de sucesso permitem quantificar a eficiência e a eficácia do sistema. No entanto, essas métricas não capturam aspectos subjetivos da experiência do usuário, como satisfação, carga cognitiva ou reações emocionais [Foster et al. 2009][ASSILA et al. 2016]. Nesse contexto, estudos defendem que, além das métricas objetivas de desempenho, é fundamental compreender as percepções dos usuários, especialmente considerando o caráter inovador, tecnicamente complexo e cognitivamente exigente desses sistemas [Saldivar et al. 2023].

4.1.1. Métricas objetivas de desempenho

Os dados estatísticos selecionados para este estudo abrangem diferentes dimensões da experiência do usuário. Inicialmente, o tempo de sessão foi adotado por ser uma métrica clássica de eficiência de normas internacionais de usabilidade, como a *ISO 9241-11*, a eficiência é expressa pelo tempo necessário para completar tarefas [for Standardization 2018], e *Nielsen* destaca o tempo como indicador fundamental da intuitividade da interface [Nielsen 1994]. Complementando essa perspectiva, a taxa de sucesso foi incluída como métrica de eficácia, pois representa diretamente a capacidade dos usuários de alcançar seus objetivos no sistema, sendo considerada uma das formas mais objetivas de verificar se a aplicação cumpre sua função essencial [Nielsen 1994][Rubin and Chisnell 2008]. Já o número de cliques reflete a carga de trabalho operacional exigida para concluir uma ação. Segundo *Shneiderman*, a redução de interações desnecessárias é fundamental para tornar sistemas mais eficientes e menos cansativos [Shneiderman and Plaisant 2004], de modo que interfaces que demandam menos cliques tendem a exigir menor esforço cognitivo e físico do usuário.

Além dessas métricas, a taxa de abandono foi utilizada como um importante indicador de frustração e de falhas no fluxo de interação, permitindo identificar pontos críticos em que a interface pode gerar desistência, um fenômeno frequentemente associado a barreiras cognitivas [Sauro and Lewis 2012]. Por fim, o mapa de calor do cursor foi adotado como complemento às métricas tradicionais, possibilitando a análise visual de padrões de atenção e áreas de confusão, permitindo compreender não apenas o resultado final das interações, mas também o percurso percorrido pelos usuários ao longo das tarefas.

Tabela 1. Métricas objetivas utilizadas no estudo

Métrica	Descrição	Forma de registro
Tempo de sessão	Intervalo total entre o início e a finalização das tarefas	Capturado automaticamente por logs de interação
Taxa de sucesso	Proporção de participantes que concluíram corretamente cada tarefa	Classificação binária (sucesso/falha)
Número de cliques	Total de interações necessárias até a conclusão da ação	Contagem automática de eventos de clique
Taxa de abandono	Percentual de usuários que desistiram antes de completar a tarefa	Identificado por interrupção sem conclusão
Mapa de calor	Áreas da interface em que o cursor permaneceu por mais tempo	Mouse tracking e visualização de densidade

4.1.2. Métricas subjetivas de experiência

Para a obtenção dos dados subjetivos relacionados às percepções dos usuários, será utilizado um formulário baseado no *System Usability Scale (SUS)*. Esse instrumento é am-

plamente adotado em pesquisas de usabilidade por oferecer uma medida padronizada, simples e confiável da usabilidade percebida em sistemas interativos [Brooke 1996]. O SUS consiste em dez afirmações avaliadas em escala *Likert* de cinco pontos, cujas respostas são posteriormente convertidas em um escore único que varia de 0 a 100. Esse escore possibilita a comparação entre diferentes interfaces, versões de um mesmo sistema ou grupos de usuários, o que o torna uma ferramenta flexível e aplicável em diferentes contextos [Sauro and Lewis 2012][Bangor et al. 2008].

A literatura recomenda o uso do SUS em situações em que é necessário obter uma avaliação rápida, de baixo custo e estatisticamente robusta da usabilidade, inclusive em estudos com amostras pequenas, já que o método mantém boa sensibilidade mesmo em cenários exploratórios [Brooke 1996][Lewis and Sauro 2009]. Além disso, estudos empíricos têm demonstrado sua validade externa, indicando que os resultados obtidos pelo SUS se correlacionam com medidas objetivas de desempenho, como tempo de execução e taxa de sucesso [Sauro and Lewis 2012][Tullis and Stetson 2004].

O cálculo do escore final segue um procedimento padronizado, para cada item positivo, se subtrai 1 do valor assinalado pelo participante (variando de 0 a 4 pontos). Para cada item negativo, se subtrai a resposta de 5 (também variando de 0 a 4 pontos). A soma de todos os itens resulta em um valor entre 0 e 40, que é multiplicado por 2,5 para gerar a pontuação final na escala de 0 a 100 [Brooke 1996]. Outro aspecto metodológico relevante é a alternância entre afirmações positivas e negativas. Essa estrutura tem a função de reduzir o viés de aquiescência (tendência dos respondentes a concordarem automaticamente com as afirmações) e aumentar a confiabilidade do instrumento [Bangor et al. 2008][Kortum and Bangor 2013].

Conforme estabelecido pelo modelo original do SUS, o questionário deve conter as 10 perguntas propostas por Brooke [Brooke 1996]. Sendo elas:

Tabela 2. Afirmações utilizadas no questionário SUS

Nº	Afirmação	Tipo
1	Eu acho que gostaria de usar este sistema frequentemente.	Positiva
2	Eu achei o sistema desnecessariamente complexo.	Negativa
3	Eu achei o sistema fácil de usar.	Positiva
4	Eu acho que precisaria de apoio técnico para usar este sistema.	Negativa
5	Eu achei que as várias funções do sistema estavam bem integradas.	Positiva
6	Eu achei que havia muita inconsistência neste sistema.	Negativa
7	Eu imagino que a maioria das pessoas aprenderia a usar este sistema rapidamente.	Positiva
8	Eu achei o sistema muito pesado para usar.	Negativa
9	Eu me senti muito confiante usando o sistema.	Positiva
10	Eu precisei aprender muitas coisas antes de conseguir usar o sistema.	Negativa

4.2. Estratificação dos participantes

Para a condução do experimento, os participantes serão classificados em dois grupos distintos de acordo com o seu nível de familiaridade com sistemas *DeFi*, usuários experientes e usuários não experientes. Essa separação permitirá observar de forma mais precisa as diferenças na percepção de usabilidade entre aqueles que já possuem contato prévio com esse tipo de aplicação e aqueles que ainda não estão habituados ao seu uso [Nielsen 1994]. A classificação será realizada por meio de autodeclaração dos participantes, uma prática recorrente em estudos de usabilidade e interação humano-computador, especialmente em contextos nos quais o nível de experiência é subjetivo e difícil de mensurar de forma objetiva [Nielsen 1994]. Dessa maneira, cada participante indicará previamente seu grau de familiaridade, possibilitando a criação de grupos mais homogêneos e comparáveis entre si.

Além disso, a ordem de exposição às versões com maior usabilidade e com menos usabilidade foi randomizada, de forma a mitigar o viés de aprendizado. Estudos apontam que participantes que utilizam primeiro uma versão podem adquirir familiaridade com as tarefas, o que tende a influenciar seu desempenho na segunda versão [Rubin and Chisnell 2008]. A randomização do protótipo inicial reduz esse efeito, aumentando a confiabilidade da comparação entre condições. A Figura 5 ilustra o fluxo completo de aplicação dos testes, incluindo a etapa de categorização dos participantes, a execução das tarefas padronizadas em ambas as plataformas e a coleta das percepções subjetivas por meio do questionário *SUS*. Assim, além de permitir comparações entre os sistemas avaliados, a metodologia também possibilita identificar se o nível de experiência dos usuários impacta significativamente a percepção de usabilidade em ambientes financeiros descentralizados.

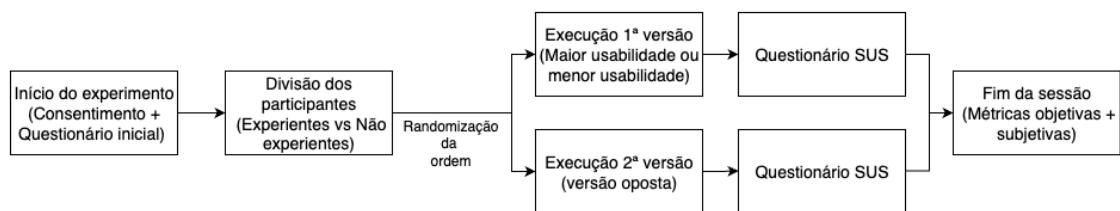


Figura 3. Fluxo de aplicação dos testes. Fonte: Autoria própria

4.3. Procedimento do teste de usabilidade

A literatura ressalta que a definição de tarefas específicas e consistentes é essencial para a validade dos testes de usabilidade [Group 2023], e que procedimentos padronizados são necessários para permitir comparações sistemáticas entre diferentes condições experimentais [Bastien 2010]. Dessa forma, para a execução dos testes, foi estabelecido um conjunto de tarefas que todos os participantes deveriam realizar em ambas as plataformas. Essas tarefas foram elaboradas de modo a contemplar as principais funcionalidades do sistema e a mimetizar o comportamento típico de usuários em plataformas *DeFi*, assegurando a padronização entre os testes e possibilitando a obtenção de resultados consistentes para a análise.

Além disso, a escolha das tarefas buscou refletir cenários de uso realistas, incorporando operações centrais identificadas na literatura como fundamentais para a experiência

de interação em ambientes *DeFi*, tais como depósito e retirada de ativos, troca de tokens, transferências entre usuários e operações de empréstimo [Gogel et al. 2021]. A inclusão desses fluxos garante não apenas a avaliação da usabilidade de funcionalidades representativas, mas também a possibilidade de analisar como diferentes níveis de experiência dos participantes impactam sua interação com o sistema.

Tabela 3. Roteiro de tarefas definidas para o teste de usabilidade

Nº	Tarefa	Explicação
1	Entrar na plataforma	Avaliar a clareza e simplicidade do processo de autenticação e acesso inicial ao sistema.
2	Depositar ativos	Testar a facilidade com que o usuário consegue adicionar stablecoins à plataforma, verificando se entende os passos e confirmações necessárias.
3	Visualizar saldo atualizado	Medir a transparência do sistema em exibir corretamente os valores depositados e transmitir confiança ao usuário.
4	Realizar uma troca de ativos (<i>swap</i>)	Avaliar a intuitividade da interface ao permitir converter uma <i>stablecoin</i> em outro <i>token</i> , incluindo clareza das taxas e resultados da operação.
5	Enviar ativos a outro usuário	Testar a clareza e segurança percebida no processo de transferência de <i>tokens</i> entre usuários, incluindo confirmação da transação.
6	Solicitar um empréstimo de ativos	Verificar se o usuário comprehende as condições de empréstimo e consegue concluir a operação sem dificuldades.
7	Retirar ativos da plataforma	Avaliar a facilidade e confiança do usuário ao realizar a retirada de fundos, garantindo que o fluxo seja transparente e direto.

4.4. Desenvolvimento dos Protótipos

Referências

- Albayati, H., Kim, S. K., and Rho, J. J. (2021). A study on the use of cryptocurrency wallets from a user experience perspective. *Human Behavior and Emerging Technologies*, 3(5):720–738.
- Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media.
- Antonopoulos, A. M. and Wood, G. (2018). *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media.
- ASSILA, A., Oliveira, K., and Ezzedine, H. (2016). Integration of subjective and objective usability evaluation based on iso/iec 15939: A case study for traffic supervision systems. *International Journal of Human-Computer Interaction*, 32.
- Back, A. (2002). Hashcash - a denial of service counter-measure. In *Technical Report*. Acesso em: 9 out. 2025.

- Bangor, A., Kortum, P. T., and Miller, J. T. (2008). An empirical evaluation of the system usability scale. *International Journal of Human–Computer Interaction*, 24(6):574–594.
- Bashir, I. (2018). *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Packt Publishing, 2nd edition.
- Bastien, J. M. C. (2010). Usability testing: a review of some methodological and technical aspects of the method. *International Journal of Medical Informatics*, 79(4):e18–e23.
- Brooke, J. (1996). Sus: A 'quick and dirty' usability scale. In Jordan, P. W., Thomas, B., Weerdmeester, B. A., and McClelland, I. L., editors, *Usability Evaluation in Industry*, pages 189–194. Taylor & Francis.
- Buterin, V. (2014). Ethereum: A next-generation smart contract and decentralized application platform. <https://ethereum.org/en/whitepaper/>.
- Dai, W. (1998). b-money. <http://www.weidai.com/bmoney.txt>. Acesso em: 9 out. 2025.
- for Standardization, I. O. (2018). *Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts*. International Organization for Standardization, Geneva, Switzerland, iso 9241-11:2018(e) edition.
- Foster, M. E., Giuliani, M., and Knoll, A. (2009). Comparing objective and subjective measures of usability in a human-robot dialogue system. In *Proceedings of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP*, pages 879–887, Suntec, Singapore. Association for Computational Linguistics.
- Froehlich, M., Wagenhaus, M. R., Schmidt, A., and Alt, F. (2021). Don't stop me now! exploring challenges of first-time cryptocurrency users. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference*, page 138–148, New York, NY, USA. Association for Computing Machinery.
- Glomann, L., Schmid, M., and Kitajewa, N. (2019). Improving the blockchain user experience - an approach to address blockchain mass adoption issues from a human-centred perspective. In *International Conference on Applied Human Factors and Ergonomics*.
- Gogel, D., Deshmukh, S., Geest, A., Resas, D., Sillaber, C., and Werbach, K. (2021). Defi beyond the hype: The emerging world of decentralized finance.
- Group, N. N. (2023). Usability (user) testing 101. Acessado em: 26 set. 2025.
- Jang, H., Han, S.-H., and Kim, J. H. (2020). User perspectives on blockchain technology: User-centered evaluation and design strategies for dapps. *IEEE Access*, 8:226213–226223.
- Kortum, P. T. and Bangor, A. (2013). Usability ratings for everyday products measured with the system usability scale. *International Journal of Human–Computer Interaction*, 29(2):67–76.
- Lewis, J. R. and Sauro, J. (2009). The factor structure of the system usability scale. In Kurosu, M., editor, *Human Centered Design, HCII 2009, LNCS 5619*, pages 94–103. Springer-Verlag Berlin Heidelberg.

- Moniruzzaman, M., Chowdhury, F., and Ferdous, M. S. (2020). Examining usability issues in blockchain-based cryptocurrency wallets. In Bhuiyan, T., Rahman, M. M., and Ali, M. A., editors, *Cyber Security and Computer Science. ICONCS 2020*, volume 325 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 637–653. Springer, Cham.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>. Acesso em: 9 out. 2025.
- Nielsen, J. (1994). *Usability Engineering*. Morgan Kaufmann, San Francisco, CA.
- Nielsen, J. and Molich, R. (1990). Heuristic evaluation of user interfaces. In *International Conference on Human Factors in Computing Systems*.
- Preece, J., Rogers, Y., and Sharp, H. (2002). *Interaction Design: Beyond Human-Computer Interaction*. Wiley, New York, NY, 1st edition.
- Rosenbaum, K. (2019). *Grokking Bitcoin*. Manning Publications, Shelter Island, NY.
- Rubin, J. and Chisnell, D. (2008). *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*. Wiley Publishing, Inc., Indianapolis, IN, 2 edition.
- Saldivar, J., Martínez-Vicente, E., Rozas, D., Valiente, M.-C., and Hassan, S. (2023). Blockchain (not) for everyone: Design challenges of blockchain-based applications. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA. Association for Computing Machinery.
- Sauro, J. and Lewis, J. R. (2012). *Quantifying the User Experience: Practical Statistics for User Research*. Morgan Kaufmann.
- Shneiderman, B. and Plaisant, C. (2004). *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. Pearson/Addison Wesley, Boston, 4 edition.
- Si, J. J., Sharma, T., and Wang, K. Y. (2024). Understanding user-perceived security risks and mitigation strategies in the web3 ecosystem. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA. Association for Computing Machinery.
- Tullis, T. S. and Stetson, J. N. (2004). A comparison of questionnaires for assessing website usability. In *Proceedings of the UPA 2004 Conference*, Minneapolis, MN. Usability Professionals' Association. Disponível em: https://www.researchgate.net/publication/228920282_A_Comparison_of_Questionnaires_for_Assessing_Website_Usability.
- Voskobojnikov, A., Wiese, O., Koushki, M. M., Roth, V., and Beznosov, K. (2021). The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*.
- Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Technical report, Ethereum Project Yellow Paper. Acesso em: 9 out. 2025.