

**Uso de blockchain para o armazenamento de dados na microchipagem animal:
considerações a partir de um estudo experimental**

*Use of blockchain for data storage in animal microchipping:
considerations from an experimental study*

Gisele Brandão KANDA¹
Marcelo AOKI²

Resumo

A pesquisa investigou a aplicabilidade da tecnologia blockchain no armazenamento de dados de microchipagem animal a partir de um experimento em laboratório. O protótipo em Python permitiu análises sobre a viabilidade técnica, a complexidade da infraestrutura, os custos operacionais e as dinâmicas de construção, atualização e consulta de dados. O estudo revelou as dificuldades na complexidade da infraestrutura blockchain em comparação com soluções tradicionais de armazenamento. Destacou-se a importância da escolha da arquitetura, do conhecimento dos processos de registro de informações e do equilíbrio dos custos e incentivos para garantir a participação e a segurança contínua dos nós da rede. Apesar dos desafios, a blockchain apresenta vantagens na integridade e autenticidade dos registros, fornecendo reflexões valiosas para futuras pesquisas e implementações na gestão de informações.

Palavras-chave: Redes distribuídas. Blockchain. Banco de dados. Microchipagem animal.

Abstract

The research investigated the applicability of blockchain technology for storing animal microchip data through a laboratory experiment. The Python prototype enabled analyses of technical feasibility, infrastructure complexity, operational costs, and the dynamics of data construction, updating, and querying. The study revealed the challenges posed by blockchain infrastructure complexity compared to traditional storage solutions. It highlighted the importance of architecture selection, knowledge of information registration processes, and balancing costs and incentives to ensure continuous participation and security of network nodes. Despite the challenges, blockchain offers advantages in record integrity and authenticity, providing valuable insights for future research and implementations in information management.

Keywords: Distributed Networks. Blockchain. Database. Animal Microchipping.

¹ Graduada em Análise e Desenvolvimento de Sistemas, Faculdade de Tecnologia de São Paulo (FATEC-SP). E-mail: gisele.kanda@fatec.sp.gov.br

² Especialista em Gestão de Projetos e Processos Organizacionais pelo Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS). Professor do Curso de Análise e Desenvolvimento de Sistemas, Faculdade de Tecnologia de São Paulo (FATEC-SP). E-mail: marcelo.aoki@fatec.sp.gov.br

Introdução

Nos últimos anos, o segmento de animais de estimação tem experimentado um crescimento significativo, estabelecendo-se como um dos setores mais promissores da economia. Segundo a Associação Brasileira da Indústria de Produtos para Animais (2023), o Brasil possui uma população de aproximadamente 167,6 milhões de animais de estimação. A relação entre as pessoas e seus animais ultrapassou a ideia de apenas companheiros, tornando-os membros da família. Essa mudança de percepção impactou diretamente o mercado, que em 2022 alcançou um faturamento mundial de US\$149,8 bilhões. O Brasil destacou-se como o terceiro maior mercado, representando 4,95% desse faturamento global, atrás apenas da China 8,7% e dos Estados Unidos 43,78% segundo a Associação Brasileira da Indústria de Produtos para Animais de Estimação (2023).

Um dos avanços tecnológicos relevantes para esse mercado é a microchipagem de animais. A microchipagem consiste na implantação de um microchip subcutâneo contendo um código único de identificação que equivale a um documento de identidade. Esse registro numérico aponta para dados existentes em um banco de dados. Exemplos práticos de uso podem incluir a localização de donos no caso de animais perdidos, registro do histórico de saúde, transferência de propriedade, certificação *pedigree*, entre outras informações.

Não há, contudo, políticas bem definidas sobre esse banco de dados sendo que cada empresa ou jurisdição no mundo é responsável pela definição das regras. Por exemplo, na publicação do *Consejo Andaluz de Colegios Oficiales de Veterinarios*, (2020), na Espanha, cada uma das 17 comunidades autônomas tem seu banco de dados e somente recentemente foram unificadas para fins de busca de animais por meio da iniciativa *Red Española de Identificación de Animales de Compañía*. Além disso, muitas tecnologias conectadas a bancos de dados privados apresentam pouca transparência em relação às regras de inserção, atualização e consulta de dados. Isso gera algumas dificuldades para localizar veterinários habilitados com a tecnologia do microchip a fim de realizar consultas e atualizações adequadas. Essa questão se torna especialmente inconveniente em situações como viagens, mudanças de domicílio ou residências em cidades remotas.

O objetivo deste estudo é discutir a viabilidade da aplicação da tecnologia de blockchain como banco de dados para a microchipagem animal, visando aprimorar a segurança, a transparência e a eficiência no armazenamento e o gerenciamento das

informações relacionadas aos animais de estimação, a partir de um experimento realizado em laboratório.

Microchipagem animal

O implante de microchip em animais tem se tornado cada vez mais comum, em alguns países, como Israel e Austrália, leis foram promulgadas para tornar a microchipagem de animais de estimação obrigatória (Fram; Rivlin e Beredjiklian, 2020; Lancaster *et al.*, 2015; Rizvi, Para e Ganguly, 2016).

O microchip funciona como um identificador digital que associa os animais às suas informações em um banco de dados externo, atuando como uma âncora digital, permitindo que esses dados sejam vinculados de forma segura e rastreável ao animal correspondente.

Os microchips inseridos em animais domésticos funcionam através da tecnologia de Identificação por Radiofrequência. Fundamentalmente, essa tecnologia é composta por três elementos distintos (Lott, 2011):

- i. O microchip, geralmente, é feito de vidro biocompatível para minimizar os impactos no organismo do animal, tem o tamanho de um grão de arroz e contém uma estrutura interna de silício, cobre e ferrite, cuja informações são acessadas pela tecnologia de Identificação por Radiofrequência.
- ii. O microchip não dispõe de uma fonte interna de energia, dependendo, assim, do scanner para fornecer energia e realizar a leitura. Uma vez energizado, o microchip emite sinais de rádio que são captados pelo scanner, transmitindo o número de identificação único.
- iii. No banco dados as informações pertinentes são subsequentemente recuperadas a partir do número de identificação, por meio de uma base de dados.

Tecnologia de ledger distribuído

O Blockchain³ é um dos principais exemplos de Tecnologia de Ledger Distribuído (DLT, *Distributed Ledger Technology*) (Zhou et al., 2022). Um *ledger*, em tradução para

³ O termo *blockchain* é a combinação das palavras *block* “bloco” e *chain* “cadeia” (Xu; Chen; Kou, 2019).

o português, é um livro-razão, também conhecido como registro contábil e seu termo é adotado em razão de sua origem a partir do contexto da tecnologia de registro de transações na ciência contábil. Apesar disso, é preferível manter o termo original *ledger* dado que atualmente, no contexto de DLT, o termo assume significado próprio usado para descrever tanto (i) o conjunto de dados mantido por um nó de rede individual, quanto (ii) o conjunto de dados mantidos em comum pela maioria dos nós de uma rede (Rauchs et al., 2018). Dessa forma, a DLT é uma abordagem para registrar e compartilhar informações de forma descentralizada e segura, e a Blockchain é uma implementação específica dessa tecnologia.

Segundo Natarajan, Krause e Gradstein (2017) o conceito central da DLT é criar um *ledger* que será mantido por várias cópias em diferentes “nós” de uma rede. Em uma rede de computadores, os “nós” são os dispositivos individuais conectados à rede que podem receber, processar e transmitir dados. Essas cópias são sincronizadas e atualizadas pela rede, e qualquer alteração nos dados requer um consenso entre a maioria dos participantes da rede.

Uma rede descentralizada é caracterizada pela distribuição do controle e da tomada de decisões entre vários nós, em oposição à centralização em um único agente. Nesse modelo, os participantes possuem alguma autonomia para tomar decisões localmente, mas ainda podem depender de uma entidade central em certos momentos.

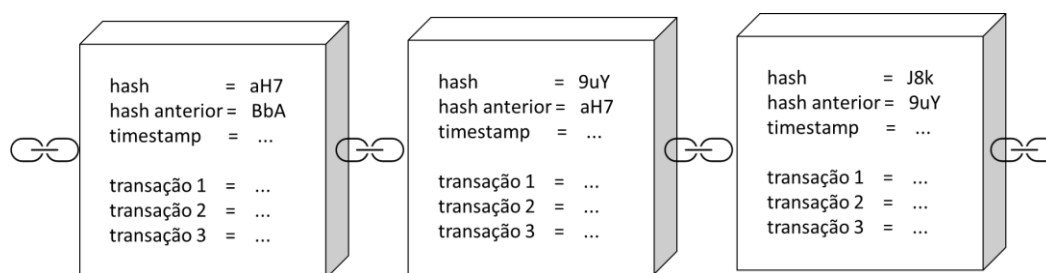
É importante mencionar que a Blockchain não é a única forma de implementação da DLT. Existem vários tipos de DLT além do Blockchain como Gráfico Acíclico Direcionado (DAG), Hashgraph, Holochain, Cerberus etc. (Zhou et al., 2022).

Blockchain

Blockchain pode ser definida como uma estrutura de dados compartilhada entre os nós de uma rede distribuída, que armazena dados em blocos interligados por meio de criptografia, permitindo que as transações sejam verificadas (Xu; Chen; Kou, 2019). Tabatabaei, Vitenberg e Veeraragavan (2023) definem o blockchain como uma tecnologia de registro distribuído que proporciona armazenamento e transferência de dados de forma segura, transparente e à prova de falsificação. Para auxiliar o entendimento, ilustra-se o funcionamento de uma blockchain, segundo Natarajan, Krause e Gradstein (2017):

1. Os dados são organizados como uma cadeia de blocos, onde cada bloco está ligado ao anterior, como ilustrado na figura 1. Segundo Dhar, Khare e Singh (2022) esses blocos podem armazenar diferentes tipos de informações, como ativos, transações ou condições. O encadeamento dos blocos de informações ocorre por meio do *hash*, que é construído a partir de uma função matemática criptográfica conhecida como função de *hash*. Cada bloco contém o *hash* do bloco anterior e seu próprio *hash*, garantindo que qualquer alteração em um bloco mude completamente o *hash* do bloco seguinte. Isso torna a cadeia de blocos segura, pois uma mudança em um bloco quebra a continuidade da cadeia, deixando claro que houve uma modificação.

Figura 1 - Representação de uma estrutura de Blockchain



Fonte: elaborado pelos autores.

2. A adição de novos dados começa com um dos membros da rede, também chamado de "nó", criando um bloco de informações que contém vários registros de transações. Para adicionar esse bloco à blockchain, pode ser necessário passar por um processo chamado "mineração". Nessa etapa, os nós da rede competem para resolver um problema matemático complexo, o que requer muito poder computacional. O processo é intencionalmente difícil e demorado para garantir a segurança e a integridade dos dados armazenados na blockchain.
3. As informações referentes a esse novo bloco de dados são, em seguida, disseminadas por toda a rede.
4. Antes de um bloco ser adicionado à blockchain, todos os participantes da rede precisam concordar que as transações nele contidas são válidas, esse mecanismo de consenso é alcançado por meio de algoritmos. Somente após essa validação, o novo bloco é adicionado aos respectivos *ledgers* de todos os membros.

A Blockchain é distribuída em uma rede de nós, onde cada nó possui uma cópia completa do histórico da blockchain, permitindo criar redundância e resistência a falhas. A descentralização impede que uma única entidade tenha controle sobre toda a rede, o que aumenta a segurança, pois torna mais difícil para um atacante comprometer a rede, já que seria necessário controlar a maioria dos nós (Pilkington, 2016).

Mecanismos de consenso

No sistema descentralizado da blockchain, onde não existe uma autoridade central, é necessário que haja um mecanismo para garantir que todos os participantes na rede concordem com o estado atual do *ledger*, é nesse contexto que entram os mecanismos de consenso (Lashkari e Musilek, 2021).

Ao invés de depender de uma autoridade central para verificar e validar transações, a blockchain permite que os “nós” (participantes da rede) cheguem a um consenso sobre o estado de registro. Como o *ledger* está distribuído, os participantes da rede precisam interagir e chegar a um acordo sobre as atualizações (Lashkari e Musilek, 2021). Atualmente, os acordos sobre as atualizações podem ser alcançados por diversos algoritmos, sendo os mecanismos de consenso mais utilizados a Prova de Trabalho (*Proof of Work*) e a Prova de Participação (*Proof of Stake*) (Yan, 2022).

A Prova de Trabalho foi introduzida pela primeira vez por Cynthia Dwork e Moni Naor em 1993. O algoritmo exige que os mineradores resolvam um quebra-cabeça computacionalmente intensivo antes de adicionar um novo bloco à blockchain. Esse quebra-cabeça foi projetado para ser difícil de resolver, mas fácil de verificar. Os mineiros competem para resolver o quebra-cabeça, e o primeiro minerador a resolvê-lo adiciona o próximo bloco ao blockchain e recebe uma recompensa (Sriman; Ganesh e Shamili, 2021).

No algoritmo de Prova de Participação, os participantes não precisam resolver problemas matemáticos difíceis. Ao invés disso, a habilidade de validar transações e criar blocos é influenciada pela quantidade de criptomoeda que o participante detém e está disposto a depositar como garantia (Sriman; Ganesh; Shamili, 2021). Quanto mais moeda um participante possui, maior é a probabilidade de ser escolhido para criar um bloco. Esse método é considerado mais eficiente em termos de consumo de energia, em comparação

com a Prova de Trabalho, que requer uma quantidade significativa de poder computacional (Sriman; Ganesh; Shamili, 2021).

Os mecanismos de consenso constituem um tópico extenso e diversificado, envolvendo algoritmos complexos e cenários específicos para cada rede. Entretanto, para aqueles que desejam compreender mais profundamente sobre o assunto, fornece-se como referências úteis os trabalhos de Lashkari e Musilek (2021) e Xiong *et al.* (2022)

Do experimento em laboratório

A pesquisa desenvolveu um código simplificado de blockchain, em Python 3.12, para registrar e gerenciar informações dos animais, abrangendo dados de propriedade, históricos médicos e eventos relevantes. Optou-se pela programação orientada a objetos por facilitar a modelagem de objetos do mundo real, melhorando a compreensão do funcionamento e relacionamento entre as entidades envolvidas. Cinco classes foram criadas, cada uma desempenhando um papel na estrutura da rede: a) o Microchip Animal, incorpora um código de identificação único, servindo como a identidade digital de um animal de estimação, a quem os dados inseridos na blockchain se referem; b) a Entidade veterinária é o profissional da área ou empresa que assume a responsabilidade pela inserção, edição e consulta dos dados associados a um animal no sistema; c) neste contexto, as "Transações" representam os dados que serão registrados na blockchain. O termo é adotado em conformidade com a tradição blockchain de se referir aos dados como "transações," embora esses dados abranjam informações variadas, como detalhes de propriedade, históricos médicos e eventos relevantes; d) cada um dos "Blocos" na blockchain é um recipiente que agrupa um conjunto de transações; e e): a "Blockchain", propriamente dita, é a infraestrutura que abriga todos os blocos de transações.

O experimento simula cenários de inserção, consulta e edição de informações dos animais, permitindo testar a aplicação prática da blockchain como uma infraestrutura vinculada ao sistema de microchipagem. A documentação técnica detalhada e código fonte encontram-se disponíveis em repositório GitHub⁴.

A escolha de criar uma rede blockchain no laboratório foi baseada em uma série de considerações, tais como: permitir a implementação controlada e acessível, ao mesmo

⁴ Código fonte da blockchain para armazenamento de dados na microchipagem animal. Disponível em: <https://github.com/giselebk/blockchain-para-armazenamento-de-dados-na-microchipagem-animal>

tempo, que examina os aspectos fundamentais da tecnologia da blockchain e a aplicação específica para armazenamentos de dados vinculados ao microchip. Embora a escala da rede seja limitada, o experimento permite realizar testes de maneira mais detalhada.

Arquitetura de rede e separação de papéis

A abordagem deste estudo envolveu a construção de uma rede na qual cada nó desempenha um papel duplo: atua, simultaneamente, como entidade veterinária e minerador.

Dentro da rede, as entidades veterinárias desempenham o papel de “guardiãs” dos dados associados aos animais. Elas possuem o conhecimento sobre os animais e o contexto das informações que desejam registrar na blockchain. Sua responsabilidade principal na rede é garantir a precisão e a integridade dos dados, bem como o cumprimento das políticas e práticas relevantes à microchipagem animal. Isso inclui a validação e a autenticação das informações antes de registrá-las na blockchain.

Por outro lado, os mineradores desempenham o papel na segurança e na rede. Eles são responsáveis pela construção dos novos blocos na blockchain por meio do processo de mineração. Para fazer isso, devem competir na resolução de desafios computacionais, exigindo capacidade de processamento e disponibilidade de recursos computacionais significativos. O ato de minerar é essencial para garantir a imutabilidade dos dados e evitar alterações maliciosas, tornando a rede à prova de adulterações.

É importante observar que as entidades veterinárias, sobretudo no Brasil, representam uma variedade de negócios de diferentes tamanhos e recursos financeiros. Frequentemente, essas entidades são estabelecimentos médicos veterinários que podem variar significativamente em termos de capital e infraestrutura. Em alguns casos, as entidades veterinárias podem não dispor de equipamentos adequados ou dos recursos computacionais necessários para competir no processo de mineração. Ou seja, isso destaca a complexidade da decisão de unir os papéis de entidades veterinárias e mineradores, uma vez que nem todas as entidades teriam a capacidade técnica ou financeira para desempenhar ambos os papéis de maneira eficaz.

Portanto, uma observação importante decorrente do experimento é a consideração da separação dos papéis da entidade veterinária (aquele que registra a informação) e do

minerador. A separação dessas funções poderá fornecer maior eficiência nas tarefas relacionadas à gestão de dados e à segurança da rede.

Processo de armazenamento de dados e fila de transações pendentes

A imutabilidade da blockchain garante a segurança e a autenticidade dos dados, uma vez que as informações registradas não podem ser excluídas. Isso implica que atualizações de registros são realizadas por meio da construção de novas transações, por exemplo, quando a posse de um animal é transferida, uma nova transação é registrada para refletir essa atualização.

No experimento realizado, o processo de armazenamento de informações em uma rede blockchain mostrou-se mais complexo e longo em comparação com sistemas de banco de dados tradicionais. Enquanto bancos de dados convencionais permitem atualizações diretas, a blockchain requer várias etapas: construção da transação, adição à lista de transações pendentes, formação de um bloco, mineração e validação das transações; até que as informações sejam gravadas na blockchain.

Durante o experimento, ficou evidente que o processo de armazenamento de informações em uma rede blockchain é mais complexo e demorado em comparação com sistemas de banco de dados tradicionais. As transações seguiram a ordem cronológica, mas percebeu-se a necessidade de implementar critérios de prioridade, como nos casos de emergências veterinárias, nos quais os dados precisam ser disponibilizados rapidamente.

A presença das transações pendentes no experimento é uma característica inerente à natureza da rede blockchain, pois algumas vezes não haverá blocos disponíveis para a inclusão de novas transações. Isso ocorre porque, em uma rede distribuída, é necessário um consenso entre os nós para haver a construção dos blocos, o que envolve o processo de mineração e a existência de transações pendentes, gerando como reflexo a espera pelo consenso entre os blocos.

Essa característica destaca a importância da escalabilidade em redes blockchain, uma vez que o aumento do número de transações e participantes pode causar atrasos.

Tempo de mineração e tempo de confirmação

Na simulação, com recursos de hardware (2 GB de memória RAM, processador de 2 núcleos e sistema operacional Linux Ubuntu 20.04.6 LTS em modo console), foram obtidos os seguintes resultados organizados na tabela 1:

Tabela 1 - Simulação do tempo de mineração

Nível de dificuldade	Tempo
1	0,0001s
2	0,003s
3	0,01s
4	0,2s
5	5,6s
6	42,9s
7	2.006,9s
8	34.427,3s
9	244.554,8s

Fonte: elaborado pelos autores.

A relação entre a dificuldade e o tempo de mineração é notável, com um aumento exponencial à medida que a dificuldade aumenta, mas dentro do esperado. Por exemplo, com uma dificuldade de 1, o tempo de mineração foi quase instantâneo. No entanto, quando a dificuldade foi aumentada para 9, o tempo de mineração atingiu 244.554,8 segundos, o que equivale a quase três dias. Essa variação significativa demonstra a importância de escolher a dificuldade apropriada especialmente em aplicações que exigem tempestividade nas transações.

O tempo de mineração afeta diretamente o tempo de confirmação das informações na rede blockchain, ou seja, até que um bloco seja minerado com a transação desejada, essa transação não é confirmada, contrapondo com os sistemas tradicionais, nas quais a confirmação rápida é uma vantagem. A segurança é uma prioridade nos sistemas blockchain, portanto a mineração é projetada para ser demorada e exigir recursos

significativos. A complexidade computacional é o que torna a rede blockchain resistente à ataques e garante a integridade das informações.

No entanto, a segurança adicional tem um custo no tempo de confirmação. À medida que a dificuldade de mineração aumenta, o tempo de espera por confirmações também cresce, tornando-se um ponto crítico em cenários que demandam transações rápidas e tempestivas.

Transparência e segurança

Sobre a segurança, é indiscutível a vantagem desse método de armazenamento. Primeiramente, porque as transações são “protegidas” pelo *hash* criptográfico e quaisquer alterações em seu conteúdo leva a um *hash* diferente. Segundo o processo de mineração pode ser demasiadamente custoso para um atacante. No exemplo desse experimento, a mineração de um bloco com a dificuldade nove leva, aproximadamente, três dias para um minerador resolver sozinho. Caso um atacante queira alterar os dados contido há algumas transações passadas, levará muito tempo para conseguir minerar novos blocos “falsos”. Por fim, o consenso distribuído requer que a maioria dos participantes da rede concorde sobre o estado atual da blockchain no processo de verificação. Isso implica que um atacante teria que controlar uma quantidade significativa de nós, uma vez que a cópia da blockchain encontra-se armazenada de forma distribuída.

Custos e incentivos

A mineração de blocos exige a resolução de desafios computacionais que requerem poder de processamento e consomem recursos, como eletricidade e internet. Para o minerador, realizar uma prova de trabalho pode ser comparado a chutar números aleatórios por um longo período, embora esse processo seja executado por computadores. Dessa maneira quais seriam os incentivos para os mineradores disponibilizarem poder computacional e incorrerem em custos no cenário do registro animal?

O experimento sugere que, além de aspectos de arquitetura, é necessário implementar um modelo econômico para a rede blockchain. Nesse ponto passa-se a compreender o porquê em muitas redes há uma criptomoeda nativa, porque parte dessas criptomoedas são a recompensa pelo trabalho realizado pelos mineradores, em outras

palavras, o incentivo para os mineradores está ligado à recompensa que recebem assim que conseguem adicionar um novo bloco à blockchain.

Ao buscarmos alternativas baseadas em negócios já existentes no setor animal, poderia ser considerado a implementação de um sistema de cobrança de tarifas. Nesse modelo, ao invés de recompensar os mineradores com criptomoedas, os usuários que desejam realizar transações ou armazenar dados na blockchain são cobrados por esses serviços.

A ausência de uma autoridade central para definir regras, tarifas e tratar de questões do negócio, como os valores cobrados, pode adicionar complexidade significativa à gestão de uma blockchain. Embora essas regras possam ser integradas durante a construção da rede, a complexidade resultante pode tornar a adoção dessa tecnologia menos atraente, já que os participantes podem avaliar que os benefícios potenciais não compensam os desafios envolvidos.

Características determinísticas da prova de trabalho

A análise de funcionamento da prova de trabalho mostrou que o algoritmo defendido por Satoshi Nakamoto (2008) tem característica determinística, diferente das abordagens probabilísticas.

Na prova de trabalho utilizada, o processo de mineração envolve a variação de um *nonce*, que inicia em *nonce=1* e é incrementado em +1 a cada teste. Entretanto, em situações em que dois computadores iniciam o processamento de um bloco simultaneamente, aquele com maior poder de processamento sempre vence. Esta peculiaridade ressalta a relevância de considerações sobre equidade e distribuição de poder de processamento na rede.

Supondo-se o cenário, no qual os papéis do minerador e da entidade veterinária se acumulam, e cada entidade veterinária é responsável por minerar blocos para suas próprias transações, identifica-se que a competição por poder de processamento pode levar à exclusão de alguns dos participantes, situação em que, devido à limitação de recursos, não conseguiriam registrar informações na blockchain.

Bifurcações na rede

No decorrer do experimento, foi observada a existência de duas blockchains de igual tamanho, porém com informações distintas em seus blocos finais.

Suponha-se uma rede distribuída com dez nós e uma blockchain com oitenta blocos. Em um dado momento, é possível que dois nós minerem quase simultaneamente o bloco oitenta e um. No contexto da blockchain, esses eventos são conhecidos como "*forks*", no qual dois ou mais nós da rede mineram blocos quase que simultaneamente resultando na criação de ramos (bifurcações) na cadeia.

Para resolver *forks*, utilizou-se a regra da cadeia mais longa, onde os nós da rede escolhem a cadeia com mais blocos confirmados como a oficial. Isso prolonga o tempo de confirmação das transações, pois os nós precisam aguardar a mineração de vários blocos subsequentes para garantir a inclusão de sua versão na ramificação principal da blockchain. Esse processo pode estender o tempo de confirmação por muitos minutos ou até horas, afetando a agilidade das transações na rede.

Conclusão

O experimento demonstrou que a utilização da blockchain como plataforma de armazenamento para microchipagem animal é tecnicamente viável. A capacidade de criar e consultar registros foi confirmada, oferecendo uma alternativa potencial aos sistemas tradicionais de armazenamento de dados. Contudo, surgiram algumas considerações ao se avaliar a eficiência do sistema.

A dualidade de papéis atribuída às entidades veterinárias, atuando como guardiãs dos dados e como mineradoras, apresenta desafios práticos significativos. A necessidade de competir na mineração pode resultar na exclusão das entidades com recursos limitados, comprometendo a eficiência operacional. O tempo necessário para a confirmação e a gravação dos dados no bloco demonstram que, em cenários de alta demanda, o processo poderá ter lentidão.

O experimento permitiu compreender que a infraestrutura da blockchain é mais complexa de implementar e configurar em comparação com as soluções tradicionais baseadas em bancos de dados. O material técnico disponível para blockchain é significativamente menor do que para os sistemas convencionais, e sua complexidade é

aumentada pela necessidade de considerar os papéis dos nós na rede, mecanismos de consenso e incentivos para os mineradores. Além do mais, os processos da blockchain envolvem mais etapas e exigem uma compreensão profunda de conceitos como prova de trabalho, gestão de transações pendentes e resolução de *forks*, resultando em uma curva relativamente mais longa de aprendizado para implementadores e usuários.

A leitura na blockchain é intensiva e consome mais recursos computacionais, pois exige percorrer bloco por bloco, ao contrário dos métodos tradicionais dos bancos de dados que permitem acesso direto aos registros, tornando o processo longo e oneroso. No entanto, a blockchain oferece maior segurança para informações de microchipagem animal devido à imutabilidade dos dados e à proteção pelo *hash* criptográfico, garantindo a integridade e autenticidade dos registros. Questões como a escolha do algoritmo de consenso, a gestão de chaves criptográficas e a configuração da rede também desempenham papéis cruciais na segurança da blockchain. Quanto ao custo para um potencial atacante fraudar um bloco na blockchain, os recursos computacionais e o tempo necessários para realizar tal feito são extremamente elevados. Esse fator, aliado à descentralização e ao consenso distribuído, torna a blockchain resistente a alterações maliciosas, proporcionando uma camada adicional de segurança.

Conclui-se que a aplicação da blockchain na microchipagem animal é um terreno fértil para inovação, mas não sem desafios. À medida que se avança, é preciso que pesquisadores, desenvolvedores e outros stakeholders colaborem na busca de soluções que equilibrem a eficiência técnica com a acessibilidade e a segurança, impulsionando assim o potencial de utilização da blockchain na microchipagem animal. Desta forma, este experimento oferece importantes aprendizados que podem orientar futuras pesquisas nesse campo.

Referências

ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA DE PRODUTOS PARA ANIMAIS DE ESTIMAÇÃO. **Mercado PET Brasil 2023**. São Paulo. Disponível em: https://abinpet.org.br/wp-content/uploads/2023/07/abinpet_folder_dados_mercado_2023_draft5.pdf. Acesso em: 13 jul. 2023.

CONSEJO ANDALUZ DE COLEGIOS OFICIALES DE VETERINARIOS. **El REIAC se reúne con Sergio García Torres, director general de bienestar animal, para conocer la gestión de la plataforma**. *Andalucía Veterinaria*, Sevilha, v. 33, n. 3, p. 8-9,

jul./dez. 2020. Disponível em: <https://cacv.es/blog/2020/12/10/av-julio-diciembre-2020/>. Acesso em: 05 jul. 2023.

DHAR, Shalini; KHARE, Ashish; SINGH, Rajani. **Advanced security model for multimedia data sharing in internet of things**. Transactions on Emerging Telecommunications Technologies, [S.l.]: John Wiley & Sons, n. 4621, p. 1-17, ago. 2022. Disponível em: <https://doi.org/10.1002/ett.4621>. Acesso em: 27 jul. 2023.

FRAM, Brianna R.; RIVLIN, Michael; BEREDJIKLIAN, Pedro K. **On emerging technology: what to know when your patient has a microchip in his hand**. The Journal of hand surgery, [S.l.], v. 45, n. 7, p. 645-649, jul. 2020. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0363502320300332>. Acesso: 6 ago. 2023.

LANCASTER, Emily et al. **Problems associated with the microchip data of stray dogs and cats entering rspca queensland shelters**. Animals, [S.l.], v. 5, n. 2, p. 332-348, mai. 2015. Disponível em: <https://www.mdpi.com/2076-2615/5/2/332>. Acesso: 6 ago. 2023.

LASHKARI, Bahareh; MUSILEK, Petr. **A comprehensive review of blockchain consensus mechanisms**. IEEE Access, [S.l.], v. 9, p. 43620-43652, mar. 2021. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9376868>. Acesso em: 17 nov. 2023.

LOTT, Stephen D. **Getting under fido's skin: analyzing the objections to mandatory pet microchipping laws**. Oklahoma Journal of Law and Technology, Estados Unidos, v. 7, p. 1, jan. 2011. Disponível em: <https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=1025&context=okjolt>. Acesso: 6 ago. 2023.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer electronic cash system**. Bitcoin. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 13 jul. 2023.

NATARAJAN, Harish; KRAUSE, Solvej; GRADSTEIN, Helen. **Distributed Ledger Technology (DLT) and Blockchain**. Washington: International Monetary Fund, n. 1, 2017. Disponível em: <https://openknowledge.worldbank.org/entities/publication/563eb421-4449-5319-953b-2ace8da058c0>. Acesso em: 26 jul. 2023.

PILKINGTON, Marc. **Blockchain Technology: principles and applications**. França: Research Handbook on Digital Transformations, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660. Acesso em: 17 nov. 2023.

RAUCHS, Michel et al. **Distributed ledger technology systems: a conceptual framework**. Cambridge: Cambridge Centre for Alternative Finance, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013#paper-citations-widget. Acesso em: 26 jul. 2023.

RIZVI, Raheeqa; PARA, Parveez Ahmad; GANGULY, Subha. **Implantation of microchip in animals: a review**. International journal of pharmaceutical and bio-medical science, [S.l.], v. 3, n. 1, p. 19-20, fev. 2016. Disponível em: https://www.researchgate.net/profile/SubhaGanguly/publication/297088924_Implantati

on_of_microchip_in_animals_A_Review/links/56dd043908aee73df6d40596/Implantati
on-of-microchip-in-animals-A-Review.pdf. Acesso em: 29 jul. 2023.

SRIMAN, B.; GANESH KUMAR, S.; SHAMILI, P. **Blockchain technology: consensus protocol proof of work and proof of stake.** In: Intelligent Computing and Applications. Singapore: Springer, 2021. p. 395-406. Disponível em: https://www.researchgate.net/profile/Saroj-Kumar-22/publication/345005910_Intelligent_Monitoring_of_Bearings_Using_Node_MCU_Module/links/61286be70360302a005f4941/Intelligent-Monitoring-of-Bearings-Using-Node-MCU-Module.pdf#page=395. Acesso em: 17 nov. 2023.

TABATABAEI, Mohammad Hossein; VITENBERG, Roman; VEERARAGAVAN, Narasimha Raghavan. **Understanding blockchain: definitions, architecture, design, and system comparison.** Computer Science Review, Oslo, v. 50, p. 100575, jul. 2023. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S1574013723000424>. Acesso em: 17 nov. 2023.

XIONG, Huanliang et al. **Research on progress of blockchain consensus algorithm: a review on recent progress of blockchain consensus algorithms.** Future Internet, Suíça, v. 14, n. 2, p. 47, jan. 2022. Disponível em: <https://www.mdpi.com/1999-5903/14/2/47>. Acesso em: 29 jul. 2023.

XU, Min; CHEN, Xingtong; KOU, Gang. **A systematic review of blockchain.** Financial Innovation, [S.l.], v. 5, n. 1, p. 1-14, jul. 2019. Disponível em: <https://jfin-swufe.springeropen.com/articles/10.1186/s40854-019-0147-z>. Acesso em: 17 nov. 2023.

YAN, Shi. **Analysis on blockchain consensus mechanism based on Proof of Work and Proof of Stake.** In: YAN, Shi. International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI). Polônia: IEEE Xplore. p. 464-467, 2022. Disponível em: <https://ieeexplore.ieee.org/document/9974007>. Acesso em: 17 nov. 2023.

ZHOU, Yue et al. **Application of distributed ledger technology in distribution networks.** Proceedings of the IEEE, United Kingdom, v. 110, n. 12, p. 1963-1975, dez. 2022. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9805829>. Acesso em: 22 jul. 2023.