CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

Faculdade de Tecnologia Baixada Santista Rubens Lara

Curso Superior de Tecnologia em Sistemas para Internet

BRUNO SILVA SIMÕES
CARLA RENATA DA SILVA BRITO

DESVENDANDO A INTERNET COMPUTER (ICP): Uma nova fronteira na tecnologia Blockchain

Santos, SP
2024

BRUNO SILVA SIMÕES
CARLA RENATA DA SILVA BRITO

DESVENDANDO A INTERNET COMPUTER (ICP): Uma nova fronteira na tecnologia Blockchain

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia Rubens Lara, como exigência para a obtenção do Título de Tecnólogo em Sistemas para Internet.

Prof. Felipe Cannarozzo Lourenço

Santos, SP
2024

RESUMO

A *Internet Computer* (ICP) é um projeto de blockchain desenvolvido pela DFINITY Foundation com o objetivo de criar uma internet descentralizada, combinando as capacidades dos serviços web tradicionais com os benefícios da tecnologia blockchain. A descentralização é fundamental para o design e implementação do ICP, permitindo resistência a ataques, transparência e imutabilidade. Além disso, a descentralização permite que o ICP seja uma rede soberana, composta por subredes que seguem a descentralização usada pela rede. O objetivo a longo prazo da ICP é substituir completamente a TI tradicional, criando uma "singularidade blockchain", onde tudo é executado totalmente na blockchain de maneira poderosa e ininterrupta, e não pode ser hackeado. Os nós da blockchain da *Internet Computer* são executados em uma rede soberana com consenso de prova de trabalho útil. Os protocolos utilizam a nova criptografia de chave de cadeia para combinar várias blockchains de sub-redes em uma única blockchain. Isso permite que ele escale horizontalmente o volume total de contratos inteligentes hospedados, e seus cálculos e dados, sem limites. O relatório de sustentabilidade do ICP de 2023 ilustra como as robustas análises de emissões implementadas em todo o protocolo em 2023 estão permitindo uma abordagem baseada em dados para a descarbonização da rede. A meta do ICP é estender a liderança da rede em 'computação consciente do clima', garantindo uma vantagem competitiva durável para todo o ecossistema.

Palavras-chaves: Blockchain, *Internet Computer* (ICP), Descentralização.

ABSTRACT

The Internet Computer (ICP) is a blockchain project developed by the DFINITY Foundation with the aim of creating a decentralized internet, combining the capabilities of traditional web services with the benefits of blockchain technology. Decentralization is fundamental to ICP design and implementation, enabling attack resistance, transparency and immutability. Furthermore, decentralization allows ICP to be a sovereign network, made up of subnets that follow the decentralization used by the network. ICP's long-term goal is to completely replace traditional IT, creating a "blockchain singularity" where everything runs entirely on the blockchain in a powerful, seamless way, and cannot be hacked. Internet Computer blockchain nodes run on a sovereign network with useful proof-of-work consensus. The protocols utilize new chain-key cryptography to combine multiple subnet blockchains into a single blockchain. This allows it to horizontally scale the total volume of hosted smart contracts, and their calculations and data, without limits. The 2023 ICP Sustainability Report illustrates how robust emissions analytics implemented across the protocol in 2023 are enabling a data-driven approach to grid decarbonization. ICP's goal is to extend the network's leadership in 'climate-aware computing', ensuring a durable competitive advantage for the entire ecosystem.

Keywords: Blockchain, Internet Computer (ICP), Decentralization.

LISTA DE ABREVIATURAS E SIGLAS

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Atualmente, um dos assuntos mais discutidos no âmbito tecnológico e econômico é sobre as blockchains e suas constantes evoluções e revoluções no tema descentralização. Partindo dessa premissa, aprofundamos nosso conhecimento na blockchain *Internet Computer* (ICP), que tem tido cada vez mais avanços significativos e pode se tornar uma referência no tema blockchain.

A *Internet Computer* (ICP) é uma blockchain desenvolvida pela DFINITY *Foundation*. E o que a torna única é que ela não é apenas uma plataforma para transações financeiras, mas uma rede na qual você pode construir e hospedar software diretamente. Isso significa que a ICP pode ser usada para criar todo tipo de aplicativo, desde redes sociais até plataformas financeiras, tudo em uma rede descentralizada e segura de acordo com a *Internet Computer Wiki*.

Nessa documentação, é dado ênfase ao uso do Sistema Nervoso de Rede (NNS), que é uma parte crucial da ICP. O NNS é responsável por governar os nós (computadores individuais na rede) e sub-redes (grupos de nós), e pode fazer atualizações na rede. O ponto de destaque desta blockchain é que, dentre as outras existentes, a *Internet Computer* (ICP), tem projetos inovadores, se escala infinitamente e, ao contrário de outras blockchains, pode se atualizar e evoluir com base nas decisões da comunidade segundo o portal do *Intenet Identity* (2024).

1.1 OBJETIVO

Esta documentação foi criada com o intuito de explicar sobre a rede ICP, suas tecnologias e, mais especificamente, mostrar como usar o Sistema Nervoso de Rede (NNS), que é uma parte fundamental da *Internet Computer* (ICP). O NNS é um sistema de governança automatizado que torna a rede autônoma e adaptável, permitindo que a *Internet Computer* se atualize e evolua com base nas decisões da comunidade.

O NNS é o que permite que a Internet Computer funcione de maneira eficiente e segura. Ele garante que a rede possa se adaptar e evoluir com o tempo, e desempenha um papel crucial na manutenção da segurança e estabilidade da *Internet Computer*.

1.1.1 OBJETIVO GERAL

A ideia central abordada, é ensinar sobre as diversas funcionalidades da *Internet Computer* (ICP) e explicar ao leitor que a rede tem como objetivo criar uma internet descentralizada onde o software pode ser construído e executado com as mesmas capacidades dos serviços web tradicionais, mas com os benefícios adicionais da tecnologia blockchain, além de permitir a execução de contratos inteligentes em escala da web, em velocidade da web e com eficiência de processamento. Esclarecendo que a rede permite que qualquer pessoa possa construir e hospedar seu próprio software na internet sem a necessidade de um intermediário, tornando a web mais democrática e segura. Englobando também o Sistema Nervoso de Rede (NNS), pois é uma parte crucial da blockchain ICP pois atua como o cérebro da rede, controlando e gerenciando todos os aspectos da ICP.

Aqui ensinaremos como usar o NNS, além de explicar sobre outras tecnologias da rede até chegarmos no NNS.

1.1.2 OBJETIVOS ESPECÍFICOS

Foi conduzida uma análise abrangente da estrutura e do funcionamento do *Network Nervous System* (NNS) dentro da blockchain da *Internet Computer*. Esta investigação detalhada incluiu uma exploração profunda de como o NNS, como um sistema de governança descentralizado, organiza, monitora e gerencia os nós e sub-redes da *Internet Computer*.

Além disso, foi examinado como o NNS facilita a tomada de decisões protocolares e a implementação de atualizações na rede da *Internet Computer*. Este estudo compreendeu uma análise detalhada de como as propostas são submetidas ao sistema, bem como o processo automático de votação e execução das mesmas.

Também foi investigado o papel dos detentores de tokens ICP no processo de votação e governança do NNS. Isso envolveu uma análise abrangente de como os detentores de tokens ICP podem bloquear seus tokens em neurônios de votação, permitindo-lhes assim a capacidade de participar ativamente votando em propostas que impactam a estrutura da ICP.

1.2 ESTADO DA ARTE

Nosso estudo atual se concentra na exploração aprofundada da *Internet Computer* (ICP), uma rede blockchain dinâmica que continua a evoluir com avanços tecnológicos significativos. Durante a condução deste trabalho, mergulhamos na compreensão das últimas inovações introduzidas nesse campo em rápida expansão. Em particular, temos dedicado atenção especial à análise detalhada do *Network Nervous System* (NNS). Este sistema, fundamental para a governança descentralizada da ICP, não só organiza e monitora os nós e sub-redes da rede, mas também facilita a tomada de decisões protocolares e a implementação eficiente de atualizações.

Além de explorar as funcionalidades do NNS, investigamos o papel dos detentores de tokens ICP no processo de governança. Uma parte crucial de nosso estudo envolveu a análise de como os detentores de tokens podem bloquear seus ICP em neurônios de votação, permitindo-lhes influenciar propostas que moldam o futuro da rede. Este aspecto da pesquisa revelou não apenas a complexidade técnica envolvida, mas também a importância de uma participação ativa da comunidade para garantir decisões robustas e inclusivas na evolução da ICP.

À medida que avançamos em nosso estudo, temos observado de perto as tendências emergentes e as implicações mais amplas dessas tecnologias. A Internet Computer não apenas representa um marco significativo na arquitetura blockchain, mas também desempenha um papel crucial na transformação digital e na descentralização da infraestrutura da web. Nossas descobertas até agora indicam um campo de pesquisa vibrante e promissor, com oportunidades contínuas para contribuições inovadoras e críticas que moldarão o futuro da governança digital e da infraestrutura descentralizada.

2 INTERNET COMPUTER (ICP)

Segundo o *whitepaper* do Bitcoin, a blockchain em geral, é como um banco de dados descentralizado onde cada informação e inserida em uma cadeia de blocos. Cada bloco contém um hash do bloco anterior, mantendo-os conectados. É uma tecnologia que permite a transferência de dados digitais com uma solução muito sofisticada e de uma maneira completamente segura.

A blockchain é mantida por uma rede de computadores pelo mundo que validam e registram transações, tornando-a resistente a fraudes e ataques. A blockchain é uma base para as criptomoedas, mas seu potencial vai muito além, oferecendo soluções para transações de todos os tipos, onde a segurança, a privacidade e a resistência à censura são primordiais.

A Web3 e Web 3.0 são frequentemente usados de maneira intercambiável, mas têm distinções importantes. Web3 refere-se à nova geração da web que usa tecnologias descentralizadas, como blockchain e criptomoedas, para devolver o controle de dados aos usuários, promovendo segurança e privacidade através de redes distribuídas e contratos inteligentes. Já Web 3.0, ou Web Semântica, descreve uma internet mais inteligente e conectada, onde a inteligência artificial e o aprendizado de máquina permitem uma compreensão e processamento avançado dos dados, resultando em experiências personalizadas e maior interoperabilidade entre sistemas. Enquanto Web3 foca na descentralização e na propriedade dos dados pelo usuário, Web 3.0 enfatiza a inteligência e a eficiência no acesso e uso das informações.

A ICP tem um design que reflete uma reavaliação completa de toda a arquitetura blockchain e a aplicação da criptografia moderna. Foi construído por um grande esforço contínuo de pesquisa e desenvolvimento em criptografia, que empregou muitos criptografistas notáveis, pesquisadores de ciência da computação e engenharia. A blockchain passou por um processo de gênese em maio de 2021 e se tornou parte da internet pública seguindo o *Internet Computer Wiki*.

A tecnologia blockchain e a Web3 estão remodelando a maneira como interagimos com a internet e os serviços digitais. Com isso, a blockchain em questão, pretende construir uma nova rede onde qualquer indivíduo pode manter um servidor web rodando a nova web3, com sistema DAO (*Descentralized Autonomous Organization*) de governança de rede, onde tudo que será desenvolvido e implementado precisa de uma aprovação prévia de sua comunidade, não tendo

necessidade de uma grande empresa ou indivíduo por trás das decisões que serão tomadas pela rede, fazendo com que o poder de tomada de decisões da rede esteja na mão dos usuários, criando uma internet mais descentralizada, distribuída e com segurança, descentralizando o poder das *big techs*, tudo isso rodando dentro de sua blockchain.

A ICP preenche uma lacuna importante entre a programação tradicional e o desenvolvimento baseado em blockchain. Isso faz com que os contratos inteligentes na ICP sejam expressivos e escaláveis como aplicativos tradicionais, mas se beneficiem da execução confiável e descentralizada de uma blockchain.

Isso é possível graças à arquitetura única da ICP, que combina máquinas de nós em blockchains de sub-redes altamente eficientes, que adicionam capacidade para hospedar recipientes à prova de violação. A ICP tem um sistema de governança automatizado e de permissão chamado SNS (Sistema Nervoso de Rede), que desempenha o papel de governança da rede, tornando a ICP uma rede descentralizada.

Aumentar a descentralização geralmente vem à custa da escalabilidade, e vice-versa. No entanto, a ICP conseguiu encontrar um equilíbrio entre esses dois aspectos e está localizada no meio do espectro entre centralização e descentralização. No entanto, ao contrário de outras soluções da blockchain, a ICP conseguiu manter um alto grau de escalabilidade sem comprometer a descentralização, representando uma nova abordagem para a programação blockchain que preenche uma lacuna entre a programação tradicional e o desenvolvimento baseado em blockchain oferecendo um equilíbrio entre escalabilidade e descentralização, tornando-o uma solução ideal para a próxima geração de serviços e aplicações Web3.

Além do projeto ter como intuito a descentralização da internet com uso da blockchain, ela traz tecnologias como a *Chain-Key*, que funciona como uma L2 (*Layer Two*), visando solucionar problemas de outras blockchains como, as mais famosas, Bitcoin e Etherium, aumentando significativamente a velocidade de transações da web e trazendo para estas redes maior segurança, escalabilidade, redundância e funcionalidades que não são possíveis hoje e também novas funcionalidades para o Bitcoin como contratos inteligentes. Essa nova iniciativa torna possível o uso de Defi, NFT e metaverso de forma nativa sem necessidade de pontes, encapsulamentos e hospedagem por terceiros, excluindo a necessidade de confiança.

Um dos objetivos principais da ICP é não substituir outras blockchains, mas sim torná-las independentes de Clouds centralizadas, dando funcionalidades que na arquitetura atual da blockchain não é possível, visando uma forma de fazer com que ambas as partes se beneficiem, a ICP dando uma base totalmente descentralizada, gerando funcionalidades onde antes não era possível para as outras blockchains e ao mesmo tempo trazendo usuários, desenvolvedores, comunidades, entusiastas etc. que já existem nestas blockchains para sua rede.

2.1 DFINITY

Fundada na Suíça, a Fundação DFINITY é uma organização sem fins lucrativos dedicada a reinventar a Internet para hospedar computadores superpoderosos e seguros, de acordo com a Internet Computer Org.

A ICP, liderada pela DFINITY, adota novas tecnologias e novas arquiteturas, como WASM (*WebAssembly)*, um formato de código binário que é portátil, seguro, eficiente e universal, permitindo que softwares escritos em várias linguagens de programação sejam executados de forma segura e rápida em qualquer hardware. Ele foi projetado para ser completamente agnóstico em relação à Web e pode ser "incorporado" em qualquer outro ambiente. Além disso, WASM é neutro em relação ao modelo de programação usado para expressar programas, servindo como uma abstração sobre o hardware comum, não sobre uma linguagem de programação ou paradigma de acordo com o website Medium.

Ele foi projetado e implementado em colaboração entre todos os principais concorrentes em seu espaço e é definido por um padrão aberto, permitindo que qualquer pessoa o use, implemente ou contribua para ele. Possui características de anti-adulteração, rápido funcionamento e escalabilidade pode atingir bilhões de usuários em todo o mundo. Ao mesmo tempo, apoia a construção independente de software, o que deverá reverter o status quo dos gigantes tecnológicos que monopolizam a Internet.

A Internet Computer (ICP) é o produto principal da Fundação DFINITY. É uma plataforma de computação geral de código aberto e um projeto de blockchain *Layer1* que visa resolver alguns dos principais desafios que a Internet tradicional enfrenta hoje, como segurança deficiente do sistema, monopólio de serviços de Internet e

abuso de dados pessoais do usuário. Com a ICP, qualquer aplicativo e serviço pode ser construído sem necessidade do uso excessivo de dados e informações pessoais.

Ao mesmo tempo, a DFINITY introduziu um sistema central na blockchain no mecanismo de governança, que pode proteger os usuários contra-ataques, ajudar a reiniciar sistemas danificados, otimizar dinamicamente a segurança e a eficiência da rede, atualizar protocolos e reduzir o abuso da plataforma.

DFINITY é uma combinação de *Decentralized Infinity*, que representa a visão do projeto de descentralização infinita.

A Internet de hoje constrói uma rede muito grande, conectando bilhões de computadores, mas não descentraliza a “computação e armazenamento de dados” na rede.

Dominic Williams, o fundador da DFINITY, queria apenas construir uma plataforma blockchain com melhor desempenho do que a Ethereum, mas com o avanço gradual do desenvolvimento, a compreensão das pessoas sobre a Internet se aprofundou gradualmente, e a DFINITY também restabeleceu a ICP, o "Computador da Internet ". Ela tem a visão de trazer um mundo compartilhado, fornecer um “contêiner” seguro e sem tempo de inatividade para “softwares autônomos” e fornecer energia para uma nova geração de sistemas de TI e serviços na Internet.

2.2 TRÊS PRINCIPAIS RECURSOS E VANTAGENS DA ICP

O projeto central da DFINITY é a Internet Computer Protocol, conhecida como ICP. O fundador Dominic Williams comparou a ICP com a Internet tradicional, dizendo que a ICP é a primeira blockchain do mundo que funciona na velocidade da rede, pode ser expandido sem um limite definido e pode transportar inúmeros contratos inteligentes para calcular e armazenar qualquer quantidade de dados (Dominic Williams, 2021).

Suas características podem ser resumidas como implantação conveniente, descentralização e backup de recuperação em caso de desastres.

As atuais oito vantagens principais da *Internet Computer* incluem modelo de gás inverso (Ao usar aplicativos baseados na ICP, os usuários não precisam pagar para interagir com contratos inteligentes, os usuários só precisam desfrutar do serviço). Alcance contratos inteligentes na velocidade da rede (O atraso na interação é um indicador importante para medir se um sistema está disponível. ICP alcançou

bons resultados na consulta de milissegundos e na atualização de segundos). Uma blockchain capaz de executar páginas da web (Os usuários podem acessar diretamente contratos inteligentes na ICP por meio de navegadores ou aplicativos móveis, sem passar por páginas da web e servidores centralizados, muito menos tocar no código da linha de comando). Identidade descentralizada na Internet (Na ICP, os usuários podem criar rapidamente uma ID descentralizada em segundos por meio de digitalização facial ou reconhecimento de impressão digital, não precisam mais gerenciar nomes de usuário e senhas e não precisam tocar em chaves privadas incompreensíveis e palavras mnemônicas para controlar facilmente sua própria ID). Expansão contínua de baixo custo (a ICP pode alcançar uma expansão suave e contínua, não apenas pode gerar automaticamente novas sub-redes de acordo com as condições de carga da rede, mas também não precisa interromper seu serviço durante o processo de expansão. Para usuários e desenvolvedores, o processo de dimensionamento é indiferente). Tecnologia *Chain-Key* (*Chain-Key* é a tecnologia central por trás da ICP, que cria uma chave pública exclusiva de 48 bytes para a *blockchain* da ICP, para que qualquer dispositivo, até mesmo um relógio inteligente, possa verificar pessoalmente a cadeia da ICP). Sistema de governança auto evolutivo (A *Internet Computer* executa um sistema de governança de token descentralizado chamado *Network Nervous System* (NNS), que é um sistema de governança que pode ajudar a rede ICP a alcançar a auto evolução). E o Gás estabilizado (O gás consumido na *blockchain Internet Computer* é chamado de Ciclos, que são trocados pelo consumo de ICP. O ciclo é estável sob o ajuste do algoritmo, ancorando 1 SDR (cálculo abrangente de moeda legal multinacional, SDR pode ser considerado como uma unidade estável))(*Internet Identity* e Kyle Langham, 2022).

2.2.1 PRINCIPAIS CONQUISTAS DE DESENVOLVIMENTO DESDE O LANÇAMENTO

2.2.1.1 LINGUAGEM DE CONTRATO INTELIGENTE MOTOKO

Motoko é uma nova linguagem de programação de contrato inteligente projetada para suportar perfeitamente o modelo de programação de computadores da Internet e facilitar o aproveitamento dos recursos exclusivos do blockchain.

Motoko é fortemente tipado, baseado em ator e possui suporte integrado para persistência ortogonal e mensagens assíncronas, recursos de produtividade e segurança, incluindo gerenciamento automático de memória, genéricos, inferência de tipo, correspondência de padrões e aritmética arbitrária e de precisão fixa.

O *Messaging* usa de forma transparente a linguagem de definição de interface *Candid* do Internet Computer e formatos de conexão para interoperabilidade digitada, de alto nível e entre idiomas.

2.2.1.2 TECNOLOGIA DE CHAVE DE CORRENTE

Chain-Key é a tecnologia central por trás do ICP. É a extensão de sub-rede e a tecnologia de gerenciamento de chaves do Internet Computer, que pode garantir a segurança e a disponibilidade da rede. Portanto, qualquer dispositivo, até mesmo um smartwatch, pode verificar pessoalmente a cadeia ICP.

Por outro lado, ao verificar blockchains tradicionais como o ETH, como cada bloco é assinado por um nó diferente, os dispositivos precisam sincronizar centenas de gigabytes de dados assinados. Na ICP, todos os nós assinam um bloco juntos. Portanto, o dispositivo só precisa salvar uma chave pública exclusiva de 48 bytes para verificar cada bloco.

O recurso fácil de verificar do Chain-Key também torna a Internet Computer naturalmente adequado para operações entre cadeias. Podemos até armazenar a chave pública blockchain da ICP no contrato inteligente ETH para verificar diretamente as transações entre cadeias.

2.2.1.3 NNS: GOVERNANÇA DE BLOCKCHAIN ICP

O *Network Nervous System* (NNS) é um sistema algorítmico aberto que gerencia o blockchain ICP. Suas inovações mais notáveis incluem a atualização do protocolo ICP e do software executado em nós, adição de novos fornecedores de nós, adição de nós à rede blockchain, criação de novas blockchains de sub-rede para aumentar a capacidade, e qualquer pessoa pode participar de Tokens no NNS.

2.2.1.4 GERAÇÃO DE CHAVE DISTRIBUÍDA NÃO INTERATIVA

O conjunto de nós que executam uma sub-rede evoluirá à medida que os nós puderem ingressar ou sair de suas respectivas sub-redes, e como os nós estão em constante mudança, o desenvolvimento de assinaturas de limite dificulta a capacidade dos nós de registrar e distribuir novas chaves públicas.

Como solução, o Internet Computer apresenta a Geração Distribuída Não Interativa de Chaves (NI-DKG), que simplifica o gerenciamento de chaves usando chaves públicas estáticas para se referir à mesma sub-rede.

NI-DKG oferece segurança ativa. Este protocolo compartilhado é adequado para ambientes assíncronos, permitindo tempos de bloqueio rápidos e escalabilidade ilimitada. Cada signatário antigo só precisa transmitir uma mensagem ao novo signatário.

Para garantir a segurança, o ICP usa vários conceitos, incluindo provas não interativas de conhecimento zero e criptografia com sigilo direto.

2.2.1.5 IDENTIDADE NA INTERNET

Para acessar e interagir com aplicativos executados em computadores na Internet, os usuários normalmente precisam ser autenticados, e um dos métodos mais comuns de autenticação em um ICP é a Identidade da Internet.

Identidade da Internet é uma estrutura de autenticação de blockchain apoiada por ICP onde os usuários primeiro criam "pontos de ancoragem" de identidade e atribuem dispositivos criptográficos compatíveis a esses dispositivos, como sensores de impressão digital em laptops, sistemas de reconhecimento facial em telefones celulares ou HSMs portáteis. DApps em execução no ICP usando qualquer dispositivo atribuído à âncora.

Isso proporciona um alto grau de conveniência, os usuários podem se autenticar em DApps de uma maneira muito simples, sem gerenciar ou manipular diretamente as chaves.

2.2.1.6 PROTOCOLO DE CONSENSO ICP

O *Internet Computer Consensus* (ICC), como protocolo subjacente do DFINITY, pode suportar o mecanismo bizantino de tolerância a falhas dos computadores da Internet (BFT, que se refere à capacidade de um sistema de computação de suportar falhas arbitrárias de certos componentes enquanto ainda funciona normalmente).

O protocolo ICC é um protocolo líder baseado no pressuposto de sincronização parcial e integração total com o blockchain. Os líderes podem ser alterados em cada rodada. O protocolo é muito simples e eficaz. Se o líder falhar em qualquer rodada (a probabilidade é inferior a um terço), o protocolo substituirá o líder e resolverá o problema a tempo nesta rodada, sem atrasar para a próxima rodada.

2.2.2 COMPUTAÇÃO E ARMAZENAMENTO

Como um dos representantes do armazenamento distribuído, as capacidades de computação e armazenamento do ICP têm atraído muita atenção.

A arquitetura do aplicativo ICP começa na camada inferior: camada P2P (coletar e distribuir dados) → camada de consenso (organizar mensagens, escrever blocos após verificação) → camada de roteamento de mensagens (transmitir informações para o destino) → camada de execução do aplicativo (através da caixa de areia de segurança WASM Computação Ambiental).

Na fase de desenvolvimento, as ferramentas de desenvolvedor do DFINITY irão abstrair cada nível e copiá-lo para a versão local do desenvolvedor para facilitar o desenvolvimento.

O estado da aplicação do ICP é armazenado na memória, gerenciado e confirmado através da fase de consenso. Os desenvolvedores não precisam se preocupar com a perda de dados ou com o local onde os dados são armazenados.

A fim de garantir a estabilidade e a fluência das aplicações ICP, o limite para se tornar um nó de data center Internet Computer é muito alto. O servidor do nó ICP precisa de 16 32 GB de memória.

Comparado com os requisitos de configuração de 4 GB de memória e SSD de 290 GB para o nó de verificação Ethereum, já é bastante exagerado. Claro que em termos de armazenamento, o mais exagerado é o Filecoin, que requer 1 TB de memória e configuração SSD de 16 TB.

Comparado ao Filecoin, o ICP não se concentra no armazenamento, mas sim no *Serverless* (computação sem servidor, um modelo de computação em nuvem). Os dados armazenados podem ser dados regulares do aplicativo, estado do aplicativo e o próprio código do aplicativo, portanto, não há necessidade de exagerar nos requisitos de armazenamento

2.2.2.1 VANTAGENS DO ICC EM COMPARAÇÃO COM OUROS PROTOCOLOS

O protocolo ICC não possui subprotocolos complexos ou não especificados; O protocolo ICC torna a tarefa de propagação confiável de blocos para as partes uma parte integrante do protocolo, em vez de deixá-la para outros subprotocolos não especificados;

O protocolo ICC responde de forma otimista, o que significa que quando o líder é honesto, o protocolo prosseguirá na velocidade da latência real da rede, e não em algum limite superior da latência da rede. Além das seis principais conquistas do ICP, o ecossistema Internet Computer também incubou muitos projetos de alta qualidade.

2.3 FUNDAMENTOS DA BLOCKCHAIN

A ideia central do blockchain é que ela permite que transações ou dados sejam armazenados em uma cadeia de blocos, cada um contendo um registro imutável e verificável das transações que ocorrem em um determinado período. Cada bloco é ligado ao bloco anterior através de um hash criptográfico, criando uma cadeia de blocos, daí o nome "blockchain".

A blockchain é descentralizada, o que significa que não é controlada por uma única entidade ou autoridade central. Em vez disso, é interligada por uma rede de computadores, chamada nós, que validam e registram transações na blockchain. Isso torna a blockchain resistente à censura e à manipulação, pois qualquer alteração em um bloco exigiria a alteração de todos os blocos subsequentes na cadeia, o que é praticamente impossível devido à quantidade de poder computacional necessário.

2.3.1 BLOCKCHAIN E WEB3

O termo utilizado atualmente para descrever a nova tecnologia é um misto entre web3 que faz uso da tecnologia blockchain e a web 3.0 que são tecnologias de intercâmbio de dados (como por exemplo: RDF, SPARQL, OWL e SKOS). Enquanto os dados na web3 são difíceis de modificar ou excluir, uma vez que estão distribuídos em vários nós da rede, os dados na web 3.0 podem ser facilmente alterados, de acordo com o site ‘made4u’.

A Tecnologia da ICP visa unir esses dois mundos e sendo construída para ser a nova web, usa sua funcionalidade de blockchain tornando os dados mais seguros, redundantes e descentralizados para criar uma internet que é controlada pelos usuários, em vez de grandes corporações, ao mesmo tempo que usa as características da Web 3.0 como rápida transferência de dados, escalabilidade e usabilidade mais amigável para usuários que estão acostumados com a Web que atualmente utilizamos.

Podemos dizer então que o misto de Web3 e Web 3.0, é a próxima geração da internet que busca criar uma versão online mais inteligente, personalizada e descentralizada e a blockchain está desempenhando um papel fundamental na formação da Web3, fornecendo uma base para a criação de aplicações descentralizadas (dapps - aplicações que funcionam em blockchain e são controladas pelos usuários e não uma única entidade). Isso permite a criação de uma internet mais democrática e justa, onde os usuários têm controle sobre seus próprios dados e podem interagir diretamente uns com os outros sem a necessidade de intermediários.

Além disso, a blockchain permite a criação de contratos inteligentes, programas de computador que executam automaticamente as condições de um contrato quando as condições pré-definidas são atendidas e isso abre novas possibilidades para a automação e a interação *peer-to-peer* na internet. A blockchain está moldando a Web3 para fornecer as ferramentas e a infraestrutura fáceis para criar uma internet descentralizada e controlada pelo usuário. À medida que a tecnologia blockchain continua a evoluir, é provável que seu impacto na Web3 aumente.

2.4 TECNOLOGIA GÁS REVERSO

A tecnologia de gás reverso é uma característica única da ICP que se distingue significativamente da plataforma de outras redes blockchain como Bitcoin (BTC), Ethereum (ETH), Solana (SOL), entre outras.

Na maioria das blockchains, os usuários são responsáveis por pagar as taxas de gás para interagir com contratos inteligentes. Isso pode ser uma barreira para a adoção em massa, pois exige que os usuários tenham uma carteira e tokens para pagar as taxas de gás, ou seja, caso fosse implementado uma rede social em alguma das blockchains o usuário teria que pagar um valor por qualquer interação que fizesse na rede.

No entanto, a ICP adota um modelo de “Gás Reverso”, onde os desenvolvedores são responsáveis por pagar as taxas de computação e armazenamento. Fazem isso por meio de carregamento de seus contratos inteligentes (ou canisters) com ciclos, que são então queimados para pagar pela computação e uso de memória, permitindo que os usuários interajam com dapps na ICP sem tokens, como fariam em qualquer aplicativo Web2.

Este modelo tem implicações para o desenvolvimento de dapps, especialmente aqueles que visam adoção em massa, como redes sociais, plataforma de jogos ou de transferências. O modelo torna a interação com dapps tão simples quanto clicar em um link e isso pode levar a uma maior adoção e uso em suas plataformas. Os desenvolvedores também têm a flexibilidade de criar modelos econômicos personalizados, atendendo estratégias e escolhendo como e quando cobrar dos usuários, em vez de serem obrigados a passar as taxas de gás para os usuários.

A tecnologia de Gás Reverso da ICP é um grande diferencial para o desenvolvimento de dapps e pode ser um fator chave para contribuir para a adoção em grande escala de dapps na Internet Computer e essa simplicidade não vem apenas do Gás Reverso, a nova arquitetura permite facilitar e deixar intuitivo o uso pelo usuário comum, tirando o conceito de que blockchain é algo difícil e deve ser estudado antes de ser utilizado.

2.5 *INTERNET IDENTITY*

A tecnologia *Internet Identity* da ICP, representa uma nova forma de realizar o login na rede e representa uma mudança significativa na forma como os usuários interagem com dapps e outros serviços online. A *Internet Identity* é um sistema de autenticação na blockchain que permite que você faça login de forma segura e pseudônima em dapps na ICP. Isso torna o login em dapps fácil e seguro para os consumidores, ao contrário dos métodos tradicionais de autenticação baseados em nome de usuário e senha, a Internet Identity permite que os usuários se autentiquem usando dispositivos habilitados para criptografia, como smartphones ou laptops.

Ao se cadastrarem na rede, os usuários criam "âncoras de identidade", transformando seu dispositivo em uma espécie de “carteira” segura onde não precisam gerenciar e lembrar de uma senha complexa ou frase de recuperação (*seed*), simplesmente usando seu dispositivo para autenticar. Isso pode ser feito através de atributos compatíveis e criptograficamente habilitados, como o sensor de impressão digital em um laptop, o sistema de ID facial em um telefone, um HSM portátil, como um *YubiKey* ou uma carteira Ledger, tornando o processo de autenticação seguro e intuitivo. Depois disso, eles podem se inscrever e autenticar em qualquer dapp rodando na ICP usando qualquer um dos dispositivos que atribuíram à sua identidade.

Além disso, a *Internet Identity* também serve como forma de backup. Como a identidade do usuário está vinculada ao seu dispositivo, eles podem recuperar o acesso às suas contas simplesmente usando o mesmo dispositivo, tendo a possibilidade de também vincular outros dispositivos confiáveis como backup para caso de perda, roubo, troca etc. Isso contrasta com os sistemas tradicionais de recuperação de conta, que geralmente desabilitam que os usuários lembrem de informações específicas ou tenham acesso a um endereço de e-mail ou número de telefone específico.

A *Internet Identity* também ajuda a melhorar a privacidade do usuário. Cada vez que um usuário interage com um dapp usando sua *Internet Identity*, o dapp vê um pseudônimo gerado especialmente para aquele dapp e isso impede que os dapps rastreiem os usuários em vários dapps, ajudando a proteger a privacidade do usuário.

2.5.1 TECNOLOGIA *CHAIN KEY*

A *Chain Key Cryptography* é um conjunto de protocolos usados e conectados em sistemas no Internet Computer. Estes protocolos são essenciais para operações em tempo real, com autenticação de mensagens e consenso entre computadores.
Um dos protocolos mais importantes é o das assinaturas BLS de limite.

As assinaturas BLS de limite são usadas para garantir que as operações na rede tenham o consenso da maioria dos computadores. Cada computador assina uma transação com sua chave privada e, quando o suficiente concorda, a transação é aceita.

Estas assinaturas têm vantagens sobre métodos tradicionais, sendo mais curtas e seguras. Elas também são eficientes em termos de geração de assinaturas e permitem verificação em lote.

Além disso, as assinaturas BLS podem ser divididas em fragmentos de chave privada, o que possibilita esquemas mais complexos, como assinaturas de limite.

Para implementar as assinaturas BLS em uma rede distribuída, é necessário um protocolo de geração de chaves distribuído (NIDKG), que permite a distribuição segura das chaves entre os computadores da rede.

Este protocolo, desenvolvido pela equipe da Dfinity, supera as limitações dos métodos tradicionais, garantindo segurança e robustez mesmo em redes assíncronas.

Em resumo, as assinaturas BLS de limite e o protocolo NIDKG são fundamentais para garantir a segurança e o funcionamento adequado de sistemas distribuídos, como blockchains. Eles permitem operações seguras e eficientes entre computadores conectados à Internet.

2.6 CENÁRIO DE USO: GOVERNANÇA + PAGAMENTO

Na visão geral do modelo econômico divulgado oficialmente pela DFINITY, o ICP tem dois usos principais, um é bloquear e abrir neurônios e o outro é convertê-lo em combustível para os Ciclos fazerem o contêiner funcionar. Em termos simples, os cenários de utilização do ICP são divididos em governança e troca de recursos computacionais.

Os titulares de ICP podem bloqueá-lo no sistema de governação, votar propostas e participar na governação para obter recompensas. Como compensação para o data center administrar o livro-razão público, ou recompensa em bloco, também é paga com ICP.

Além disso, o ICP também pode ser usado como taxa de pagamento. No ecossistema ICP, a execução de um contrato inteligente (ou contêiner) requer um ciclo de taxas. Ao contrário do Ethereum, a taxa ICP é um preço fixo e basicamente não muda em nenhum momento.

2.6.1 MOEDAS ESTÁVEIS

Além do ICP, dois tipos de Tokens são projetados no DFINITY, que são Ciclos e moedas estáveis. Stablecoins não serão liquidados no curto prazo. A configuração de vários Tokens é baseada na ideia de manter a estabilidade da moeda.

ICP e Ciclos são trocas unidirecionais e a proporção não é fixa, portanto, os Ciclos podem ser mantidos dentro de uma faixa de valor estável. Se a relação de conversão de *Cycles* e ICP for ajustada em tempo real, os *Cycles* também podem ser considerados uma moeda estável.

No futuro, a DFINITY planeja introduzir um data center de recompensa de moeda estável no sistema. A fonte de stablecoins é problemática porque o ICP usado pelo lado do pagamento é destruído. Se as stablecoins vierem das reservas da fundação, todo o sistema deixará de ser um sistema sustentável.

Se a parte de pagamento também for substituída por moeda estável, poderá formar um modelo em que os proprietários de contêineres paguem diretamente ao data center, reduzindo a capacidade de captura de valor do ICP.

Antes de o esquema stablecoin ficar online, a entrada de valor do sistema vem do cenário em que o proprietário do contêiner compra o ICP e o destrói, melhorando assim o escopo e a popularidade do ICP. O valor do ICP aumentará com o uso de redes de computação. Portanto, nos primeiros dias do DFINITY, a solução de moeda estável não será adotada.

O esquema de moeda estável pode reduzir o impacto das flutuações dos preços do ICP no sistema. Depois disso, o valor do ICP só pode refletir os direitos de

governação da rede. Se o valor do ICP for mantido, a solução stablecoin só poderá ser implementada após a conclusão do desenvolvimento do DFINITY.

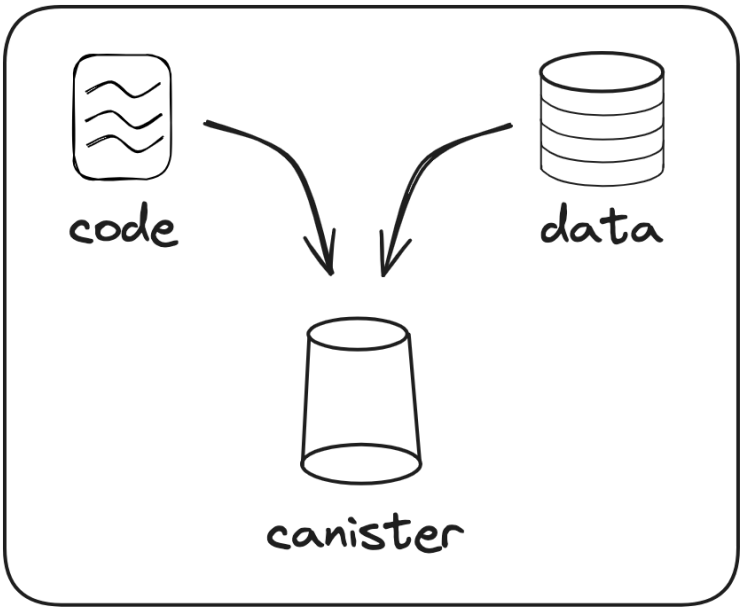
O computador Internet é um projeto único, os atuais sistemas e serviços Internet funcionam a partir de infraestruturas privadas, a tecnologia Chain-Key do ICP mudou tudo isso, permite ter uma chave pública, permitindo que qualquer dispositivo, incluindo relógios inteligentes e celulares, verifique o Autenticidade de artefatos de computador na Internet.

Isso não é impossível para blockchains tradicionais, o ICP pode realizar transações em 5 a 10 segundos e tem escalabilidade quase ilimitada, o que é uma grande melhoria em comparação ao Ethereum.

2.7 CANISTER

Os contratos inteligentes que rodam na ICP são uma evolução dos contratos inteligentes tradicionais, as APIs. Na ICP, os contratos inteligentes são chamados de Canisters e são unidades computacionais que combinam código e dados. Os Canister podem conter qualquer tipo de código ou dados arbitrários, desde veiculação de páginas da web até a criação de um aplicativo de mensagens ou implementação de uma troca de tokens descentralizada.

Ilustração 1 - **Imagem do funcionamento simplificado de um Canister**



Fonte: internetcomputer.org

De acordo com o site oficial da ICP, os Canisters possuem propriedades que permitem aos desenvolvedores construírem serviços na Web3 de forma totalmente escalável. Um desenvolvedor da Ethereum pode pensar em Canisters como contratos inteligentes, enquanto alguém com formação acadêmica em ciência da computação pode fazer associações com atores e com o modelo de ator (atores e modelos de atores em ciência da computação é um modelo matemático de computação simultânea de acordo com a Wikipédia, site fornecido como exemplificação a partir do site oficial da ICP).

2.7.1 CANISTERS COMO CONTRATOS

Os Canisters, assim como os contratos habituais e tradicionais, têm a sua execução regida por um protocolo; neste caso, o protocolo ICP. São à prova de violação, seu estado só pode ser modificado por meio de mensagens executadas na cadeia. O estado de um canister pode ser auditado e verificado criptograficamente, usando a criptografia de chave de cadeia do ICP.

2.7.2 CANISTERS COMO ATORES

Seguindo o modelo de ator da computação simultânea em ciência da computação, os canisters respondem às mensagens que recebem executando uma ou mais das seguintes ações:

- Modificando seu estado privado.
- Envio de mensagens para outros canisters (atores).
- Criando mais canisters (atores).

Embora canisters tenham um único encadeamento de execução, vários podem ser executados simultaneamente. Esta é uma característica fundamental para diferenciar a ICP de outras blockchains, a ICP supera os desafios de escala de outras plataformas de contratos inteligentes.

2.7.3 CANISTERS COMO PROCESSOS

Os Canisters se comportam de maneira semelhante a processos do sistema operacional e da mesma forma que um sistema operacional agenda processos a ICP agenda a execução de canisters.

Os processos do sistema operacional não podem modificar diretamente sua tabela de descritores de arquivos ou manipular dispositivos periféricos, da mesma forma que os canisters não podem modificar diretamente o equilíbrio de seus ciclos de acordo com o site oficial da ICP.

A ICP fornece APIs para os canisters que lhes permitem fazer pagamentos para outros canisters, enviar-lhes mensagens e criar e gerenciar outros canisters.

2.7.4 CANISTERS COMO INSTÂNCIAS

Os Canisters são implementados como módulos *WebAssembly* e isso permite interoperabilidade máxima na aplicação já que os desenvolvedores podem escrever canisters em uma variedade de linguagens direcionadas ao *WebAssembly*.

Um Canister é uma instância do módulo *WebAssembly* que completa seu próprio estado e sua pilha de execução. A memória dos Canisters usa persistência ortogonal, o que torna o armazenamento dos dados do Canister transparente para os usuários. Os dados do módulo *WebAssembly* dos canisters são persistidos automaticamente pelo sistema e estão presentes na próxima vez que o canister for planejado para execução. O próprio módulo *WebAssembly* é armazenado junto com outros bits do estado do Canister.

2.8 DAO

As DAOs (Organizações Autônomas Descentralizadas), são uma das inovações mais importantes trazidas pela tecnologia blockchain. São organizações governadas por regras codificadas como contratos inteligentes, por serem organizadas em torno de tokens blockchain dão aos detentores de tokens o direito de votar em propostas de governança.

DAOs são totalmente transparentes e abertos a qualquer pessoa que possua tokens, tornando-as organizações democráticas e descentralizadas. Eles permitem

que comunidades de indivíduos sejam coordenadas de maneira descentralizada em torno de objetivos comuns, sem a necessidade de uma autoridade central ou intermediária.

2.8.1 DAOS NA GOVERNANÇA DESCENTRALIZADA

Os DAOs desempenham um papel crucial na governança descentralizada, permitindo que os detentores de tokens tomem decisões coletivas sobre o futuro de uma organização, projeto ou protocolo. Isso pode incluir decisões sobre alocação de recursos, desenvolvimento de produtos, contratação de equipe e muito mais.

A governança descentralizada através de DAOs tem o potencial de criar organizações mais justas e equitativas. Ao dar a todos os detentores de tokens uma voz na governança da rede, os DAOs podem ajudar a garantir que as decisões sejam tomadas no melhor interesse de toda a comunidade, em vez de um pequeno grupo de acionistas ou executivos.

2.8.2 DAO SNS

A estrutura do *Service Nervous System* (SNS) é a solução integrada do Internet Computer para organizações autônomas descentralizadas (DAOs) para governar dapps. Um SNS consiste em um sistema de governança aberto e sem permissão e em um token de governança integrado que é exclusivo para cada SNS. A estrutura do SNS inclui um processo sobre como lançar um novo SNS que inclui a angariação de fundos iniciais para o DAO e a descentralização do poder de voto do DAO. Qualquer dapp pode ser tokenizado e descentralizado, entregando-o a um novo SNS DAO.

O Sistema Nervoso de Serviços (SNS) é um recurso fundamental do Internet Computer que permite aos desenvolvedores criarem sistemas de governança descentralizados e baseados em tokens para seus dapps (aplicações descentralizadas). O SNS é um DAO para um dapp específico que usa o mesmo formato e arquitetura que o NNS (*Network Nervous System*) usa para governar o ICP (*Internet Computer Protocol*).

2.8.3 OIS

A ICP é formada em OIS (Open Internet Service), um serviço que mantém todo o seu código, experiência do usuário, computação e dados on-chain e deve ser configurado, atualizado e instruído de forma transparente por um DAO (Descentralized Autonomous Organization) avançado: que no caso, é a estrutura de governança pública chamada por SNS (Service Neuro System), de acordo com o site oficial da ICP.

O primeiro IOS implementado na ICP foi o OpenChat, uma plataforma descentralizada de mensagens, onde, bitcoin e icps podem ser transferidos instantaneamente em mensagens de bate-papo de forma não rastreável e é um serviço governado completamente pela comunidade ICP como um DAO e possui seu próprio token CHAT, que são dados como recompensa aos usuários para impulsionar o crescimento e criar uma equipe de milhões de defensores da ideia.

Um “Serviço de Internet Aberta” (OIS) é um serviço de Internet com a diferença de que funciona inteiramente em uma World Computer blockchain (blockchain mantida por todo o mundo, não tendo apenas um servidor que o mantém), sem centralização.

O OpenChat é um serviço construído a partir de Canisters que são os contratos inteligentes da ICP e que armazenam e processam todos os seus dados, oferecendo a experiência do usuário em navegadores da web. O serviço OpenChat é controlado de forma total pelo DAO SNS (Service Neuro System), que assume o papel que é predominantemente tradicional de uma empresa. Em toda a ICP, não há uma estrutura, conselho de administração ou desenvolvedores no controle, ela é gerada por milhares de membros da comunidade que decidem todas as decisões que serão tomadas na rede, seus desejos são mediados por algoritmos de democracia digital.

2.8.4 COMO O SNS PERMITE A CRIAÇÃO DE SISTEMAS DE GOVERNANÇA DESCENTRALIZADOS E BASEADOS EM TOKENS PARA DAPPS

O SNS permite que os desenvolvedores de dapps criem sistemas de governança descentralizados para seus dapps. Isso é através da criação de um token de governança exclusivo para cada dapp, que é então distribuído aos donos dos

tokens. Os donos dos tokens podem então votar em propostas de governança, permitindo que decidam coletivamente sobre o futuro do dapp.

Isso permite que os dapps sejam realmente descentralizados, com a governança e o controle do dapp nas mãos da comunidade de detentores de tokens. Isso pode levar a uma maior transparência, justiça e responsabilidade, pois todas as decisões são tomadas coletivamente pela comunidade.

DAOs e SNS estão no centro da revolução da Web3 em conjunto para uma revolução no uso da internet, permitindo a criação de organizações e aplicações verdadeiramente descentralizadas.

2.8.5 GOVERNANÇA DO DAPP ATRAVÉS DO DAO SNS

O DAO SNS do *OpenChat* por exemplo, é responsável por tomar decisões importantes sobre o futuro do dapp. Isso inclui decisões sobre novos recursos, alterações na interface do usuário, modificações no contrato inteligente subjacente e muito mais. As decisões são tomadas através de um processo de votação, onde os detentores de tokens do OpenChat podem votar em propostas de governança.

O DAO SNS do OpenChat também é responsável por gerenciar os fundos do dapp. Isso inclui alocação de recursos para desenvolvimento, marketing, recompensas da comunidade e outras despesas operacionais. Os fundos são controlados pela comunidade de detentores de tokens, garantindo que sejam usados de maneira que beneficie a comunidade como um todo.

2.8.6 DESAFIOS E OPORTUNIDADES

Embora a governança descentralizada através de um DAO SNS ofereça muitas vantagens, também apresenta vários desafios. Um dos principais desafios é garantir uma participação ampla e representativa na governança. Isso pode ser difícil de alcançar, especialmente se a distribuição de tokens for específica para um pequeno número de detentores.

Outro desafio é garantir que as decisões de governança sejam tomadas de maneira informada e considerada. Isso requer uma comunicação eficaz e a disponibilidade de informações relevantes para os detentores de tokens.

Apesar desses desafios, a governança descentralizada através de um DAO SNS também oferece muitas oportunidades. Ela permite que a comunidade de usuários tenha uma voz direta no desenvolvimento e gerenciamento do dapp. Isso pode levar a um maior engajamento e satisfação do usuário, bem como decisões que refletem os melhores interesses da comunidade.

2.8.7 IMPLICAÇÕES FUTURAS PARA O ICP, DAOS E SNS

Para o ICP, a adoção bem-sucedida de DAOs e SNS por dapps como por exemplo o OpenChat demonstra o potencial do ICP como uma plataforma para a criação de dapps verdadeiramente descentralizados. Isso pode ajudar a atrair mais desenvolvedores para a plataforma e promover a adoção do ICP.

Para DAOs e SNS, um breve estudo de caso do OpenChat mostraria como essas tecnologias podem ser inovadoras na prática. Isso pode servir como um modelo para outros dapps que buscam implementar uma governança descentralizada.

2.9 NNS

O Sistema Nervoso da Rede (*Network Nervous System*) é a Organização Autônoma Descentralizada (DAO) que governa a *Internet Computer*. Ele é responsável por propor e votar em decisões, como a qual sub-rede um nó deve pertencer, qual versão do protocolo os nós devem executar e quando os nós devem ser atualizados para uma nova versão do protocolo. Qualquer pessoa pode participar do NNS apostando tokens ICP e votando em propostas.

O NNS é responsável por várias operações de gerenciamento de rede, como:

- Atualizar o protocolo e o software do sistema operacional usado pelas máquinas de nós.
- Induzir novos provedores de nós e máquinas para a rede.
- Criar novas sub-redes para aumentar a capacidade da rede.
- Dividir sub-redes para equilibrar a carga da rede.
- Configurar parâmetros que controlam quanto deve ser pago pelos canisters pelo uso de recursos.
- Desativar nós com baixo desempenho para proteger a rede.

As solicitações de mudanças e atualizações na rede são enviadas ao NNS na forma de propostas. O NNS decide adotar ou rejeitar propostas com base na atividade de votação dos detentores de neurônios.

O Sistema Nervoso da Rede (*Network Nervous System*) é a organização autônoma descentralizada (DAO) que governa a *Internet Computer*.
Composta pela comunidade que possuem os tokens do protocolo ICP e bloqueiam seus ativos, com isso ganham a autonomia de participar da liderança da rede e ter poder de voto nas escolhas tomadas dentro do protocolo. Ele é responsável por fazer atualizações de protocolo no ICP e tem controle total sobre a rede. O NNS permite que o ICP seja governado de maneira segura, aberta e descentralizada.

Alguns exemplos de atualizações feitas no ICP através do NNS incluem a atualização do protocolo e do software usados pelas máquinas de nós da rede, a criação de novos sub-redes e a configuração de parâmetros econômicos que controlam quanto os usuários pagam pelos recursos.

Todos os projetos que passam pelo SNS e decidem virar um DAO, após a aprovação da comunidade ele também ganha todas as funcionalidades de um NNS onde o projeto passará a ser governado pela comunidade. Quando uma proposta do NNS é submetida, os participantes da rede votam se devem adotar as mudanças propostas ou rejeitá-las.

A votação é feita por meio de uma democracia líquida, onde os detentores de ICP podem apostar ICP dentro de um neurônio de votação em troca da capacidade de votar em propostas que mudam a ICP. A ICP é usada de incentivo econômico poque é usando de recompensa para pessoas que votam em propostas e participam da rede, fazendo com que seja um impulsionador de uma comunidade engajada e que participe das propostas de votações que decidiram o caminho da rede, assim como é usado de recompensa para pessoas que decidem hospedar seus servidores e nodos ao redor do mundo, tornado uma rede descentralizada e autônoma. O NNS é realizado por um conjunto de canisters. Para tomar decisões, dois desses canisters são fundamentais:

1. **Canister de Governança**: Armazena propostas, que são sugestões de como o Internet Computer deve ser alterado. Essas propostas podem então ser votadas. Ele também armazena neurônios, que determinam quem pode participar da governança.

2. **Canister de Registro**: Armazena a configuração de toda a *Internet Computer* que pode ser consultada por outros. Por exemplo, armazena quais nós pertencem a uma determinada sub-rede.

O NNS também combina nós de centros de dados independentes para criar sub-redes, que são usadas para hospedar contratos inteligentes. O NNS continua a criar sub-redes com base nas demandas de capacidade de hospedagem de contratos inteligentes e na capacidade de se conectar a outras sub-redes, permitindo que o Internet Computer escale indefinidamente.

Um DAO é de extrema importância para uma rede que quer se tornar descentralizada. Como podemos ver na arquitetura do Bitcoin e nas demais redes onde não existe um DAO como no ICP, fazendo com que esses outros protocolos se tornem um ponto de centralização em algo fundamental como é na governança de uma rede.

Um exemplo é o Bitcoin, onde muitas propostas são tomadas por desenvolvedores que continuam atualizando e fazendo melhorias no protocolo, mas que não seguem um consenso de governança como um DAO, com isso o maior incentivo de um desenvolvedor para não realizar uma ação mal intencionada é o fato do código ser *open source*, e que muitos desses desenvolvedores estão na rede desde o gêneses do Bitcoin, fazendo com que tenham uma quantidade muito grande de BTC, tornando isso seja um grande incentivo para esses desenvolvedores tomarem boas decisões mesmo que seja a benefício próprio, mas pensando em um logo prazo de 20, 30 40, 50 anos onde esse desenvolvimento será ocupado por novos programadores, onde muito desses não terão uma quantia tão grande de BTC, fazendo com que tenhamos uma diminuição pelo interesse na manutenção do código e atualização da rede, tornando isso um ponto focal de um problema de longo prazo.

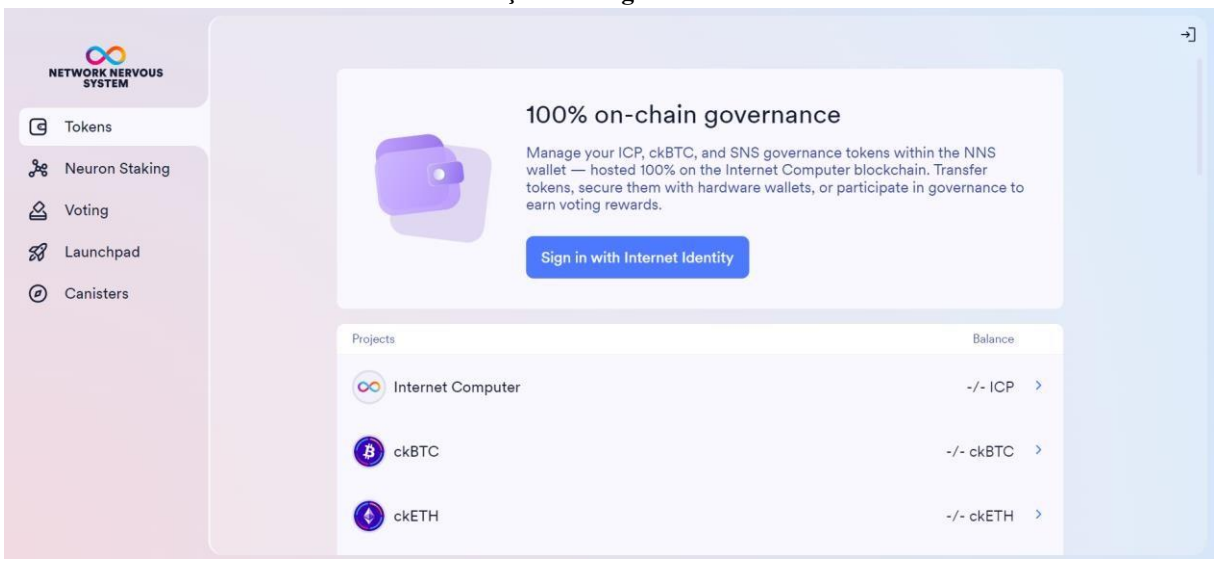
Com um sistema de NNS que roda em um DAO, podemos implementar e votar em propostas de tesouraria para desenvolvimento e atualizações futuras contínuas, tudo isso sendo feito por um sistema de governança descentralizada, sem a necessidade de confiança em terceiros e feita por contratos inteligentes. Assim temos a arquitetura de uma rede que pode ser escalada infinitamente autônoma, se adaptar a mudanças engajar seus participantes e ter uma grande equipe global de desenvolvimento e manutenção de código de forma segura, autônoma e descentralizada.

2.9.1 COMO USAR O NNS

Para interagir com o NNS, você pode usar o aplicativo NNS ou outras ferramentas, como o quill e o ic-js. Aqui mostraremos pode mostrar como usar o NNS através do aplicativo NNS.

Ao acessar o site https://nns.ic0.app/ aparecerá a seguinte página

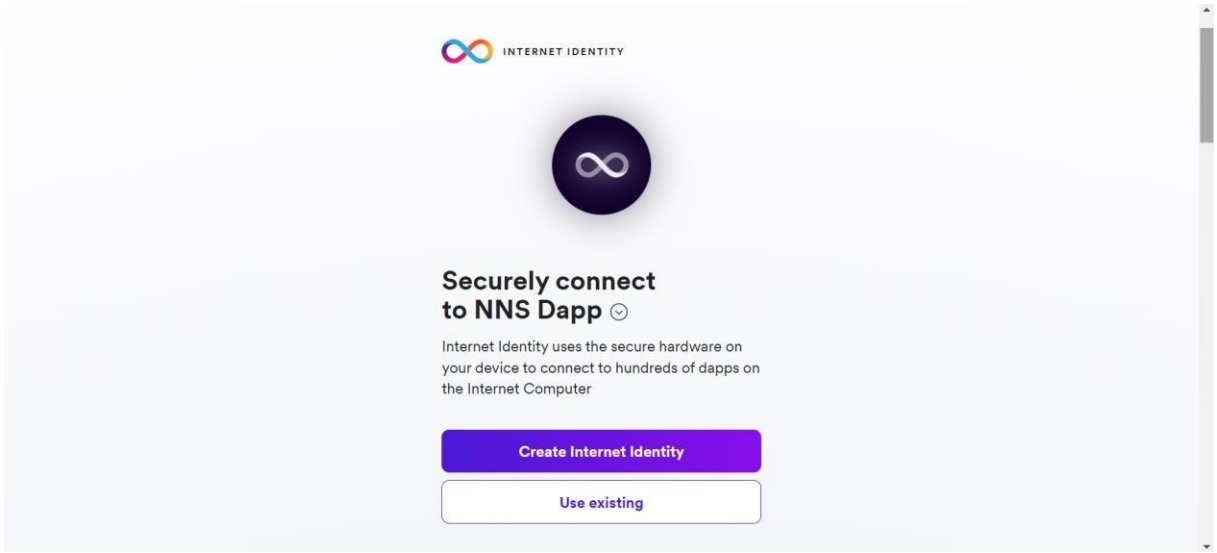
Ilustração 2 – Página de início



Fonte: Imagem do autor

Para entrar na sua carteira NNS ou criar uma, clicaremos em “Sign in with Internet Identity”

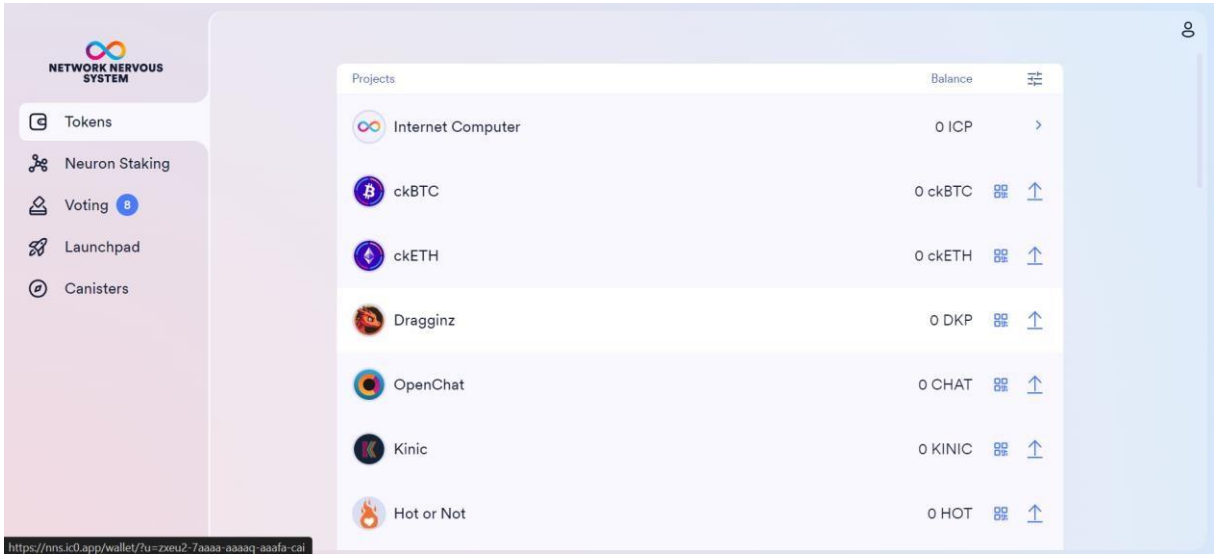
Ilustração 3 – Página de login/criação de carteira



Fonte: Imagem do autor

Ao entrar na sua carteira, a primeira guia que irá abrir será a “Tokens”, é onde você terá acesso aos tokens que você fez investimento, assim como outros tokens que a rede tem disponíveis para compra e os atalhos para que você possa votar, fazer a gestão dos tokens que você tem disponível e outras funcionalidades que a *Internet Computer* fornece na plataforma.

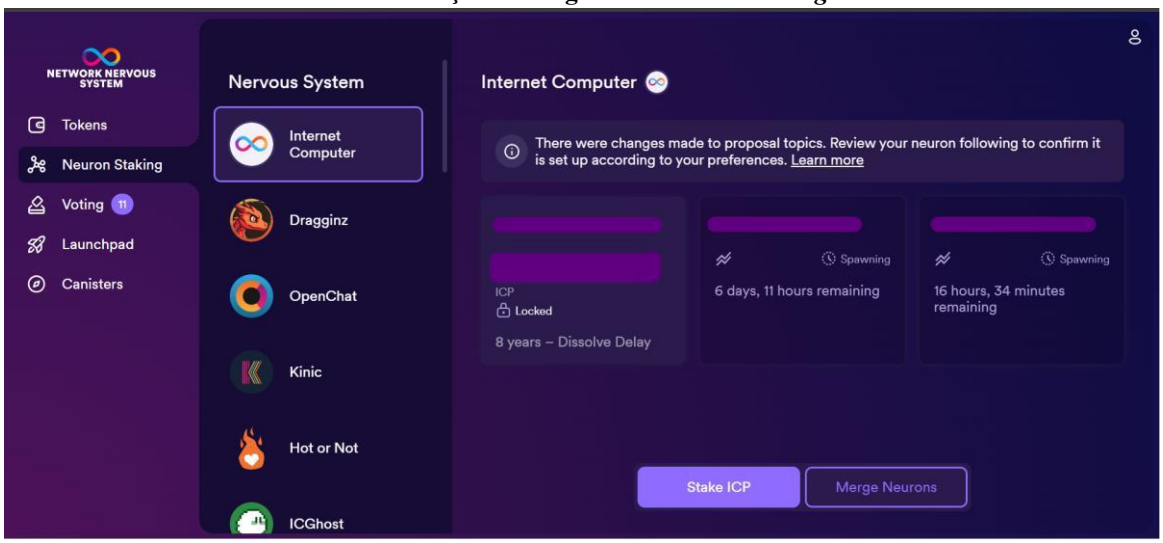
Ilustração 4 – Página inicial ao logar no NNS



Fonte: Imagem do autor

Para fazer votações, você precisa ter um token bloqueado em um neurônio na guia *Neuron Staking* em sua carteira. O token bloqueado terá o tempo que você irá definir e de acordo com o tempo que foi dado, o neurônio terá mais maturidade (mais poder de voto) para as votações que serão feitas na comunidade e o seu token irá render mais a cada token injetado neste neurônio. Entrando na guia de *Neuron Staking*, em uma carteira que tem um token bloqueado, teremos a seguinte visão.

Ilustração 5 – Página de *Neuron Staking*

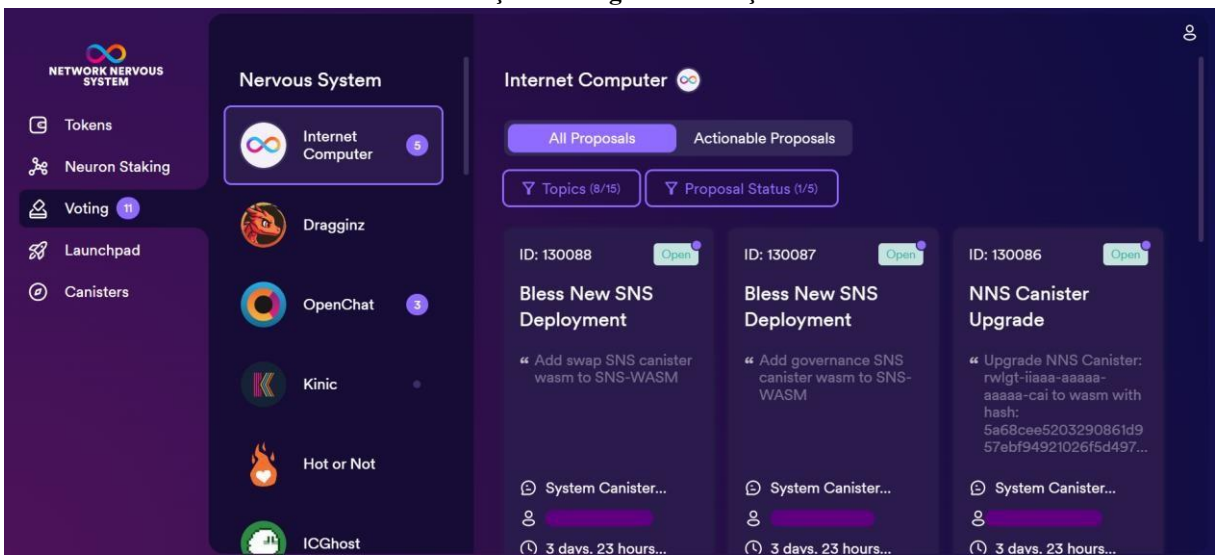


Fonte: Imagem do autor

Ao entrar em *Neuron Staking*, você terá acesso aos neurônios que estão bloqueados em sua carteira, no exemplo acima, temos uma carteira bloqueada em 8 anos (tempo máximo de bloqueio de neurônio) e mais outras duas carteiras que ainda não estão disponíveis para o usuário (no caso, o usuário ganhou em *air-drops* ou como recompensa em algum outro investimento).

Ao entrar no neurônio você tem acesso ao rendimento do token, opções como *Dissolve Increase* para que você possa começar a dissolver seu neurônio (o tempo irá diminuindo e ao final do tempo decorrido que escolher o neurônio estará desbloqueado e você conseguirá usar os tokens). Para fazer votações, o usuário precisa acessar a guia *Voting* e lá, todas as propostas da comunidade, em que você tem um neurônio com maturidade, estarão disponíveis para voto.

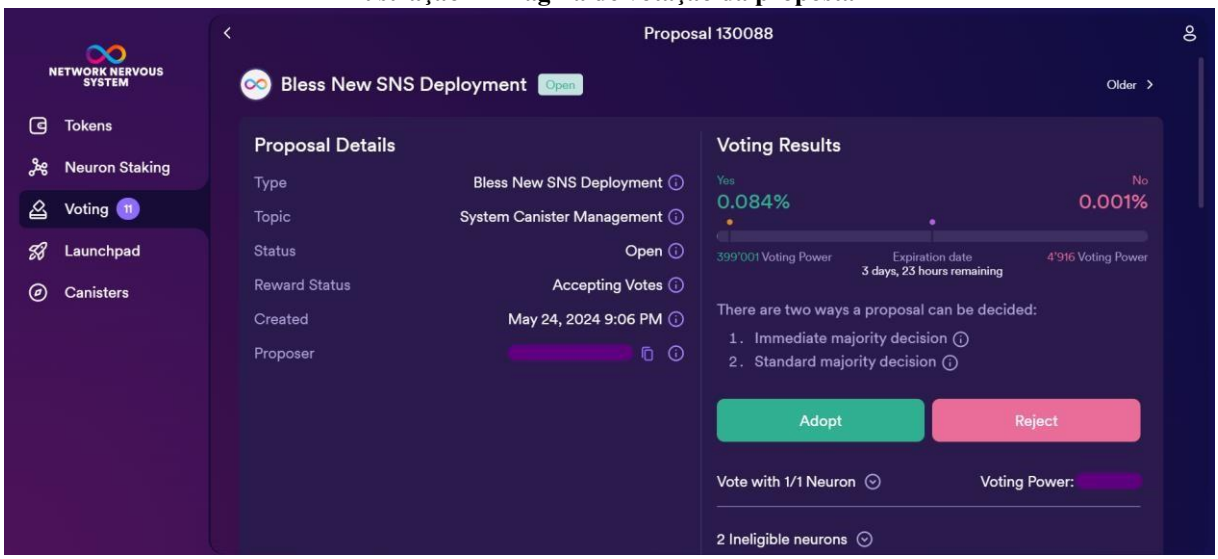
Ilustração 6 – Página de votação



Fonte: Imagem do autor

Assim como mostra a ilustração acima, ao clicar em *Voting*, as propostas da comunidade são exibidas para o usuário, que ao clicar em alguma, terá acesso à leitura do material de implementação da proposta, porcentagem de aceite e aos botões de *Adopt* ou *Reject* para adoção ou rejeição da proposta que propuseram.

Ilustração 7 – Página de votação da proposta



Fonte: Imagem do autor

3 CONCLUSÃO

Em conclusão, a Internet Computer representa uma inovação significativa na interação entre a internet e a tecnologia blockchain. Desenvolvida pela DFINITY Foundation, este projeto ambicioso busca criar uma internet descentralizada onde o software pode ser construído e executado com capacidades equivalentes aos serviços web tradicionais, mas com os benefícios adicionais da tecnologia blockchain.

A Internet Computer utiliza o token ICP, que permite aos usuários participar da governança da rede através do Sistema Nervoso da Rede (NNS), uma DAO que controla a blockchain do projeto. Esse sistema de governança, baseado em participação e democracia líquida, oferece uma plataforma descentralizada onde qualquer pessoa pode influenciar diretamente o desenvolvimento e a governança do sistema.

Além disso, a eficiência energética do ICP, que utiliza um mecanismo de votação em seu algoritmo de consenso, se destaca em comparação com blockchains baseadas em Prova de Trabalho, pois evita desperdícios de energia em cálculos desnecessários. O ICP também tem a capacidade de hospedar websites, aplicativos e ecossistemas inteiros na blockchain, sem depender de provedores de nuvem tradicionais, democratizando o acesso à internet e tornando-a mais acessível.

A capacidade do ICP de interagir diretamente com outras blockchains, como a Bitcoin, através de contratos inteligentes que podem ler e escrever o estado dessas redes de forma segura e descentralizada, é outro diferencial importante. O projeto também promove a educação e o envolvimento da comunidade através do Programa de Subsídios da Comunidade ICP, que apoia equipes e indivíduos na missão de educar e inspirar comunidades globais e locais sobre as capacidades do Internet Computer.

Em suma, a Internet Computer tem o potencial de transformar a TI tradicional e impulsionar uma nova geração de serviços e aplicações Web3, oferecendo uma internet mais eficiente, acessível e descentralizada.

REFERÊNCIAS

CORREIA, Kenneth. **Web 3.0: o que é, quais as vantagens e diferenças para a Web 2.0?** Disponível em: https://digital.futurecom.com.br/especialistas/web-30-o-que-e-quais-vantagens-e-diferencas-para-web-20?gad_source=1&gclid=EAIaIQobChMI5vep4-vghgMVYV5IAB231wlxEAAYASAAEgJy0PD_BwE. Acesso em: 09 mar. 2024

LOURENTI, André. **O que é a Web3?** Disponível em: https://canaltech.com.br/internet/o-que-e-a-web3/. Acesso em: 09 mar. 2024

DFINITY. **Web3: The bull case for the Internet Computer**. Disponível em: https://wiki.internetcomputer.org/wiki/Web3:_The_bull_case_for_the_Internet_Computer. Acesso em: 09 mar. 2024

DFINITY. **Introduction to ICP**. Disponível em: https://wiki.internetcomputer.org/wiki/Introduction_to_ICP#firstHeading. Acesso em: 10 mar. 2024

SILVA, Genilson. **Web3 vs Web 3.0: Descubra as Diferenças e Seu Impacto**. Disponível em: https://www.made4u.com.br/conteudo/blog/web3-vs-web-3-0-diferencasimpacto#:~:text=A%20web3%20faz%20uso%20da,0%20podem%20ser%20facilmente%20alterados. Acesso em: 10 mar. 2024

NathanosDev. **Overview of ICP**. Disponível em: https://internetcomputer.org/docs/current/developer-docs/getting-started/overview-of-icp. Acesso em: 11 mar. 2024

MONGEON, Jesse. **Smart Contracts, Overview, Introduction.** Disponível em: https://internetcomputer.org/docs/current/developer-docs/smart-contracts/overview/introduction. Acesso em: 13 mar. 2024

DFINITY TEAM. **The Internet Computer for Geeks.** Disponível em: https://internetcomputer.org/whitepaper.pdf. Acesso em: 20 mar. 2024

ROSSBERG, Andreas. **Motoko, a Programming Language Designed for the Internet Computer, Is Now Open Source.** Disponível em: https://medium.com/dfinity/motoko-a-programming-language-designed-for-the-internet-computer-is-now-open-source-8d85da4db735#d62f. Acesso em: 21 mar. 2024

DFINITY TEAM. **Compute on Blockchain**. Disponível em: https://internetcomputer.org/. Acesso em: 21 mar. 2024

DFINITY. **WebAssembly on the Internet Computer.** Disponível em: https://medium.com/dfinity/webassembly-on-the-internet-computer-a1d0c71c5b94#f829. Acesso em: 21 mar. 2024

DFINITY. **WebAssembly.** Disponível em: https://wiki.internetcomputer.org/wiki/WebAssembly#firstHeading. Acesso em: 21 mar. 2024

DFINITY. **Introducing The Newly Improved ICP Community Grants Program**. Disponível em: https://medium.com/dfinity/introducing-the-newly-improved-icp-community-grants-program-d19562ec309e#f5dd. Acesso em: 01 abr. 2024

DFINITY. **Internet Computer: Unique Features**. Disponível em: https://identitysupport.dfinity.org/hc/en-us/articles/27213203194004-Internet-Computer-Unique-Features. Acesso em: 17 abr. 2024

WILLIAMS, Dominic. **Why Totally Decentralizing Dapps Wins, and How to Do It**. Disponível em: https://medium.com/dfinity/how-dapp-developers-placing-their-faith-in-total-decentralization-will-inherit-the-world-79419a3e36c9#a27f. Acesso em: 19 abr. 2024

LANGHAM, Kyle. **Enterprise Software on the Internet Computer Blockchain**. Disponível em: https://medium.com/dfinity/blockchain-technology-is-already-rapidly-transforming-software-but-the-internet-computer-is-47fbec098267#42e7. Acesso em: 23 abr. 2024

DFINITY. **Why Bitcoin needs smart contracts**. Disponível em: https://medium.com/dfinity/why-bitcoin-needs-smart-contracts-5191fbec294a#acf6. Acesso em: 24 abr. 2024

MONGEON, Jesse. **NNS Quickstart.** Disponível em: https://internetcomputer.org/docs/current/developer-docs/daos/nns/nns-app-quickstart#overview. Acesso em: 10 mai. 2024

DFINITY. **Is there anything the Internet Computer Protocol is doing or anything about the technology that makes it an environmentally sustainable option?** Disponível em: https://support.dfinity.org/hc/en-us/articles/4417926836372-Is-there-anything-the-Internet-Computer-Protocol-is-doing-or-anything-about-the-technology-that-makes-it-an-environmentally-sustainable-option. Acesso em: 13 mai. 2024