Carbono 21: Mecanismos de Transparência e Auditoria de Blockchains Permissionadas Aplicados à Promoção de Florestamento por Tokenização de Ativos

Pedro Henrique Barcha Correia[1], **Marcos Antonio Simplicio Junior**[1]

[1]Laboratório de Arquitetura e Redes de Computadores (LARC)
Universidade de São Paulo (USP)

{pedro.correia,msimplicio}@usp.br

Abstract. *Apesar de seus benefícios ambientais, o florestamento (i.e., plantio de árvores e preservação de vegetação nativa) é frequentemente preterido por atividades agrícolas mais lucrativas, porém ambientalmente prejudiciais. Em resposta, este trabalho fomenta o florestamento por meio de incentivos financeiros criados a partir da tokenização de ativos verdes. Mais especificamente, áreas florestadas e ativos ambientais são representados por Tokens Infungíveis (NFTs) em uma blockchain de consórcio. Diante do caráter permissionado desse tipo de rede, são propostos mecanismos de transparência para a auditoria de transações e da utilização dos ativos tokenizados. Esses mecanismos, foco deste documento, são essenciais para assegurar a adequada promoção do florestamento na plataforma e podem ser estendidos a blockchains permissionadas em geral, ampliando sua transparência e auditabilidade.*

1. Introdução

Para enfrentar os desafios impostos pelas mudanças climáticas, diversas iniciativas de florestamento (i.e., ações voltadas ao plantio e à manutenção de árvores ou vegetação nativa) foram propostas nas últimas décadas. Destacam-se os mercados de carbono, que geram certificados de redução de emissões de CO2, e as leis de compensação ambiental. No Brasil, esta última iniciativa permite compensar desmatamentos adquirindo direitos de compensação de proprietários que preservam vegetação nativa.

1.1. Definição do problema e motivação

Em geral, as iniciativas de florestamento apresentam diversos desafios que este trabalho busca solucionar. Um problema recorrente é sua **baixa rentabilidade** para os proprietários de terra, levando à preferência por monoculturas de alto impacto, como cana e soja. Há também **falta de transparência** do ciclo de vida de ativos ambientais (e.g., créditos de carbono e direitos de compensação), dificultando sua auditoria e gerando riscos como o gasto duplo de ativos.

Outro problema é a viabilização de créditos de carbono, que exige grandes extensões de terra, tornando o **mercado de créditos de carbono inacessível a pequenos proprietários**. Em contraste, a compensação ambiental brasileira aceita áreas a partir de 1 hectare e engloba biomas não florestais, como o Cerrado, o que permite a participação de proprietários de pequenas terras ou terras inférteis para culturas convencionais.

Apesar disso, a maioria das plataformas de florestamento foca na digitalização e negociação de unidades de carbono [Moss nd]. As poucas soluções que exploram alternativas como a compensação ambiental [Trustt 2025] ainda apresentam baixa rentabilidade e **não incorporam múltiplas estratégias de florestamento**, o que limita sua contribuição ambiental e adesão de usuários. Além disso, as plataformas digitais existentes não oferecem mecanismos confiáveis para acompanhar a situação dos ativos reais correspondentes aos digitalizados, permitindo **representações digitais que divergem da realidade**, o que cria margem para fraudes e negociação de ativos ilegítimos.

2. Objetivos

Este trabalho tem como objetivo desenvolver a **Carbono 21, uma plataforma digital destinada a promover florestamento por meio de ativos ambientais digitalizados**. Baseando-se nas lacunas identificadas na literatura – detalhadas na Seção 3.2 da dissertação de mestrado do autor [Correia and Simplicio 2024]) –, esta proposta apoia-se em dois pilares que representam os objetivos específicos do trabalho:

- **Pilar I – Mecanismos de transparência** para garantir a correta implementação dos esforços ambientais. Esses mecanismos devem fornecer: (a) transparência dos dados reais, permitindo o acompanhamento do estado de ativos de florestamento e eventos de desmatamento; e (b) transparência dos dados digitais da plataforma, incluindo a operação dos ativos digitais.
- **Pilar II – Mecanismos versáteis**, adaptáveis a múltiplas iniciativas de florestamento e legislações. Os mecanismos devem facilitar a aquisição de ativos ambientais para além do mercado de carbono. Para proprietários, devem tornar o florestamento mais atrativo e permitir iniciativas que favoreçam pequenas terras e biomas menos férteis.

Nota: Este documento concentra-se principalmente nos mecanismos de transparência de dados digitais (Pilar Ib), por serem mais diretamente ligados à Segurança de Sistemas Computacionais. Detalhes sobre os Pilares Ia e II podem ser encontrados na dissertação [Correia and Simplicio 2024].

3. Carbono 21 e auditoria de blockchains permissionadas

A plataforma digital proposta, Carbono 21, permite que **Proprietários** de terras solicitem que seus ativos ambientais sejam digitalizados. Em seguida, os **Administradores** do sistema validam a documentação enviada e emitem Tokens Infungíveis (*Non-Fungible Tokens* – NFTs) correspondentes aos ativos reais. Os proprietários são então recompensados financeiramente ao longo do tempo se preservarem a vegetação correspondente aos ativos tokenizados, a qual é monitorada via satélite e bases governamentais (Pilar Ia). Contratos inteligentes são utilizados para conferir versatilidade às regras de negócio, permitindo a adaptação do sistema a diferentes legislações e iniciativas de florestamento (Pilar II).

Após tokenizados, os ativos ambientais podem ser vendidos na plataforma para **Compradores** interessados, por exemplo, em utilizar esses ativos para fins legais relacionados à compensação ambiental ou de carbono. Para aumentar a confiança no sistema, as transações são gerenciadas (isto é, executadas, verificadas e armazenadas) não apenas pelos Administradores da Carbono 21, mas por uma **Federação** composta por entidades relevantes, como órgãos ambientais e universidades. Essa Federação constitui uma rede blockchain de consórcio, criada com Hyperledger Fabric 2.5. Esse tipo de rede

adota um modelo permissionado, no qual apenas entidades previamente autorizadas (e supostamente confiáveis) podem participar da rede. Isso possibilita o uso de protocolos de consenso leves e energeticamente eficientes, alinhados aos objetivos ambientais do projeto. Além disso, diferentemente das blockchains públicas, uma blockchain permissionada permite que as transações sejam gerenciadas apenas por organizações efetivamente interessadas nos dados. Outro benefício é a governança compartilhada: políticas da rede e contratos inteligentes (i.e., as regras de negócios) são acordados coletivamente pelos membros da Federação.

Embora blockchains permissionadas apresentem vantagens para o cenário da Carbono 21, elas tendem a oferecer menor transparência do que blockchains públicas [Correia et al. 2024]. Mesmo que o acesso de leitura seja aberto, observadores externos não possuem mecanismos para validar diretamente o comportamento dos nós da Federação. Isso difere de blockchains públicas, onde qualquer entidade pode se tornar um nó e acompanhar a atividade dos demais. Assim, em ambientes permissionados, a detecção de fraudes – como modificação de blocos passados e execução de transações inválidas – torna-se difícil para entidades externas [Kimura et al. 2024], aqui denominadas **Monitores**. No contexto da Carbono 21, isso significaria que Compradores, Proprietários e ONGs, por exemplo, não conseguiriam auditar adequadamente o sistema e suas iniciativas de florestamento.

Para contornar esse problema, o presente trabalho adota a publicação periódica do estado da blockchain pela Federação no InterPlanetary File System (IPFS), um sistema de compartilhamento de arquivos baseado em Peer-to-Peer (P2P). As publicações são assinadas digitalmente pelos nós da rede e podem ser armazenadas e gerenciadas por Monitores. Isso permite que esses atores comparem, a qualquer momento, o estado passado da blockchain (fornecido diretamente pela Federação) com o estado passado e canônico armazenado no IPFS. Consequentemente modificações indevidas na blockchain podem ser detectadas e os responsáveis podem ser identificados, o que, na prática, tende a desencorajar esse tipo de ataque.

Diferente de trabalhos da literatura que armazenam apenas o último bloco [Robinson and Brainard 2019], a solução proposta estende esse conceito, salvando *append-only logs* (i.e., publicações encadeadas por hash) de diversos dados relevantes no IPFS (conforme detalhado na Seção 4.2.1.3 da dissertação [Correia and Simplicio 2024]). Isso permite a detecção não apenas de modificações em blocos passados, mas de múltiplos ataques feitos pela Federação, conforme explicado na próxima seção. Além disso, implementa-se um processo automatizado de auditoria de blockchains permissionadas, assim como uma interface avançada de inspeção para especialistas. Outra contribuição da solução é permitir a recuperação da blockchain (*fork*) para um estado seguro anterior ao ataque, por meio do armazenamento periódico do *world state* (i.e., um sumário da blockchain) no IPFS.

4. Resultados: Ataques detectáveis

A análise a seguir é realizada sob a perspectiva dos Monitores, buscando avaliar sua capacidade de detectar ataques realizados por um ou mais membros da Federação (incluindo a própria Carbono 21). Para essa análise, assume-se que, ao solicitar blocos da blockchain, o Monitor envia requisições para todos os nós da Federação. Note que tanto

os *append-only logs*, acessíveis via IPFS, como os blocos fornecidos diretamente pela Federação são assinados digitalmente pelos nós da rede e, portanto, os Monitores conseguem produzir evidências em casos de ataque.

Table 1. Alguns ataques que nós da Federação podem realizar e como Monitores podem detectá-los. Ataques marcados com (*) exigem Monitores especializados, enquanto os demais são detectados automaticamente pela ferramenta.

Ataque (pela Federação)	Descrição	Detecção (pelo Monitor)
Modificação furtiva	Modificação do conteúdo da blockchain	Recomputar a cadeia de hashes
Modificação da cadeia de hashes	Modificação da blockchain e atualização da cadeia de hashes	Comparar a blockchain com os *append-only logs*
Visão dividida (*split-view*)	Versões distintas do mesmo bloco são mostradas para diferentes usuários	Comparar a blockchain com os *append-only logs*
Transação inválida (*)	Uma transação não definida nos contratos inteligentes é aprovada	Simular a transação usando o suposto contrato correspondente
Contrato alternativo	Um contrato diferente dos anunciados é implantado	Verificar se o hash do contrato em questão está registrado na blockchain
Contrato malicioso (*)	O contrato implementa regras que beneficiam a Federação indevidamente	Inspecionar o código-fonte
Criação ilegítima de NFT	Um NFT que não corresponde a um ativo real é criado	Verificar os metadados do NFT

A Federação pode realizar um ataque de **modificação furtiva** ao criar, remover ou alterar blocos indevidamente (e.g., para criar tokens para nós da rede). Note, no entanto, que a modificação de um bloco consolidado quebraria a cadeia de hashes e, portanto, o Monitor poderia detectar a fraude reconstruindo a cadeia de hashes. Para evitar isso, a Federação poderia recalcular e **modificar a cadeia de hashes** de acordo. Contudo, comparar a blockchain atual (fornecida pela Federação) com os *append-only logs* no IPFS revelaria a fraude, uma vez que o IPFS contém um histórico de blocos canônicos. Esse mecanismo também permite a detecção de ataques de visão dividida (ou **split-view**), nos quais versões diferentes do mesmo bloco são apresentadas a usuários distintos.

Nos ataques anteriores, as transações forjadas ainda obedecem às regras do contratos inteligentes implantados na rede. Entretanto, os nós também podem realizar um ataque de **transação inválida**, executando operações que não seguem as regras definidas pelos contratos (e.g., movimentação não autorizada de tokens de carteiras arbitrárias). Para detectar esse comportamento, o Monitor deve simular localmente a transação utilizando o respectivo suposto contrato inteligente implantado na rede e comparar os resultados obtidos com aqueles fornecidos pela Federação [Kimura et al. 2024]. Assume-se, portanto, que os contratos que ditam as regras de negócio possuem código-fonte aberto. Note que no Hyperledger Fabric e em blockchains permissionadas em geral, seria possível identificar de maneira irretratável os nós responsáveis por executar e validar transações inválidas, uma vez que tais ações são assinadas digitalmente.

No Hyperledger Fabric, após a aprovação de um novo contrato inteligente pela rede, um evento contendo o hash do contrato é registrado na blockchain. Esse mecanismo permite a detecção de ataques de **contratos alternativos**, nos quais a Federação implanta um programa distinto do alegado. Considerando novamente que os contratos implantados pela rede são disponibilizados com código aberto, Monitores podem calcular seus hashes e compará-los aos valores registrados na blockchain. Note que caso a Federação, em

conluio, registre um hash fraudado na blockchain, na prática seria possível detectar as transações inválidas do contrato alternativo, conforme explicado anteriormente.

Ainda sobre os benefícios de contratos inteligentes de código aberto, vale mencionar que esses programas proporcionam transparência de governança aos usuários. Permite-se, assim, uma compreensão mais aprofundada da lógica de negócios do sistema, incluindo as operações que são permitidas com seus tokens. Combinando isso com as verificação acima de que o programa é de fato o implantado pela rede, é possível averiguar que a Federação não executa um **código malicioso** que a favoreça. No entanto, deve-se mencionar que, embora ofereça garantias contra ataques da Federação, um contrato de código aberto pode representar maior risco de ataques provenientes de entidades externas. A ampla disponibilização do software permite que agentes mal-intencionados o analisem em busca de vulnerabilidades. Consequentemente, ataques de dia zero – cujo impacto é desconhecido *a priori* – podem ser facilitados, uma vez que os potenciais atacantes não precisam recorrer a técnicas de engenharia reversa para compreender os mecanismos do contrato. Para mitigar esse problema, recomenda-se instituir consultas públicas ao código, utilizar ferramentas de detecção de vulnerabilidades em contratos inteligentes como o Slither [Feist et al. 2019] e, possivelmente, contratar empresas especializadas em auditoria desse tipo de software para avaliá-lo antes de sua implantação.

Em relação ao contexto específico de tokenização, a ferramenta de auditoria proposta permite a detecção da **criação de NFTs ilegítimos**, que não representam um ativo real de fato. No caso da Carbono 21, apenas Administradores do sistema possuem autorização para criar NFTs e, portanto, poderiam criar ativos fraudulentos, como créditos de carbono inexistentes ou já consumidos, para se favorecer. Para detectar esse tipo de ataque, propõe-se adicionar um conjunto de informações e documentações nos metadados dos NFT, de modo a comprovar a legitimidade do ativo subjacente. Note, porém, que, a depender do contexto em que essa abordagem é utilizada, há de se realizar um balanço entre transparência e privacidade, uma vez que a informação inserida no token torna-se pública. No caso da Carbono 21, alguns ativos ambientais devem ser auditados através de documentações privadas. Assim, esses documentos só podem ser entregues a Monitores mediante autorização de seus proprietário. Considera-se essa a maior limitação da solução de auditoria proposta, conforme elaborado na Seção 6.2 da dissertação [Correia and Simplicio 2024].

5. Contribuição e considerações finais

As propostas identificadas na literatura que utilizam IPFS para aumentar a transparência de blockchains permissionadas normalmente são direcionadas a domínios específicos, como votação eletrônica [Liu et al. 2023]. Em contraste, a solução apresentada na dissertação independe da aplicação e é agnóstica, oferecendo uma plataforma de transparência para blockchains permissionadas quaisquer. O resultado é uma ferramenta que permite a detecção de ataques feitos pela Federação e de seus responsáveis de maneira irretratável, o que, na prática, desencoraja comportamento adversarial. Além disso, dado que a publicação no IPFS ocorre em intervalos consideráveis (uma vez ao dia ou a cada hora), a solução não introduz gargalos. Essa afirmação é corroborada pelos experimentos descritos em detalhes na Seção VI-B de [Correia et al. 2025].

Assim, o trabalho propõe uma ferramenta inédita de auditoria de blockchains per-

missionadas, cujas principais contribuições são:

1. Agregação de mecanismos de transparência conhecidos em uma única ferramenta, incluindo: leitura de blocos, reconstrução do encadeamento de hashes da blockchain [Nakamoto 2008] e armazenamento periódico de partes da blockchain no IPFS [Kimura et al. 2024, Al-Sarray et al. 2024];
2. Novos mecanismos de auditoria: adaptação do mecanismo de IPFS para o formato *append-only logs*; utilização do Interplanetary Name System (IPNS) para facilitar a obtenção dos logs, inclusive por meio de subscrição (vide Seção 4.2.1.3 da dissertação [Correia and Simplicio 2024]); e mecanismo de detecção de implantação de contratos inteligentes distintos dos alegados pela rede.
3. Automação dos mecanismos de auditoria, facilitando a detecção de ataques de modificação do conteúdo da blockchain, ataques de visão fragmentada e uso de contratos inteligentes ilegítimos em blockchains permissionadas;
4. Interface para auditoria aprofundada, permitindo que entidades especializadas identifiquem transações ilegítimas;
5. Mecanismo que possibilita a recuperação (*fork*) da blockchain a estados prévios a ataques realizados pela rede;
6. Disponibilização da ferramenta, integrada com Hyperledger Fabric 2.5 e IPFS[1].

Além dessas contribuições para as áreas de Segurança da Informação e Sistemas Distribuídos, a dissertação aplica os mecanismos de transparência propostos ao contexto da Carbono 21, levando ao cumprimento do Pilar Ib (i.e., transparência dos dados digitais, descrito na Seção 2). Esse pilar é essencial para que a plataforma promova efetivamente o florestamento, uma vez que permite que Monitores verifiquem seu correto funcionamento. Isto inclui a auditoria da criação, utilização e negociação dos ativos digitalizados, de sua situação no mundo real e também da lógica de negócios da plataforma, o que inclui as operações permitidas à Federação e aos usuários.

Devido ao espaço limitado, este documento apresenta apenas uma visão geral do sistema Carbono 21, o qual é explicado em detalhes na dissertação [Correia and Simplicio 2024]. Para sintetizar suas contribuições: enquanto trabalhos relacionados propõem métodos pouco confiáveis e com baixa escalabilidade para monitorar ativos ambientais [ForestCoin nd, OFP 2023], a Carbono 21 suporta bases governamentais e imagens de satélite de alta resolução (Pilar Ia); e a plataforma possui uma arquitetura flexível capaz de suportar incentivos financeiros ao florestamento e adaptar-se a diferentes legislações, biomas e iniciativas ambientais, inclusive aquelas acessíveis a pequenos produtores (Pilar II). Como contribuição adicional, o trabalho implementa e avalia experimentalmente o sistema Carbono 21. Seu código-fonte está disponível mediante solicitação[2]. Além de atingir os objetivos de transparência e versatilidade (Pilares I e II), o sistema apresentou desempenho satisfatório, sendo capaz de consultar mais de 1400 ativos por segundo e criar mais de 700 ativos digitais por segundo (aproximadamente 60 milhões por dia), dependendo da configuração de rede utilizada. Considerando que o Brasil possuía cerca de 8,1 milhões de imóveis rurais ativos em 2020 [Governo brasileiro 2020], os resultados indicam que a solução é viável e escalável, conforme discutido nas seções 5 e 6 da dissertação [Correia and Simplicio 2024].

[1] `https://github.com/Carbon-21/fabric-transparency`
[2] `https://github.com/Carbon-21/4orgs-ERC1155`

6. Subprodutos

Ao longo dos três anos de projeto, diversos subprodutos foram gerados.

6.1. Artigos

As principais produções decorrentes da dissertação de mestrado são:

- **Periódico Qualis A1**: Correia, P. H. B., Marques, M. A., Pillon, M. A., Miers, C. C., and Simplicio, M. A. Carbono 21: Promoting Forestation Through Asset Tokenization. IEEE Access (2025).
- **Conferência Qualis A1**: Correia, P. H. B., Marques, M. A., Simplicio, M. A., Ermlivitch, L., Miers, C. C., and Pillon, M. A. Comparative analysis of permissioned blockchains: Cosmos, Hyperledger Fabric, Quorum, and XRPL. IEEE International Conference on Blockchain (2024).
- Correia, P. H. B., Martins, O. V., and Simplicio, M. A. Mecanismos de Transparência e Auditoria de Blockchains Permissionadas. Anais Estendidos do XXV Simpósio Brasileiro de Cibersegurança (SBSeg), 2025.
- Bunn, C. D., Neto, M. P. P., Pillon, M. A., Miers, C. C., Correia, P. H. B., Marques, M. A., and Simplicio, M. A. Comparative Analysis of Consensus Protocols in Blockchains: IBFT 2.0, QBFT, and SmartBFT. IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON) (2025).

6.2. Prêmios e apresentações

Em 2025, o trabalho "Mecanismos de Transparência e Auditoria de Blockchains Permissionadas" recebeu menção honrosa no *Salão de Ferramentas* do SBSeg. Já em 2023, a Carbono 21 recebeu o *Selo de Inovação*, concedido pela Sociedade Brasileira de Computação (SBC)[3]. A premiação foi obtida por meio de uma competição que avalia projetos acadêmicos inovadores. A etapa final ocorreu durante o Congresso da SBC (CSBC) de 2023, em João Pessoa, onde o autor apresentou a Carbono 21.

O projeto também foi apresentado a professores e estudantes da Universidade de Groningen (Países Baixos) durante o intercâmbio do autor, no evento Bite of Science. Além disso, o trabalho foi exposto no evento UBRI Connect 2024, realizado na Universidade de Zurique (Suíça)[4].

6.3. Software

O código-fonte da prova de conceito da Carbono 21 está disponível no GitHub[5] (acesso sob solicitação). Além disso, a ferramenta de auditoria de blockchains permissionadas possui código-fonte aberto[6]. A ferramenta inclui um portal de transparência e se integra ao IPFS e ao Hyperledger Fabric 2.5.

6.4. Startup

Este projeto de pesquisa resultou na criação da *startup* Carbono 21. A empresa encontra-se incubada no Centro de Inovação, Empreendedorismo e Tecnologia (CIETEC) da Universidade de São Paulo (USP)[7]. O protótipo atualmente encontra-se no nível de maturi-

[3] https://tinyurl.com/yjpmzfp4

[4] https://web.archive.org/web/20240831134442/https://www.ubriconnect.com

[5] https://github.com/Carbon-21/4orgs-ERC1155

[6] https://github.com/Carbon-21/fabric-transparency

[7] https://cietec.org.br/empresas/carbon-21/

dade tecnológica TRL-4 (*Technology Readiness Level* 4). O sistema está hospedado nos servidores do Laboratório de Arquitetura e Redes de Computadores (LARC/USP) e ainda não está disponível publicamente. O próximo passo consiste na realização de estudos de caso com proprietários rurais e demais partes interessadas, visando levar a solução ao mercado. Apesar disso, a plataforma já vem sendo divulgada. Atualmente, o produto possui uma página web[8], uma página no LinkedIn[9] e uma conta no Instagram[10], que conta com 568 seguidores no momento da escrita.

References

Al-Sarray, A. M., Hamdani, T. M., and Alimi, A. M. (2024). Decentralized distribution for secure GAN using IPFS with the Hyperledger blockchain. In *2024 IEEE ATSIP*, volume 1, pages 110–115.

Correia, P. H. B., Marques, M. A., Pillon, M. A., Miers, C. C., and Simplicio, M. A. (2025). Carbono 21: Promoting forestation through asset tokenization. *IEEE Access*, 13:179711–179732.

Correia, P. H. B., Marques, M. A., Simplicio, M. A., Ermlivitch, L., Miers, C. C., and Pillon, M. A. (2024). Comparative analysis of permissioned blockchains: Cosmos, Hyperledger Fabric, Quorum, and XRPL. In *2024 IEEE Blockchain*, pages 464–469.

Correia, P. H. B. and Simplicio, M. A. (2024). Carbono 21: Promovendo florestamento utilizando tokenização. Master's thesis, University of São Paulo. Disponível em: `https://repositorio.usp.br/item/003232385`.

Feist, J., Grieco, G., and Groce, A. (2019). Slither: a static analysis framework for smart contracts. In *2019 IEEE/ACM 2nd international workshop on emerging trends in software engineering for blockchain (WETSEB)*, pages 8–15. IEEE.

ForestCoin (n.d.). White paper. `https://tinyurl.com/4baxhbph`.

Governo brasileiro (2020). Estatísticas e Dados Abertos dos Imóveis Rurais. `https://tinyurl.com/mvy6rn3v`.

Kimura, L. T., Shiraishi, F. K., Andrade, E. R., Carvalho, T. C., and Simplicio, M. A. (2024). Amazon biobank: Assessing the implementation of a blockchain-based genomic database. *IEEE Access*.

Liu, Z., Zhang, X., Lao, L., Li, G., and Xiao, B. (2023). DBE-voting: A privacy-preserving and auditable blockchain-based e-voting system. In *ICC 2023-IEEE International Conference on Communications*, pages 6571–6577. IEEE.

Moss (n.d.). White paper. `https://tinyurl.com/bdh756x6`.

Nakamoto, S. (2008). Bitcoin whitepaper. `bitcoin.org/bitcoin.pdf`.

OFP (2023). White paper. `https://tinyurl.com/nt533b8a`.

Robinson, P. and Brainard, J. (2019). Anonymous state pinning for private blockchains. In *2019 IEEE TrustCom/BigDataSE*, pages 827–834.

Trustt (2025). Trustt Green. `https://tinyurl.com/3n5k8xu3`.

[8] `http://carbono21.com.br/`
[9] `https://br.linkedin.com/company/carbono-21`
[10] `https://www.instagram.com/carbono21_/?hl=en`