Fundamentos e Aplicações da Blockchain: Um Estudo de Caso em Autenticidade

Fundamentals and Applications of Blockchain: A Case Study in Authenticity

Vinicius de Paola Barbieri*

Orientador: Prof. Dr. Rómulo Alberto Castillo Cardenas†

2025

Resumo

O mercado tradicional de ingressos para eventos, apesar de digitalizado, sofre com falhas crônicas de autenticidade, como fraudes, falsificações e a ação de cambistas, gerando perdas financeiras e insegurança. Este trabalho argumenta que a arquitetura Web3, baseada em blockchain, oferece uma solução superior para garantir a autenticidade e a propriedade verificável de ativos digitais. O objetivo deste artigo é analisar os fundamentos da blockchain e suas aplicações, validando esta tese através de um estudo de caso prático, o "FanPass". A metodologia combinou pesquisa bibliográfica dos fundamentos (Web3, NFTs e Abstração de Conta) com o desenvolvimento de uma Prova de Conceito (PoC) na Chiliz Chain. A solução implementou inovações-chave: a tokenização de ingressos como NFTs (ERC-721) para garantir autenticidade e a Abstração de Conta (AA) via Biconomy para prover uma experiência de usuário acessível (login social e transações *gasless*). Os resultados demonstram que a arquitetura Web3 com Abstração de Conta é uma solução de engenharia viável que unifica a segurança criptográfica com a usabilidade necessária para adoção em massa.

Palavras-chave: Blockchain. Autenticidade. NFT. Abstração de Conta. Web3.

*Graduando em Ciência e Tecnologia pela Universidade Federal de Santa Catarina (UFSC), Centro Tecnológico de Joinville.

†Professor na Universidade Federal de Santa Catarina (UFSC).

Abstract

The traditional event ticketing market, despite digitalization, suffers from chronic authenticity failures such as fraud, counterfeiting, and ticket scalping. These issues generate financial losses for organizers and an insecure experience for fans. This paper argues that a Web3 architecture, based on blockchain, offers a superior solution for guaranteeing authenticity and verifiable ownership of digital assets. The objective of this study is to analyze blockchain fundamentals and validate this thesis through a practical case study, "FanPass". The methodology combined bibliographic research with the development of a Proof of Concept (PoC) on the Chiliz Chain. The solution implemented key innovations: ticket tokenization as NFTs (ERC-721) to ensure authenticity and Account Abstraction (AA) via Biconomy to provide an accessible user experience (social login and gasless transactions). The results show that Web3 architecture with Account Abstraction is a viable engineering solution that unifies cryptographic security with the usability required for mass adoption.

Keywords: Blockchain. Authenticity. NFT. Account Abstraction. Web3.

Data de submissão: 03/12/2025

1 Introdução

O mercado de ingressos para eventos, abrangendo setores de grande impacto cultural como o futebol e concertos, representa um ecossistema econômico de relevância global. Contudo, as soluções digitais atuais, frequentemente baseadas em arquiteturas centralizadas (Web2), ainda enfrentam desafios crônicos. A literatura especializada identifica que sistemas tradicionais sofrem com problemas de falta de transparência, segurança de dados e privacidade (OKOKPUJIE et al., 2025). Entre os principais desafios estão as fraudes e falsificações de ingressos, que prejudicam tanto os consumidores quanto os organizadores (MEYER, 2024; REGNER; URBACH; SCHWEIZER, 2019). Paralelamente, a ação de cambistas (*scalpers*) distorce o mercado e gera frustração nos compradores, enquanto os organizadores perdem o controle sobre o mercado secundário e potenciais receitas de *royalties* (PORTO; CARDOSO; BUSSADOR, 2024).

A persistência desses problemas decorre, em parte, da arquitetura centralizada que cria silos de dados e pontos únicos de falha (PREECE; EASTON, 2020). Neste cenário, a tecnologia blockchain surge como uma solução arquitetônica promissora. Através da tokenização, cada ingresso pode ser emitido como um Token Não Fungível (NFT), geralmente seguindo o padrão ERC-721. Este padrão garante a unicidade criptográfica do ativo digital, tornando-o seguro, inalterável e impossível de falsificar (REGNER; URBACH; SCHWEIZER, 2019). Diferente de um banco de dados centralizado, a blockchain funciona como um livro-razão distribuído e imutável, oferecendo transparência total e permitindo a auditoria do histórico de propriedade (OKOKPUJIE et al., 2025).

No entanto, a adoção da Web3 enfrenta barreiras significativas de usabilidade, como a gestão complexa de chaves privadas e taxas de transação (*gas*), o que dificulta o acesso ao usuário comum. Diante disso, este trabalho levanta a questão: como estruturar uma arquitetura de software que resolva os problemas de autenticidade sem comprometer a experiência do usuário?

Este artigo argumenta que a aplicação da blockchain, especificamente através da união entre NFTs (ERC-721) e a Abstração de Conta (*Account Abstraction*), oferece uma

arquitetura superior para o mercado de ingressos. O objetivo deste trabalho é analisar os fundamentos dessa tecnologia e demonstrar sua viabilidade através de um estudo de caso, a Prova de Conceito (PoC) "FanPass", desenvolvida na *Chiliz Chain*. A solução proposta visa unificar a segurança criptográfica da Web3 com a usabilidade acessível da Web2.

O restante deste trabalho está estruturado da seguinte forma: a Seção 2 revisa os fundamentos teóricos da tecnologia blockchain e o conceito de Abstração de Conta. A Seção 3 apresenta o desenvolvimento da PoC FanPass e suas decisões de arquitetura. A Seção 4 realiza uma análise comparativa com abordagens tradicionais e, por fim, a Seção 5 apresenta as conclusões e trabalhos futuros.

2 Fundamentação Teórica

A tecnologia blockchain, introduzida em 2008, propôs uma solução para um problema central da ciência da computação: como estabelecer confiança entre partes desconhecidas em uma rede digital sem a supervisão de uma autoridade central (NAKAMOTO, 2008). Este capítulo detalha os fundamentos dessa arquitetura e sua evolução para uma plataforma computacional programável.

2.1 Arquitetura Blockchain e a Confiança Digital

O comércio na Internet depende quase exclusivamente de instituições financeiras que atuam como "terceiros confiáveis" (*trusted third parties*) para processar pagamentos (NAKAMOTO, 2008). Este modelo, embora funcional, possui fraquezas inerentes, como custos de mediação. O principal obstáculo que historicamente impediu um sistema de dinheiro eletrônico puramente *peer-to-peer* (P2P) é o problema do "gasto duplo" (*double-spending*).

2.2 Pilares Conceituais da Blockchain

Para alcançar este consenso distribuído, a arquitetura da blockchain se baseia em três pilares conceituais: criptografia, uma estrutura de dados encadeada e um mecanismo de consenso.

2.2.1 Criptografia e Integridade

A blockchain utiliza dois fundamentos criptográficos principais para garantir segurança e autenticidade. O primeiro são as **Funções de Hash Criptográficas**, algoritmos que mapeiam dados de tamanho arbitrário para uma sequência de bits de tamanho fixo, gerando uma "impressão digital" (*fingerprint*) única para cada bloco de dados (LUCKS, 2004). Qualquer alteração mínima na entrada resulta em um hash completamente diferente, garantindo a integridade dos dados armazenados.

O segundo pilar é a **Criptografia Assimétrica** (ou Criptografia de Chave Pública). Diferente da criptografia simétrica, comumente associada à confidencialidade, no contexto da blockchain este mecanismo desempenha a função crítica de garantir a **autenticidade** e o **não-repúdio**.

O sistema opera através de um par de chaves matematicamente vinculadas: uma Chave Privada (secreta) e uma Chave Pública (acessível a todos). Na prática, o proprietário de um ativo utiliza sua Chave Privada para gerar uma **Assinatura Digital** sobre os dados de uma transação. Os nós da rede utilizam a Chave Pública correspondente para verificar

matematicamente a validade dessa assinatura. Esse processo assegura que a transação foi inequivocamente autorizada pelo detentor da chave privada, sem que o segredo precise ser revelado à rede (NAKAMOTO, 2008).

2.2.2 Estrutura de Dados (Blocos e Cadeia)

A estrutura de dados que dá nome à tecnologia é uma "cadeia de blocos" (*block chain*). Um bloco é um contêiner de dados que agrupa as transações validadas e é estruturalmente dividido em duas partes principais: o Corpo (que contém os dados) e o Cabeçalho (que contém os metadados de validação).

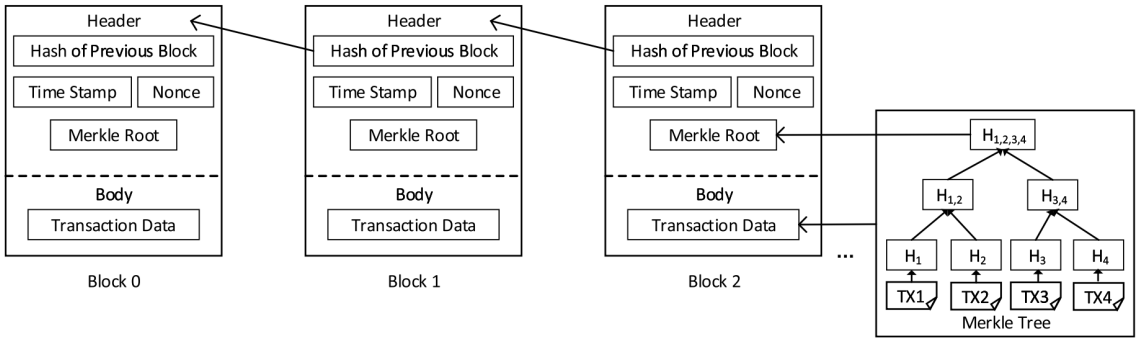
O **Corpo do Bloco** armazena a lista completa de todas as transações que o minerador decidiu incluir. Para garantir a integridade desse conjunto de dados de forma eficiente, as transações são "hasheadas em uma Merkle Tree". Este processo resulta em um único hash, a **Raiz Merkle (Merkle Root)**, que funciona como um resumo criptográfico ou "impressão digital" de todas as transações no corpo.

O **Cabeçalho do Bloco** é a estrutura que contém os **metadados de validação e encadeamento**. Ele armazena os seguintes elementos-chave:

- **O Hash do Bloco Anterior:** O ponteiro criptográfico que "acorrenta" este bloco ao seu predecessor, garantindo a ordem cronológica.
- **O Timestamp:** O carimbo de tempo (em formato Unix) de quando o bloco foi minerado.
- **A Raiz Merkle (Merkle Root):** O hash único (derivado da Árvore de Merkle) que valida a integridade de todas as transações no Corpo do Bloco.
- **O Nonce:** Um número arbitrário que é usado como variável de tentativa no processo de validação.

O "Hash do Bloco" (o identificador único do bloco) é o resultado criptográfico da aplicação de uma função de hash sobre todo o Cabeçalho. O processo de encontrar um "Hash do Bloco"que seja aceito pela rede é a responsabilidade do Mecanismo de Consenso.

Figura 1 – Estrutura de blocos na Blockchain



Fonte: Liang (2020)

2.2.3 Mecanismos de Consenso: Evolução do PoW ao PoS

Para que os participantes da rede (nós) concordem sobre qual cadeia é a correta sem uma autoridade central, a rede precisa de um Mecanismo de Consenso. O Bitcoin introduziu o modelo pioneiro conhecido como *Proof-of-Work* (PoW) (NAKAMOTO, 2008).

O PoW é um sistema que exige dos participantes (mineradores) um esforço computacional significativo para validar um novo bloco. Este processo não é a resolução de uma equação algébrica, mas sim um processo de **força-bruta computacional**.

As máquinas testam iterativamente milhões de valores para o **Nonce** por segundo. Para cada tentativa, elas calculam o hash de todo o Cabeçalho. O objetivo é encontrar um "Hash Válido", definido por uma **condição de Dificuldade**. A rede define um valor-limite, conhecido como **Alvo (Target)**, e um hash é considerado válido se, numericamente, for *menor* que esse Alvo (ex: iniciando com '0000...').

A rede ajusta essa Dificuldade periodicamente para garantir que um novo bloco seja encontrado em um tempo médio constante. É essa exigência de trabalho que torna a manipulação inviável: para alterar uma transação antiga, um atacante precisaria refazer o trabalho (minerar) não apenas daquele bloco, mas de todos os subsequentes, superando a velocidade de toda a rede honesta combinada (NAKAMOTO, 2008).

Contudo, o PoW apresenta limitações de escalabilidade e alto consumo energético. Em resposta, surgiram mecanismos alternativos, sendo o *Proof-of-Stake* (PoS) o mais relevante para a Web3 moderna. No PoS, a segurança não deriva do gasto de energia, mas de incentivos econômicos: validadores travam tokens como garantia (*stake*) para ter o direito de propor blocos.

Essa distinção é fundamental para este trabalho. A rede utilizada no estudo de caso (Chiliz Chain) utiliza o consenso *Proof-of-Stake Authority* (PoSA). Este modelo sacrifica parte da descentralização extrema do PoW em troca de maior escalabilidade, taxas de transação reduzidas e eficiência energética, características essenciais para viabilizar um mercado de ingressos de alto volume.

2.3 A Evolução para a Web3: Plataformas Programáveis

O Bitcoin provou a viabilidade da blockchain como um sistema monetário (Blockchain 1.0), mas seu design possuía limitações que impediram o desenvolvimento de aplicações mais complexas (BUTERIN, 2014). A linguagem de script do Bitcoin não era *Turing-complete* (não permitia *loops*) e seu modelo de transações era "sem estado" (*stateless*), limitando-se a registrar "gasto" ou "não gasto" (BUTERIN, 2014).

A emergência da Web3 (ou Blockchain 2.0) foi impulsionada pelo Ethereum, uma plataforma que introduziu "uma blockchain com uma linguagem de programação *Turing-complete* embutida" (BUTERIN, 2014). O objetivo desta nova arquitetura é permitir que desenvolvedores criem e implantem **Smart Contracts** (Contratos Inteligentes).

Um *smart contract* é um programa autônomo implantado na blockchain. Pode ser metaforicamente definido como uma "caixa criptográfica que [...] só o desbloqueia se certas condições forem atendidas" (BUTERIN, 2014). Essas condições são definidas em código, que é executado de forma distribuída e determinística pela *Ethereum Virtual Machine* (EVM) (OKOKPUJIE et al., 2025; BUTERIN, 2014).

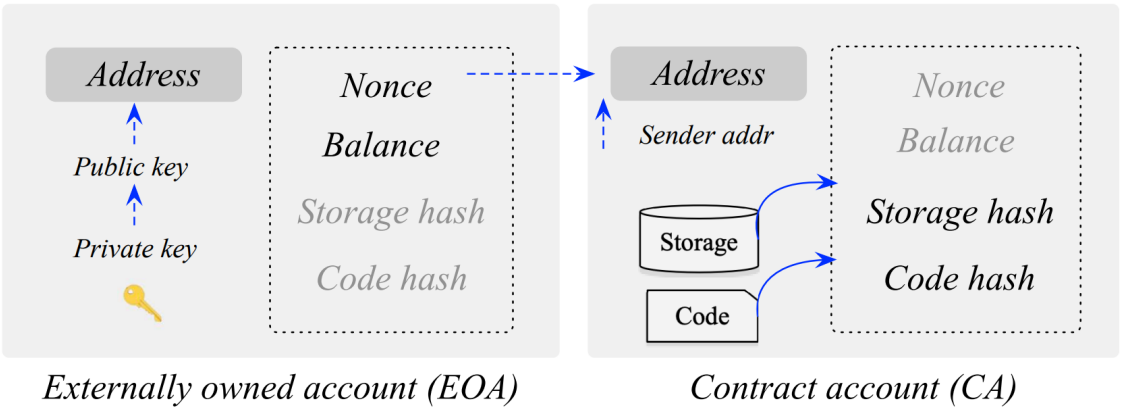
Para permitir isso, o Ethereum substituiu o modelo de Saídas Não Gastas (UTXOs) do Bitcoin pelo "Modelo de Contas com Estado" (BUTERIN, 2014). Conforme ilustrado

na Figura 2, existem dois tipos de contas:

- **Contas de Proprietário Externo (EOA):** Controladas por usuários através de **chaves privadas**. São as únicas que podem iniciar transações.
- **Contas de Contrato (CA):** Controladas exclusivamente pelo código do *smart contract* nelas implantado. Elas apenas reagem a transações recebidas e possuem armazenamento ('Storage') e lógica ('Code').

A interação na rede ocorre quando uma EOA (usuário) envia uma "mensagem" (transação) para uma CA, ativando seu código (BUTERIN, 2014). Como a EVM é *Turing-complete*, o Ethereum implementou um mecanismo de taxação computacional chamado **Gas** para prevenir ataques de *loops* infinitos. O Gas é o "cripto-combustível" da rede: toda operação computacional tem um custo, e o usuário (a EOA) deve pagar uma taxa (em Gas) para que sua transação seja executada e validada pelos mineradores (BUTERIN, 2014).

Figura 2 – Diferença estrutural entre EOA (controlada por chave) e CA (controlada por código)



Fonte: Wang e Chen (2023)

2.4 Tokenização (NFTs) e o Desafio da Usabilidade

Uma das aplicações mais poderosas dos *smart contracts* é a *tokenização*. O padrão **ERC-721**, ou Token Não Fungível (NFT), é pilar da autenticidade digital, pois a não-fungibilidade é a característica de um ativo que é "único", "distinguível" e "indivisível" (REGNER; URBACH; SCHWEIZER, 2019).

Enquanto tokens fungíveis (ERC-20) são intercambiáveis, cada token ERC-721 é criptograficamente único (OKOKPUJIE et al., 2025). Essa capacidade de garantir a autenticidade e a proveniência torna o padrão ERC-721 a ferramenta ideal para o mercado de ingressos, que funcionam como um "ingresso de tipo usuário único" (OKOKPUJIE et al., 2025).

Contudo, o modelo de Contas de Proprietário Externo (EOA) introduz um gargalo de usabilidade (UX) significativo para a adoção em massa:

1. **Gestão de Chaves:** A dependência de chaves privadas (introduzida na Seção 2.3) é complexa e arriscada. A perda da chave pelo usuário resulta na perda permanente do acesso aos ativos (WANG; CHEN, 2023).

2. **Taxas de "Gas":** A necessidade de pagar *gas* (introduzida na Seção 2.3) em cada transação obriga o usuário a possuir a criptomoeda nativa da rede, criando uma barreira de entrada e fricção contínua (BUTERIN, 2014; REGNER; URBACH; SCHWEIZER, 2019; WANG; CHEN, 2023).

Essas limitações de UX são o principal obstáculo para a adoção de soluções Web3 pelo público geral, exigindo uma solução de engenharia que abstraia essa complexidade.

2.5 A Solução de Engenharia: Abstração de Conta

A **Abstração de Conta (AA)** surge como a principal solução para o gargalo de usabilidade. Formalizada na EIP-4337, a AA é uma atualização fundamental na arquitetura do Ethereum que visa "melhorar a acessibilidade do usuário" (WANG; CHEN, 2023).

O conceito central é tornar as contas dos usuários "programáveis". Em vez de uma EOA (controlada por uma chave privada), a Abstração de Conta permite que a "carteira"do usuário seja, na verdade, um *smart contract* (uma Conta de Contrato) (WANG; CHEN, 2023). Isso permite inovações cruciais:

- **Transações Patrocinadas (Gasless):** A AA permite a implementação de "meta-transações", um método onde redes de *retransmissores (relay)* pagam o *gas* em nome do usuário, que pode então pagar a taxa em outro token ou tê-la patrocinada pela aplicação (tornando-a *gasless* para o usuário) (UBAMADU et al., 2022).
- **Login Social e Recuperação:** Ao dissociar a conta da chave privada, a AA permite métodos de autenticação flexíveis, como login social (via e-mail) ou mecanismos de "recuperação social", onde um usuário pode recuperar o acesso à sua conta sem depender de uma *seed phrase* (WANG; CHEN, 2023).

Esta abordagem, como será visto no estudo de caso, é a ponte que unifica a segurança criptográfica da Web3 com a experiência de usuário acessível da Web2.

3 Estudo de Caso: A Prova de Conceito FanPass

Após a fundamentação teórica, este capítulo apresenta o estudo de caso prático que valida a tese deste trabalho. O estudo de caso é a Prova de Conceito (PoC) "FanPass" (BARBIERI; BARROS, 2025), uma plataforma Web3 desenvolvida para validar a aplicação da blockchain no mercado de ingressos.

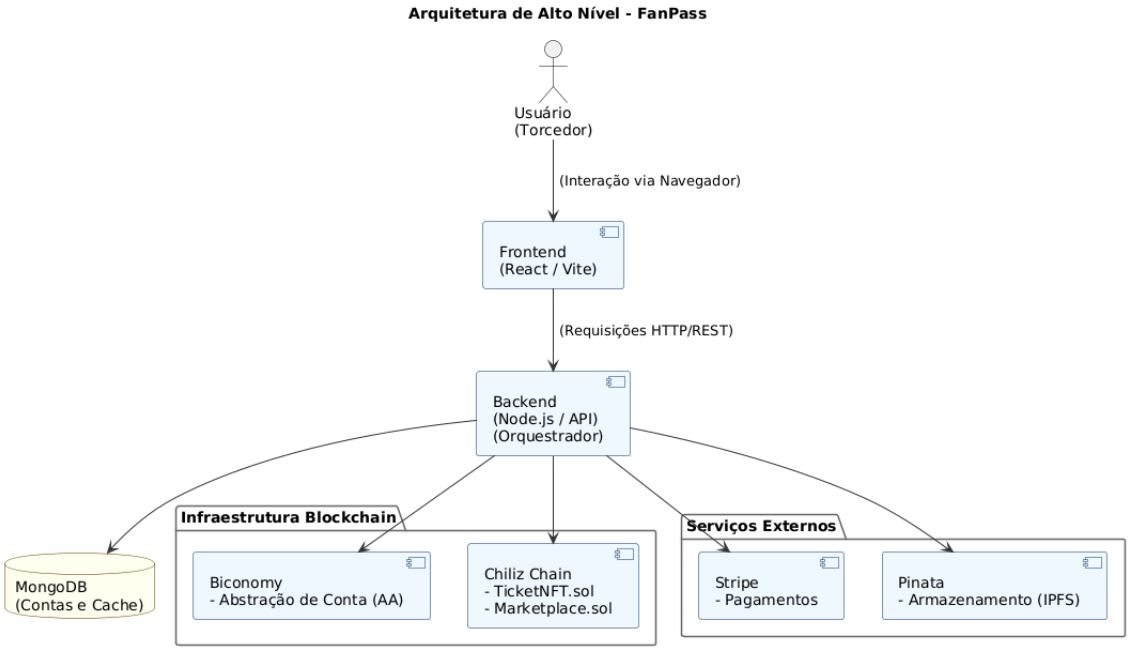
O FanPass foi projetado com três objetivos centrais:

1. **Transformar Ingressos em Ativos:** Tokenizar ingressos como NFTs (ERC-721) para garantir autenticidade e propriedade durável.
2. **Novos Modelos de Receita:** Permitir que os clubes implementem *royalties* automáticos sobre a revenda desses ingressos-NFT.
3. **Prover uma Experiência Web2:** Abstrair a complexidade da blockchain para o usuário final, oferecendo login social e transações *gasless*.

3.1 Arquitetura de Alto Nível

Para atingir esses objetivos, a PoC foi arquitetada em um **modelo de 3 camadas (Frontend, Backend e Blockchain)** que desacopla a experiência do usuário da complexidade da blockchain, ilustrado na Figura 3. Um *Backend* (Orquestrador) atua como o intermediário central, gerenciando as requisições do *Frontend* e orquestrando as interações com a infraestrutura blockchain (Chiliz Chain e Biconomy).

Figura 3 – Diagrama da Arquitetura de Alto Nível do FanPass



Fonte: Autoria própria

3.1.1 Fluxo de Validação e Acesso (Arquitetura Proposta)

Para responder à questão operacional do acesso físico ao evento, a arquitetura do FanPass prevê um módulo de validação (Gatekeeper). Embora a implementação atual da PoC tenha focado nas camadas de emissão e transação, o fluxo de acesso foi projetado para garantir que a posse do token se traduza em entrada física sem vulnerabilidades de cópia.

O fluxo projetado opera da seguinte maneira:

1. **Solicitação de Uso:** Na entrada do evento, o usuário acionará a função "Utilizar Ingresso" na interface.
2. **Assinatura de Prova:** A aplicação solicitará à carteira (Smart Account) uma assinatura criptográfica de uma mensagem temporária (*challenge*), gerando um QR Code dinâmico que contém não apenas o ID do token, mas essa prova de posse assinada.
3. **Validação em Tempo Real:** O dispositivo do validador lerá o QR Code e consultará o estado atual na blockchain. O acesso só é liberado se: (1) a assinatura for válida para aquele endereço e (2) aquele endereço ainda for o proprietário do NFT naquele exato segundo.

Este mecanismo garante que, se o usuário vender o ingresso minutos antes do evento, o QR Code antigo (ou um *print*) será invalidado instantaneamente pela rede, pois a propriedade na blockchain terá mudado.

3.2 Justificativa das Decisões de Design

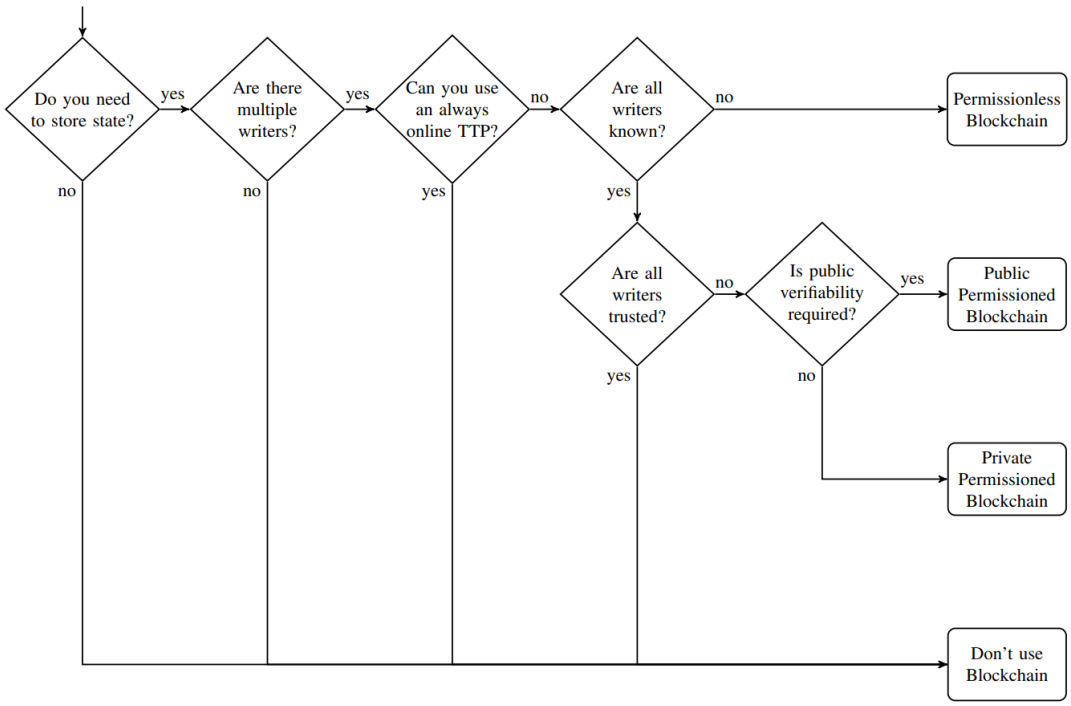
As escolhas de engenharia do FanPass respondem diretamente aos desafios identificados na literatura para validar a tese deste artigo.

3.2.1 A Escolha pela Blockchain Pública (Chiliz Chain)

A decisão arquitetural pelo uso de uma blockchain pública foi fundamentada no framework decisório proposto por Wüst e Gervais (WüST; GERVAIS, 2018), conforme ilustrado na Figura 4. A aplicação satisfaz os critérios de necessidade de armazenamento de estado compartilhado e existência de múltiplos escritores (organizadores emitindo e torcedores transacionando).

Crucialmente, a opção por não depender de uma Terceira Parte Confiável (TTP), visando mitigar riscos de censura e ponto único de falha, aliada ao fato de que os participantes do mercado secundário (fãs) são desconhecidos e não possuem confiança mútua, conduz à classificação da rede necessária como uma *Permissionless Blockchain*.

Figura 4 – Framework de Decisão Proposto por Wüst e Gervais



Fonte: Wüst e Gervais (2018)

Enquanto a literatura demonstra a viabilidade de arquiteturas de blockchain privada (ex: Hyperledger Fabric) para consórcios fechados (PREECE; EASTON, 2020; MEYER, 2024), essas redes não resolvem satisfatoriamente a questão da propriedade incensurável do ativo pelo usuário final em um ambiente de varejo aberto.

Nesse contexto, a escolha da **Chiliz Chain** foi estratégica. Embora opere com um mecanismo de consenso *Proof of Staked Authority* (PoSA), que sacrifica grau de descentralização no nível dos validadores em prol de escalabilidade, ela oferece um ambiente de execução permissionless para os usuários, compatibilidade com EVM e as baixas taxas necessárias para viabilizar microtransações de fãs (HX Entertainment Limited, 2025; VIDAL-TOMÁS, 2023).

3.2.2 A Escolha pelo NFT (ERC-721) como Pilar da Autenticidade

O pilar central da tese deste trabalho é a "autenticidade". A escolha pelo padrão ERC-721 (NFT) é a implementação técnica direta dessa tese. A literatura define os NFTs como a ferramenta ideal para representar a propriedade sobre ativos digitais únicos (REGNER; URBACH; SCHWEIZER, 2019).

Este padrão foi escolhido especificamente porque a **não-fungibilidade** é crucial para o modelo de negócio de ingressos. Cada ingresso (ativo) precisa ter um **histórico de propriedade individual e auditável** (proveniência) e deve ser controlado de forma atômica. O ERC-721 permite que regras de negócio, como *royalties* de revenda, sejam programadas e vinculadas a um 'tokenId' único, algo que padrões fungíveis (ERC-20) ou mesmo semi-fungíveis (ERC-1155) não oferecem com a mesma clareza e robustez para este caso de uso.

3.2.3 A Solução para o Gargalo de Usabilidade (Abstração de Conta)

Conforme discutido na Seção 2.4, o maior desafio para a adoção em massa é a complexidade da UX. A necessidade de que usuários comuns gerenciem chaves privadas e paguem taxas de *gas* é a principal barreira (REGNER; URBACH; SCHWEIZER, 2019; PORTO; CARDOSO; BUSSADOR, 2024).

A solução de engenharia do FanPass foi a implementação da **Abstração de Conta (AA)**, via SDK da Biconomy. O Biconomy é uma plataforma de retransmissores (*relayer*) reconhecida por sua capacidade de implementar "meta-transações", um método onde a própria aplicação patrocina o *gas* em nome do usuário (UBAMADU et al., 2022).

Ao integrar o Biconomy, o FanPass (1) patrocina as taxas de transação, tornando-as *gasless*, e (2) permite um login social (via e-mail), resolvendo o principal problema de UX.

4 Análise e Discussão dos Resultados

A arquitetura do FanPass pode ser melhor compreendida quando comparada analiticamente com as arquiteturas alternativas propostas na literatura, conforme resume o Quadro 1.

Tabela 1 – Análise Comparativa das Arquiteturas de Ingressos

Critério	**Web2 Tradicional**	**Web3 Privada** *(Hyperledger)*	**Web3 Híbrida** *(com BD)*	**FanPass** *(Web3 Púb. + AA)*
Autenticidade	Baseada em confiança	Criptográfica (Limitada)	Parcial (Dados off-chain)	Total (NFT Público)
Propriedade	Inexistente (Licença)	Do consórcio	Ofuscada (Dados em BD)	Plena (Dono do NFT)
Royalties	Nenhum	Teórico (Trabalho Futuro)	Auditabilidade complexa	Nativo (On-chain)
UX (Usuário)	Alta (Simples)	N/A (Foco B2B)	Baixa (Exige *gas*)	Alta (AA, Gasless)

Fonte: Autoria própria.

4.1 FanPass vs. Arquitetura Web2 Tradicional

O modelo Web2 tradicional baseia-se em uma arquitetura centralizada (API + Banco de Dados) (MEYER, 2024; PORTO; CARDOSO; BUSSADOR, 2024). A limitação fundamental desta abordagem não é apenas tecnológica, mas conceitual, e se desdobra em três áreas críticas:

1. **Autenticidade baseada em Confiança, não Verificação:** No modelo Web2, a "autenticidade" é baseada na confiança. O ingresso é apenas uma entrada em um banco de dados privado. O usuário deve confiar que o servidor da empresa (ex: Ticketmaster) é seguro, íntegro e que a empresa não emitirá ingressos duplicados (MEYER, 2024). Esta arquitetura de "caixa-preta" é a raiz dos problemas crônicos de fraude, pois o consumidor não pode verificar publicamente a proveniência ou a validade de um ingresso no mercado secundário.

2. **Ausência de Propriedade Real:** Fundamentalmente, o modelo Web2 não oferece propriedade real; ele concede uma **licença de uso** revogável. O usuário não é dono do ingresso, mas sim de um registro que aponta para ele dentro do sistema da empresa. Esse ingresso fica "preso" no silo de dados da aplicação, sem interoperabilidade.

3. **Controle Centralizado e Ponto Único de Falha:** O intermediário (a tiqueteira) detém controle absoluto sobre o ativo, podendo revogá-lo ou bloquear transferências. Além disso, a infraestrutura centralizada representa um ponto único de falha (*Single Point of Failure*), onde uma falha no servidor da empresa pode tornar todos os ingressos inacessíveis (PREECE; EASTON, 2020).

É pertinente abordar uma crítica comum a esta análise: a indagação se a confiança não poderia ser estabelecida apenas via **Certificação Digital** (PKI), sem o uso de blockchain. Embora assinaturas digitais garantam a integridade e a autenticidade do emissor (provando que o ingresso foi gerado pelo organizador), elas não resolvem, isoladamente, o problema do **gasto duplo** (ou clonagem) em um ambiente de mercado secundário.

Um arquivo digital assinado (como um ingresso em PDF com certificado) pode ser copiado infinitamente; a assinatura criptográfica permanece válida em todas as cópias. Para impedir que múltiplas cópias acessem o evento, um sistema baseado puramente em

PKI reintroduz a necessidade de um **banco de dados central** para validar o estado ("já utilizado" ou "revogado"). A blockchain remove a necessidade desse validador central, transferindo o estado da propriedade para o ativo em si.

O FanPass, portanto, utiliza a criptografia não apenas para assinar, mas para mudar o paradigma de confiança para **verificação de estado**. A autenticidade não é garantida por uma empresa, mas pelo protocolo. O ingresso (NFT) é um ativo digital que reside na carteira inteligente (*Smart Account*) do usuário, garantindo **propriedade digital plena** e interoperabilidade.

Mais importante, o controle é descentralizado. Em vez de um intermediário ditar as regras do mercado secundário, as regras (como *royalties* para o criador do evento) são programadas diretamente no *smart contract*, permitindo que os organizadores recuperem o controle e a receita de transações secundárias (REGNER; URBACH; SCHWEIZER, 2019).

4.2 FanPass vs. Arquitetura Web3 Privada (Hyperledger)

A literatura apresenta estudos robustos utilizando blockchains permissionadas, como o Hyperledger Fabric (PREECE; EASTON, 2020). Essas redes são eficazes para a governança de consórcios (ex: clubes de futebol) (MEYER, 2024). Contudo, essa abordagem não resolve a questão da propriedade real para o fã; o ingresso ainda existe dentro de um ecossistema fechado.

Uma análise da pesquisa local (MEYER, 2024) sobre o uso de Hyperledger revela um ponto crucial: embora o estudo tenha validado o Fabric para o gerenciamento, ele identificou a implementação de NFTs e um "Mercado com royalties" como "Trabalhos Futuros". O estudo de caso FanPass avança precisamente nesta lacuna, implementando na prática as funcionalidades que o estudo anterior com Hyperledger apenas pôde sugerir como uma evolução teórica.

4.3 FanPass vs. Arquitetura Web3 Híbrida (Blockchain + BD Off-chain)

Outra abordagem encontrada na literatura é a híbrida, exemplificada por Porto, Cardoso e Bussador (2024). Nesse modelo, um banco de dados NoSQL (MongoDB) é mantido *off-chain* (fora da blockchain) para armazenar "informações de usuários e histórico de vendas". Embora essa arquitetura possa melhorar o desempenho, ela reintroduz um ponto de falha centralizado e, crucialmente, **compromete a transparência total**. Se o histórico de vendas (a proveniência) está em um banco de dados privado, a auditoria pública do ativo é ofuscada.

O FanPass, embora também utilize um banco de dados *off-chain* (MongoDB), o faz de maneira fundamentalmente diferente. Conforme a arquitetura da PoC, o MongoDB é utilizado estritamente para: (1) **Dados de Aplicação Web2**, como a autenticação de usuários (e-mail, senha) e a vinculação da identidade Web2 à carteira ('publicKey'); e (2) **Cache e Dados Comerciais**, como o preço do ingresso e seu *status* atual (ex: "à venda", "alugado").

Em contrapartida, a **fonte da verdade**, a propriedade do ingresso (o NFT) e o histórico imutável de suas transferências (proveniência), permanece 100% *on-chain* e é gerenciada pelo *smart contract*. Desta forma, o FanPass utiliza o banco de dados para garantir uma UX acessível (login social) e performance (cache), sem sacrificar o pilar da autenticidade e proveniência auditável da Web3.

4.4 Limitações do Estudo de Caso

É imperativo conduzir uma análise honesta das limitações do FanPass. Trata-se de uma Prova de Conceito (PoC) desenvolvida no contexto restrito de um *hackathon*, e não um produto comercial finalizado. O foco foi validar a arquitetura central (Autenticidade via NFT) e a inovação de UX (Abstração de Conta).

5 Considerações Finais

Este trabalho se propôs a analisar a viabilidade da tecnologia blockchain como uma solução arquitetônica para os problemas crônicos de autenticidade no mercado de ingressos (MEYER, 2024; PORTO; CARDOSO; BUSSADOR, 2024). Os resultados obtidos corroboram a hipótese de que a arquitetura Web3, fundamentada na tokenização de ingressos como NFTs (ERC-721), oferece uma alternativa robusta para ampliar a garantia de autenticidade e o controle programável desses ativos (REGNER; URBACH; SCHWEIZER, 2019).

A principal contribuição deste artigo foi a **demonstração da viabilidade técnica** desta abordagem através do estudo de caso "FanPass". A Prova de Conceito (PoC) buscou não apenas replicar as soluções de autenticidade baseadas em NFT já estabelecidas (OKOKPUJIE et al., 2025; REGNER; URBACH; SCHWEIZER, 2019), mas explorar avanços em duas frentes críticas:

1. **Domínio e Royalties:** O estudo de caso implementou NFTs com *royalties* programáveis em uma blockchain pública (Chiliz Chain) de domínio específico para a indústria do esporte (VIDAL-TOMÁS, 2023; HX Entertainment Limited, 2025). Ao fazer isso, o trabalho avançou experimentalmente naquilo que pesquisas anteriores em arquiteturas privadas (MEYER, 2024) haviam identificado como "Trabalho Futuro".
2. **Usabilidade e Adoção:** O FanPass buscou mitigar o principal gargalo de adoção da Web3: a complexidade da UX e a necessidade de pagar "taxas de *gas*" (REGNER; URBACH; SCHWEIZER, 2019; PORTO; CARDOSO; BUSSADOR, 2024). A PoC endereçou este desafio ao implementar uma arquitetura de Abstração de Conta (AA) (WANG; CHEN, 2023), utilizando o Biconomy para prover "transações sem *gas*" (*gasless*) e login social (UBAMADU et al., 2022).

Em síntese, o FanPass **evidencia o potencial** de uma arquitetura de engenharia que unifica duas qualidades anteriormente distantes: a segurança e a autenticidade criptográfica da Web3 com a acessibilidade e a usabilidade fluida da Web2.

Apesar dos resultados promissores, a pesquisa possui limitações inerentes ao escopo de PoC, que não foi submetida a uma auditoria de segurança rigorosa ou testes de carga em ambiente de produção. Como trabalhos futuros, sugere-se a realização desta auditoria, o aprofundamento na Abstração de Conta para implementar a "recuperação social" (*social recovery*) (WANG; CHEN, 2023), e a análise de escalabilidade da rede sob alta demanda.

Referências

BARBIERI, V. D. P.; BARROS, M. M. de. *FanPass: Prova de Conceito de Ingressos NFT com Abstração de Conta*. [S.l.]: GitHub, 2025. <https://github.com/vinibarbieri/FanPass>. Acessado: 03 dez. 2025. Citado na página 7.

BUTERIN, V. *A Next-Generation Smart Contract and Decentralized Application Platform*. [S.l.], 2014. Disponível em: <https://ethereum.org/en/whitepaper/>. Citado 3 vezes nas páginas 5, 6 e 7.

HX Entertainment Limited. *Chiliz White Paper Version 1.0.0*. [S.l.], 2025. Disponível em: <https://docs.chiliz.com/>. Citado 2 vezes nas páginas 10 e 13.

LIANG, Y.-C. Blockchain for dynamic spectrum management. In: *Dynamic Spectrum Management*. [S.l.]: Springer Singapore, 2020. p. 121–146. Citado na página 4.

LUCKS, S. *Design Principles for Iterated Hash Functions*. [S.l.], 2004. E-print (September 29, 2004). Disponível em: <http://th.informatik.uni-mannheim.de/people/lucks/>. Citado na página 3.

MEYER, R. N. *Sistema para a comercialização de ingressos de futebol utilizando o framework Hyperledger Fabric*. Trabalho de Conclusão de Curso (Ciências da Computação) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, Santa Catarina - Brasil, 2024. Citado 5 vezes nas páginas 2, 9, 11, 12 e 13.

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [S.l.], 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Citado 3 vezes nas páginas 3, 4 e 5.

OKOKPUJIE, K. et al. A single-user electronic ticketing system using erc-721 protocol for smart contracts. *Bulletin of Electrical Engineering and Informatics*, v. 14, n. 4, p. 3110–3120, August 2025. Citado 4 vezes nas páginas 2, 5, 6 e 13.

PORTO, P. H. R.; CARDOSO, L. d. S.; BUSSADOR, A. Venda de ingressos online com autenticação via blockchain na web3.0. In: *Anais do 21º Congresso Latino-americano de Software Livre e Tecnologias Abertas (Latin.Science 2024)*. Foz do Iguaçu, Brasil: [s.n.], 2024. Citado 5 vezes nas páginas 2, 10, 11, 12 e 13.

PREECE, J. D.; EASTON, J. M. Blockchain technology as a mechanism for digital railway ticketing. In: *2019 IEEE International Conference on Big Data (Big Data)*. [S.l.: s.n.], 2020. p. 3599–3606. Citado 4 vezes nas páginas 2, 9, 11 e 12.

REGNER, F.; URBACH, N.; SCHWEIZER, A. Nfts in practice - non-fungible tokens as core component of a blockchain-based event ticketing application. In: *Proceedings of the 40th International Conference on Information Systems (ICIS 2019)*. Munich, Germany: [s.n.], 2019. Citado 6 vezes nas páginas 2, 6, 7, 10, 12 e 13.

UBAMADU, B. C. et al. Optimizing smart contract development: A practical model for gasless transactions via facial recognition in blockchain. *International Journal of Multidisciplinary Research and Growth Evaluation*, v. 3, n. 1, p. 978–989, Jan/Feb 2022. Citado 3 vezes nas páginas 7, 10 e 13.

VIDAL-TOMÁS, D. Blockchain, sport and fan tokens. *Journal of Economic Studies*, April 2023. Citado 2 vezes nas páginas 10 e 13.

WANG, Q.; CHEN, S. Account abstraction, analysed. *arXiv preprint arXiv:2309.00448*, 2023. Citado 3 vezes nas páginas 6, 7 e 13.

WüST, K.; GERVAIS, A. Do you need a blockchain? In: *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. [S.l.]: IEEE, 2018. p. 45–54. Citado na página 9.

Agradecimentos

Agradeço ao Prof. Dr. Rómulo Alberto Castillo Cardenas pela orientação e apoio fundamentais na condução deste trabalho.

Estendo minha gratidão ao Matheus Mascarenhas de Barros, pela colaboração no desenvolvimento do FanPass durante o hackathon da Chiliz.