Ações estratégicas para redes futuras

Tendências em Blockchain para Redes de Telecomunicações

M1 A1.2

FUNTTEL

FUNDO PARA O DESENVOLVIMENTO TECNOLÓGICO DAS TELECOMUNICAÇÕES

AGRADECIMENTOS

Os autores agradecem o apoio financeiro dado a este trabalho por meio do FUNTTEL (Fundo para o Desenvolvimento Tecnológico das Telecomunicações) e da FINEP (Financiadora de Estudos e Projetos), sob o processo n.º 1508/22. Este artigo reflete apenas as opiniões dos autores; as agências não são responsáveis por qualquer uso que possa ser feito das informações nele contidas.

TENDÊNCIAS EM BLOCKCHAIN
PARA REDES DE TELECOMUNICAÇÕES

1. INTRODUÇÃO

A Blockchain é a mais proeminente implementação de tecnologia de livro de registro distribuído (Distributed Ledger Technology ou DLT) que utiliza princípios criptográficos e algoritmos avançados para armazenar, trocar e sincronizar dados de forma imutável em uma rede descentralizada. As DLTs possibilitam que os nós em uma rede distribuída alcancem um consenso e registrem dados sem depender de uma autoridade central. Cada bloco de dados é criptograficamente vinculado e protegido contra adulteração e revisão. Essa estrutura garante a integridade dos dados registrados e oferece segurança e confiabilidade aos participantes da rede, uma vez que qualquer tentativa de alteração exigiria a modificação de todos os blocos subsequentes na cadeia, tornando o sistema altamente resistente a manipulações [ITU-T, 2019].

A tecnologia Blockchain foi construída considerando as principais características arquiteturais: (i) segurança das operações; (ii) descentralização de armazenamento e computação; (iii) integridade de dados; e (iv) imutabilidade de transações [MARINO et al., 2020].

A evolução da Blockchain começou com as criptomoedas em 2008, quando Satoshi Nakamoto propôs a criptomoeda Bitcoin como um livro-razão descentralizado, frequentemente denominado “especificação Blockchain 1.0”. Mais tarde, na Blockchain 2.0, os contratos inteligentes (Smart Contracts ou SC) foram projetados para automatizar os fluxos transacionais entre pares por meio de regras definidas e especificações de configurações de contrato [SARASWAT et al., 2022].

A Blockchain 3.0 surgiu com o design de vários aplicativos descentralizados e a adoção da tecnologia em diferentes setores como saúde, finanças e outros. Atualmente, o processo de transformação da Indústria 4.0 permitiu a comunicação orientada por sensores, o que fez com que as aplicações de *big data* ganhassem atenção. Com a geração e ingestão massiva de dados, os requisitos de segurança e privacidade tornaram-se primordiais [SARASWAT et al., 2022].

2. BLOCKCHAIN E A WEB 3.0

A Web 3.0, também conhecida como Web descentralizada, é a evolução da Web atual (Web 2.0) para uma Internet na qual os usuários terão maior controle sobre seus dados e interações on-line, promovendo a descentralização, a privacidade e a segurança. Ao contrário da Web 2.0, na qual muitos serviços e dados estão centralizados em empresas e plataformas, a Web 3.0 propõe o uso de tecnologias descentralizadas, blockchain e contratos inteligentes, que permitirão a criação de aplicativos e serviços que operem em redes *peer-to-peer* e deem mais autonomia e controle aos usuários [SHUKLA et al., 2022].

A arquitetura da Web 3.0 visa superar os problemas da Web 2.0, caracterizada pelo controle de conteúdo por autoridades centrais. Na Web 3.0, os usuários passam a ser os proprietários do conteúdo que publicam, permitindo a tomada de decisão baseada nos interesses dos usuários. Eles têm controle sobre quais dados são coletados e como são utilizados. Iniciativas como o navegador Brave exemplificam esse modelo, compartilhando uma porcentagem da receita publicitária gerada com a coleta de dados dos usuários, sendo que 70% da receita é destinada aos usuários e apenas 30% são retidos pela empresa. Isso reflete um modelo de negócios mais justo e transparente na Web 3.0 [SHUKLA et al., 2022].

- **BRAVE (BASIC ATTENTION TOKEN - BAT)**

O projeto Brave introduz o BAT (Basic Attention Token), um token usado para facilitar a troca descentralizada de anúncios. Ele compensa os

usuários do navegador com base em sua atenção, sem deixar de proteger sua privacidade.

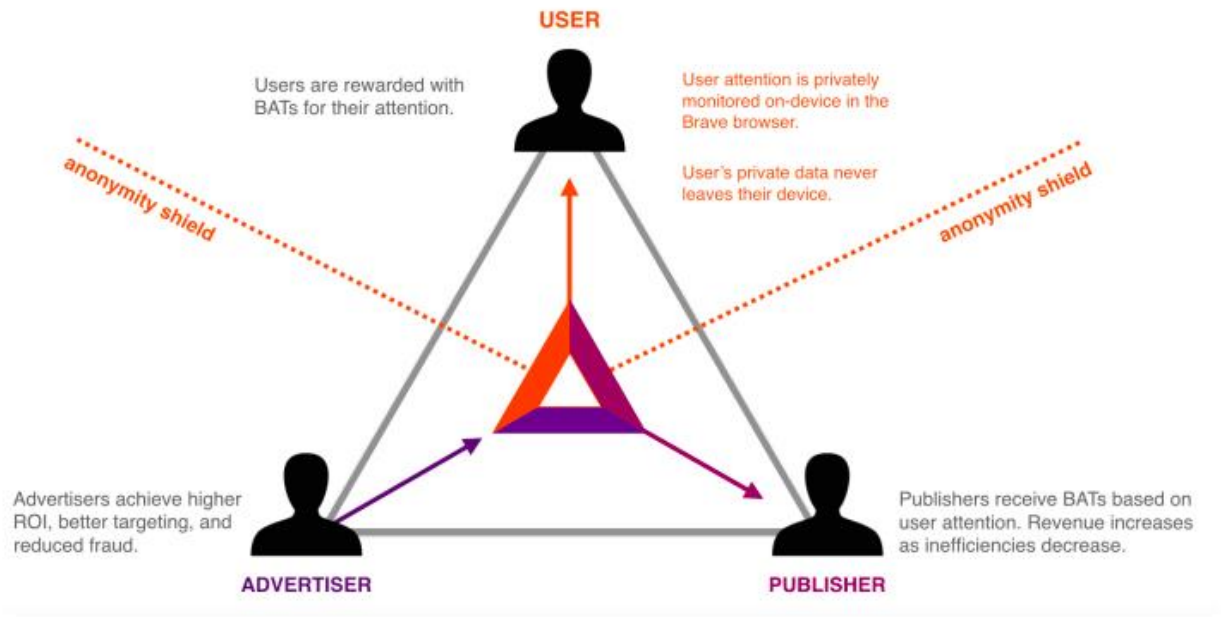

Figura 1 – BAT Digital Ad Flow [BRAVE SOFTWARE, 2021]

O BAT conecta anunciantes, editores e usuários, eliminando os problemas encontrados nas redes de anúncios convencionais, como, por exemplo: fraudes, violações de privacidade e anúncios maliciosos. Vemos o BAT e suas tecnologias associadas como uma parte integral dos futuros padrões da Web, resolvendo o desafio essencial de monetizar o conteúdo dos editores, ao mesmo tempo que protege a privacidade dos usuários [BRAVE SOFTWARE, 2021].

- **MOBI - MOBILITY OPEN BLOCKCHAIN INITIATIVE**

MOBI é um consórcio focado na criação de padrões e colaboração necessários para habilitar a infraestrutura digital Web 3.0 para veículos conectados e o comércio IoT (Internet das Coisas). O consórcio foi

fundado pelas principais montadoras de carros, incluindo: Renault, Ford, GM e BMW, e agora representa mais de 80% da produção automotiva global em volume [MOBI, 2021]. Os membros do MOBI incluem *startups* atuantes em Blockchain e grandes corporações como a IBM, Accenture e ConsenSys. Também estão envolvidas organizações não governamentais, como o Fórum Econômico Mundial, e instituições acadêmicas, como o grupo Blockchain em Berkeley. Todas essas partes acreditam no valor do desenvolvimento multipartidário e cooperativo de novas soluções de tecnologia Blockchain para a indústria.

O primeiro projeto é construir um protótipo de identidade digital de veículo ou passaporte de carro que possa rastrear e proteger o odômetro de um veículo e dados relevantes em livros distribuídos. Isso pode reduzir drasticamente a fraude nas vendas de carros usados, pois os compradores poderão finalmente ter um histórico preciso do veículo.

3. BLOCKCHAIN E OS SISTEMAS OSS/BSS

Atualmente, estão sendo desenvolvidas várias aplicações que utilizam a tecnologia DLT para tarifação de serviços, controle de SLA via contratos inteligentes e construção de *marketplace* descentralizado de serviços de comunicação. Um exemplo disso é a iniciativa do TM Forum denominada Catalyst, cujo objetivo é promover colaborações mutuamente benéficas entre prestadores de serviços, permitindo a interoperabilidade de uma

variedade de plataformas DLT maduras e prontas para integração, usando um conjunto de padrões aceitos pela indústria de telecomunicações.

A solução desenvolvida para confiança de dados e garantia de negócios torna-se facilmente acessível a todas as partes do ecossistema em qualquer estágio de seu processo de integração. A Figura 2 mostra a arquitetura do Catalyst, do TM Forum 2020 [ADHIAPPAN et al., 2020].

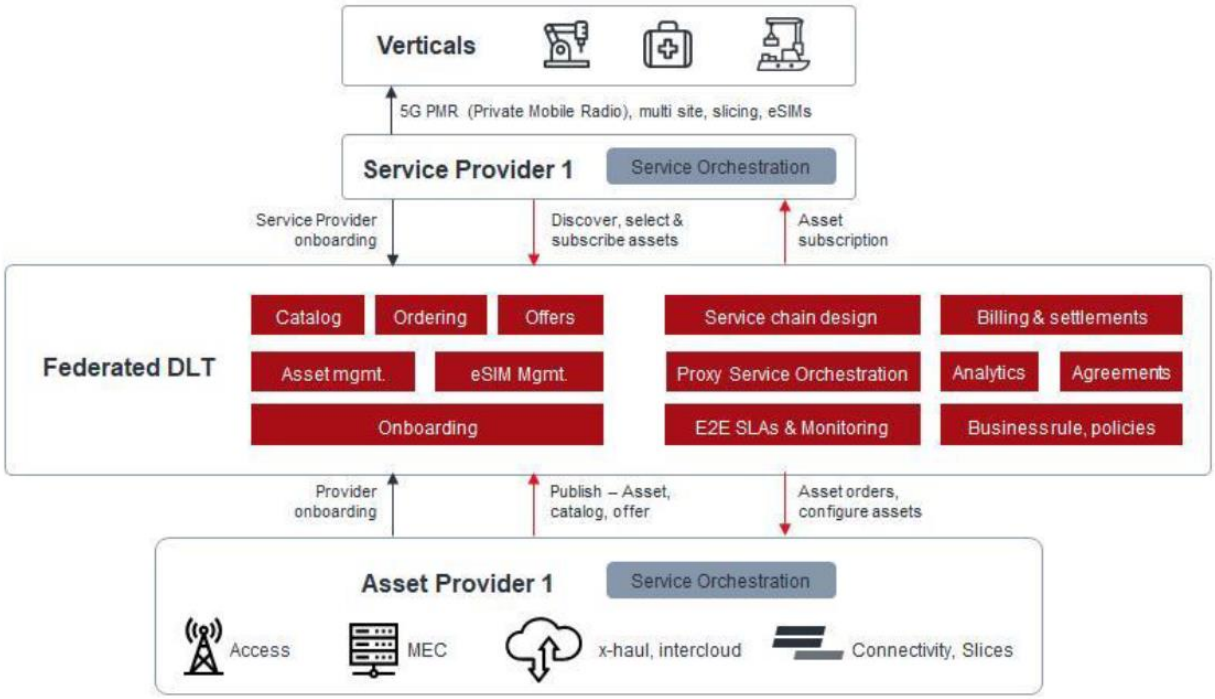

Figura 2 – TM Forum 2020 Catalyst ecosystem

Aproveitando a tecnologia DLT, esse mercado federado alcança a ambição de garantir maior confiança e reduzir o tempo de liquidação, riscos e fraudes quando os Provedores de Serviços de Comunicação (Communication Service Provider ou CSP) colaboram entre si e, de modo

federado e seguro, compartilham seus ativos. A infraestrutura de confiança de dados desenvolvida torna-se então disponível para a integração do Catalyst. Dessa forma, os futuros operadores de mercado também podem explorar a oportunidade de tornar os tokens a "moeda de troca" dos mercados de CSPs federados, fazendo com que todos os participantes e partes interessadas tenham que comprar e trocar seus ativos por uma quantidade predefinida de tokens.

Um segundo exemplo está relacionado com a tarifação de energia elétrica para veículos elétricos. Nesse contexto, a tecnologia Blockchain é utilizada para simplificar os processos de pagamento relacionados ao uso desses veículos. A adição da tecnologia Blockchain pode viabilizar uma rede de carregamento de veículos elétricos mais eficiente [AWAIS et al., 2022]. Nesse caso, a Blockchain funciona como uma tecnologia semelhante à criptomoeda Bitcoin, registrando todas as transações em um banco de dados público. Inicialmente, obtém-se o valor do nível de carga da bateria dos veículos elétricos e sua localização em tempo real. Com base nessas informações, é possível estimar a quantidade de tokens (criptomoeda) a ser cobrada do usuário [RUAN et al., 2017]. Em seguida, são coletadas informações das transações registradas no banco de dados ou dos tokens presentes nas carteiras dos usuários, e essas informações são transmitidas aos fornecedores de energia elétrica. Por fim, os registros das transações são enviados de volta ao usuário.

Para esses cenários, as abordagens mais comuns são as tecnologias Blockchain permissionadas, nas quais as aplicações são desenvolvidas com o devido nível de controle e gerenciamento. A confiabilidade dos nós é garantida por meio de condições estabelecidas pelo iniciador da

rede, e o compartilhamento de dados é determinado pelo provedor dos dados. Os protocolos de consenso utilizados nessas tecnologias Blockchain permissionadas consomem menos energia e tempo. Exemplos de tecnologias Blockchain que podem ser utilizadas são o Hyperledger Fabric e o R3 Corda [GUR et al., 2019].

O método tradicional na gestão das transações entre distribuidoras e consumidores é caracterizado pela falta de automação e transparência nos sistemas de faturamento e distribuição de energia. Os sistemas de medição atuais dependem principalmente de leituras manuais dos medidores de consumo, o que impede o monitoramento eficiente dos níveis de consumo. A Figura 3 mostra uma arquitetura descentralizada de uma blockchain na qual os dispositivos IoT podem ser integrados para medir automaticamente o consumo de energia e interagir com a blockchain, permitindo o desenvolvimento de uma solução econômica, escalável, segura e energeticamente eficiente de monitoramento do consumo de energia doméstico [GUR et al., 2019].

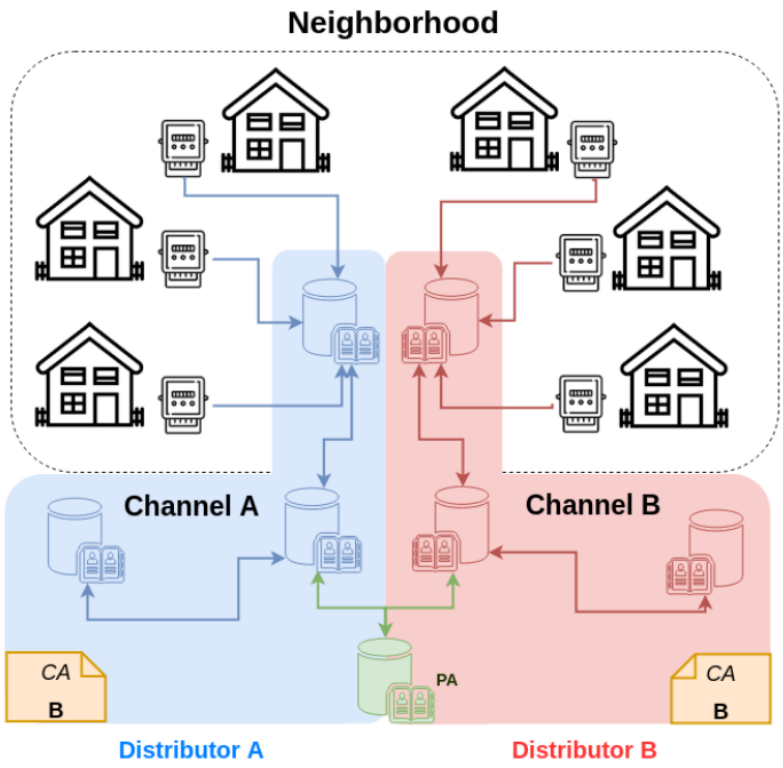

Figura 3 – Arquitetura de caso de uso de monitoramento do consumo de energia doméstico com dispositivos IoT e Blockchain

4. BLOCKCHAIN E SISTEMAS AVANÇADOS SEM FIO

Na pesquisa sobre redes 6G e Blockchain, um foco importante é aprimorar a segurança, especialmente para redes IoT. Uma solução promissora envolve descentralizar o aprendizado de máquina, uma técnica em que algoritmos aprendem padrões a partir de dados, aplicando esse aprendizado à "inteligência de borda". Inteligência de borda refere-se ao processamento de dados próximo à fonte dos dados

(por exemplo, dispositivos IoT) em vez de em um local centralizado, como a nuvem. Isso é crucial para as redes 6G, que suportarão enormes quantidades de dispositivos IoT, exigindo processamento rápido e seguro [NGUYEN et al., 2022].

A Blockchain, um sistema de registro seguro e descentralizado, pode autenticar parâmetros relevantes dos modelos de inteligência artificial (IA) usados na borda. Ou seja, permite que os dispositivos de borda verifiquem se um modelo de IA é confiável, sem expor os dados sensíveis utilizados para treinar o modelo. Além disso, a segurança do fluxo de dados no modelo de IA pode ser reforçada com técnicas de criptografia baseadas em Blockchain, protegendo contra alterações maliciosas dos dados [NGUYEN et al., 2022].

Essas estratégias visam assegurar a integridade, privacidade e segurança dos dados em redes 6G, criando um ambiente confiável para aplicativos que dependem de processamento de dados em tempo real na borda da rede, como dispositivos IoT avançados [NGUYEN et al., 2022].

Os nós na arquitetura 6G são projetados para fornecer suporte às comunicações por meio de serviços virtualizados e gerenciamento de rede avançado, ampliando as interfaces de acesso sem fio, para permitir a criação de um sistema distribuído e sem células com múltiplos pontos de acesso massivos. A tecnologia 6G é capaz de operar em frequências terahertz, oferecendo uma taxa de dados de experiência do usuário de até 1 terabit por segundo e uma latência de ida e volta de até 0,1 milissegundo. Além disso, o 6G suporta serviços como comunicações extremamente confiáveis de baixa latência (eRLLC) com uma taxa de confiabilidade de 99,9999999%, superando as redes 5G em termos de desempenho e confiabilidade [SAAD et al., 2020].

Em redes baseadas em 6G, a segurança e a privacidade representam desafios práticos decorrentes da natureza distribuída desses sistemas, que estão sujeitos a diversos riscos e ameaças. Garantir a privacidade dos dados em ambientes de compartilhamento aberto, como o compartilhamento de dados veiculares em veículos autônomos, é particularmente crítico. O uso da tecnologia Blockchain surge como uma solução inovadora para enfrentar esses desafios de segurança e privacidade nas redes 6G.

Nesse sentido, a Blockchain desempenha um papel crucial no estabelecimento de sistemas autônomos seguros, permitindo que Veículos Aéreos Não Tripulados (Unmanned Aerials Vehicles ou UAVs) atuem como clientes da rede Blockchain e se comuniquem com estações-base terrestres para troca e compartilhamento de dados, a fim de cumprir suas missões, como busca de emergência ou monitoramento ambiental. Isso é possível por meio de um livro-razão ponto a ponto, conforme ilustrado na Figura 4. A utilização da Blockchain permite que UAVs, usuários terrestres e operadores de rede confiem nos dados armazenados no registro, graças ao controle compartilhado e ao direito de rastreamento possibilitados pelo ambiente distribuído. Outra aplicação viável é a assistência médica inteligente, na qual sistemas de saúde baseados em 6G podem implementar a verificação de dados de saúde por meio da Blockchain e sua tecnologia de contrato inteligente, eliminando a necessidade de intermediários e garantindo um alto grau de confiabilidade. No entanto, é importante considerar que a implementação da Blockchain em redes 6G-IoT futuras também pode resultar em custos adicionais, como aumento de latência e consumo de energia [NGUYEN et al., 2022].

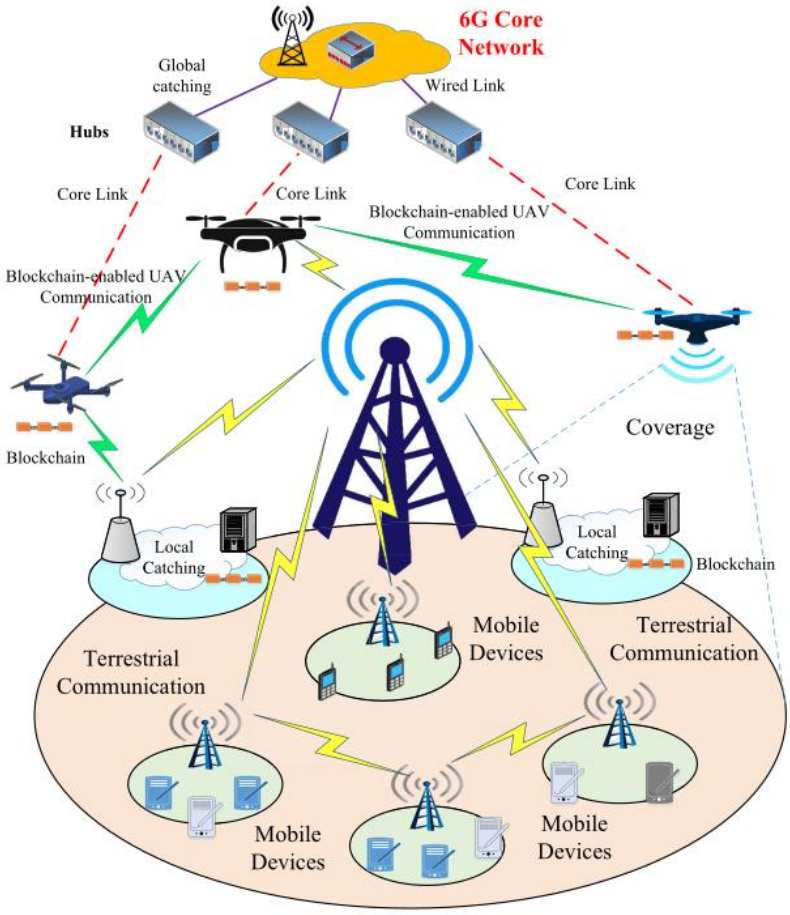

Figura 4 – Blockchain redes seguras 6G UAV

- **HELIUM NETWORK**

Helium é uma infraestrutura de comunicações sem fio constituída por uma rede de pontos de acesso (*hotspot)* vinculados a uma Blockchain. Os Helium Hotspot são dispositivos IoT sem fio capazes de fornecer uma área de cobertura muito maior do que o Wi-Fi. Dependendo da região e dos requisitos, podem ser necessários apenas 50 pontos de acesso para fornecer conectividade para uma cidade inteira. Por ser uma rede descentralizada, o Helium não só é totalmente criptografado – tornando privadas as informações que trafegam pela rede – como também é

capaz de oferecer um nível de segurança que uma empresa centralizada não oferece. Com os *hotspots* espalhados pelo mundo, a rede está protegida em relação a um único ponto de ataque [DZHUNEV, 2022].

Para que um dispositivo final utilize a rede Helium para transferência de dados, conforme apresentado na Figura 5, ele deve ser capaz de se comunicar com os *gateways*, através do protocolo LoRaWAN (*Long Range Wide Area Network*), e com a Blockchain Helium. Sem conexão com a rede Helium, os dados não podem ser trocados entre os dispositivos finais e a Internet. Ou seja, a rede Helium funciona como um intermediador de comunicação e transferência de dados.

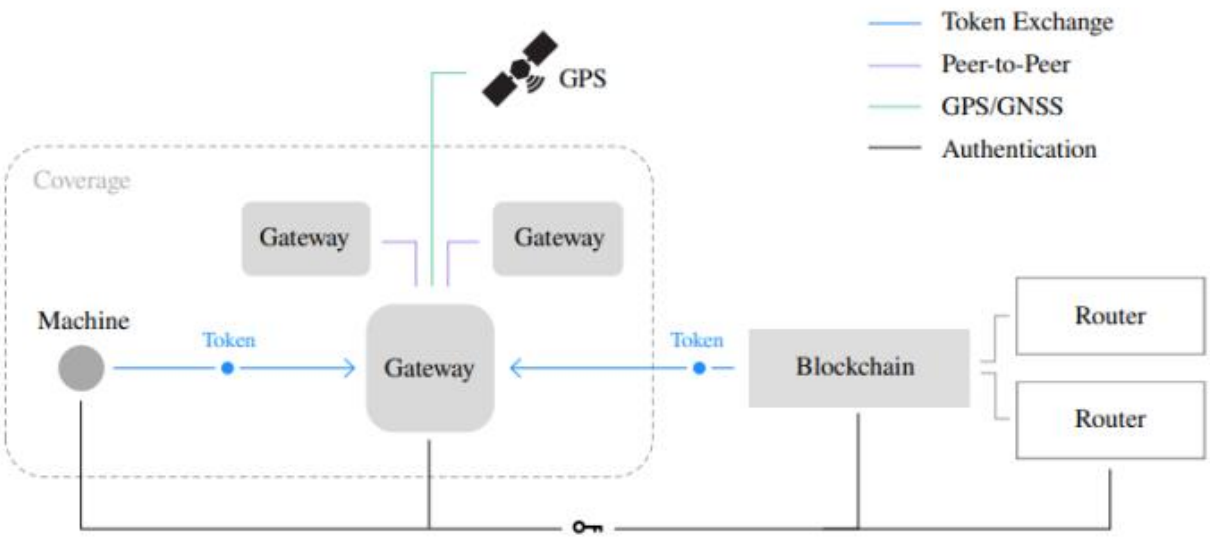

Figura 5 – Visão geral da rede Helium

5. ATUAÇÃO DO CPQD EM BLOCKCHAIN

O CPQD tem se dedicado às atividades de pesquisa e desenvolvimento tecnológico em Blockchain desde 2016, envolvendo-se em capacitação tecnológica, desenvolvimento de soluções e colaboração nacional e internacional. Nossa atuação abrange tanto o setor privado quanto o governo, contribuindo para o avanço da tecnologia no Brasil. Duas plataformas desenvolvidas pelo CPQD, o Trace e o iD , desempenham um papel relevante nas atividades de Pesquisa, Desenvolvimento e Inovação (PD&I). O Trace é uma plataforma modular e altamente adaptável, que oferece rastreabilidade e gestão de ativos ao longo de toda a cadeia produtiva. Baseado na tecnologia Blockchain, ele garante o compartilhamento seguro de dados, a criação de trilhas de auditoria e contratos inteligentes, promovendo eficiência e reduzindo atritos entre os diversos participantes do ecossistema de negócios. O iD, por sua vez, consiste em um conjunto de APIs que possibilitam a definição, emissão e autenticação de credenciais armazenadas em uma carteira digital. Isso confere confiança e valor aos processos de *onboarding*, autenticação, autorização e assinatura digital, melhorando a experiência do usuário em ambientes digitais. Essa abordagem tem grande potencial para fortalecer a segurança e a confiabilidade em um cenário em que a integração e a conectividade frequentemente enfrentam desafios de segurança e privacidade.

Além disso, o CPQD está pronto para apoiar atividades de desenvolvimento de soluções de Blockchain que resolvam desafios reais de negócios em diferentes segmentos de mercado.

6. REFERÊNCIAS

ADHIAPPAN, A.; CHERNETSOV, A.C.; FENOMENOV, M.; KARABUDAK, U.; KORABANOVA, A.; KISLYAKOV, S.; BELLER, L.; NATI, M.; RADIER, B.; SUSHKOV, A.; USTIMENKO, A.; VEDIN, A.; YURLOV, O.; MERIEM, T.; MESSIÉ, V.; LABIDURIE OMNES, N. **Federated CSPs Marketplace: A DLT-based Data Trust enabling Business Assurance for CSPs Platforms Federation**, 2020. Disponível em: <https://www.tmforum.org/wp-content/uploads/2020/11/Federated_CSPs_Marketplace_Whitepaper_C20.0.34.pdf>

AWAIS, M.; AHMAD, A.; AHMAD, S.; SHOUKAT, A. "Advanced Billing Architecture for Charging of Electric Vehicles using Blockchain," 2022 International Conference on Technology and Policy in Energy and Electric Power (ICT-PEP), Jakarta, Indonesia, 2022, pp. 128-132, doi: 10.1109/ICT-PEP57242.2022.9988861.

BAI, Y.; LEI, H.; LI, S.; GAO, H.; LI J.; LI, L. "Decentralized and Self-Sovereign Identity in the Era of Blockchain: A Survey," 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 500-507, doi: 10.1109/Blockchain55522.2022.00077.

BRAVE SOFTWARE. Basic Attention Token (BAT): Blockchain Based Digital Advertising. Feb, 2021. Disponível em: <https://basicattentiontoken.org/static-assets/documents/BasicAttentionTokenWhitePaper-4.pdf>. Acesso em: 04 jun. 2023.

DZHUNEV, P. Helium network - integration of blockchain technologies in the field of telecommunications. In: 2022 13th National Conference with International Participation (ELECTRONICA). [S.l.: s.n.], 2022. p. 1–4.

GÜR, A. Ö.; ÖKSÜZER, S.; KARAARSLAN, E. "Blockchain Based Metering and Billing System Proposal with Privacy Protection for the Electric Network," 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 2019, pp. 204-208, doi: 10.1109/SGCF.2019.8782375.

ITU-T. . Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions. [S.l.], 2019. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>.

LUNDKVIST, C; HECK, R; TORSTENSSON, J; MITTON, Z; SENA, M. “uPort: A Platform for Self-Sovereign Identity”. 2017, vol. 2.

MARINO, F.; MORI, L.; FORMIGONI, R.; RIBEIRO, S.; OLIVEIRA, V. Finid – gestão de identidades financeiras descentralizadas. LIFT Papers / Banco Central do Brasil, v. 2, n. 1, p. 246–294, 2020.

MOBI. THE NEW ECONOMY OF MOVEMENT: Business White Paper. [S.l.], 2021. Disponível em: <https://dlt.mobi/wp-content/uploads/2021/09/MOBI-WP_V3.0.pdf>.

MOYA OSORIO, D. P. et al. "Towards 6G-Enabled Internet of Vehicles: Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 3, pp. 82-105, 2022, doi: 10.1109/OJCOMS.2022.3143098.

NAIK, N.; JENKINS, P. "uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain," 2020 IEEE International Symposium on Systems

Engineering (ISSE), Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/ISSE49799.2020.9272223.

NGUYEN, D.C. et al. "6G Internet of Things: A Comprehensive Survey," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 359-383, 1 Jan.1, 2022, doi: 10.1109/JIOT.2021.3103320.

NGUYEN, D.C.; PATHIRANA, P.N.; DING, M.; SENEVIRATNE, A. “Blockchain for secure EHRs sharing of mobile cloud based E-Health systems,” IEEE Access, vol. 7, pp. 66792–66806, 2019.

RUAN, J.; WANG, H.; AZIZ, S.; WANG, G.; ZHOU, B.; FU, X. “Interval state estimation based defense mechanism against cyber-attack on power systems,” in 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 2017, pp. 1–5.

SAAD, W.; BENNIS, M.; CHEN, M. “A vision of 6G wireless systems: Applications, trends, technologies, and open research problems,” IEEE Netw., vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

SARASWAT, D. et al. "Blockchain-Based Federated Learning in UAVs Beyond 5G Networks: A Solution Taxonomy and Future Directions," in IEEE Access, vol. 10, pp. 33154-33182, 2022, doi: 10.1109/ACCESS.2022.3161132.

SHUKLA, S.; GUPTA, I.; NARESH, K. "Addressing Security Issues and Future Prospects of Web 3.0," 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India, 2022, pp. 1-7, doi: 10.1109/ASIANCON55314.2022.9908800.

ZHANG, Y. Cross-domain authentication scheme based on Blockchain [J], Computer Application Research, 2021, 38(06), pp. 1637-1641.

cpqd
Sua conexão
com o futuro.
WWW.CPQD.COM.BR